Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 14 058

www.leeuwarden.nl
E-mail gemeente@leeuwarden.nl

KVK-nummer 59734817
BTW-nummer NL 0019.03.664.B01

Gemeente Leeuwarden

[redacted]

Per e-mail: [redacted]@live.nl

Onderwerp	Woo-besluit
Uw kenmerk	
Ons kenmerk	2026-169018
Dienst	Veiligheidsdomein
Sector	Juridische- en Veiligheidszaken
Contact	14 058, [redacted]
WhatsApp	
Bijlagen	Documenten, toelichting inventarisatie en bezwarenbijsluiter
Datum	8 september 2026

Beste [redacted],

Op 26 juni 2026 ontvingen wij uw Woo-verzoek dat u via de website indiende. Dit verzoek gaat over de uitvoering van de AVG. In deze brief leest u ons besluit.

Uw verzoek
U verzoekt om het volgende:

‘1. Alle gegevensbeschermingseffectbeoordelingen (DPIA's) die vanaf 1 januari 2024 zijn opgesteld of geactualiseerd, inclusief de daarbij behorende adviezen van de Functionaris Gegevensbescherming en de definitieve besluitvorming.
2. Geanonimiseerde documenten betreffende datalekken, waaronder meldingen van datalekken, interne onderzoeksrapporten, evaluaties, conclusies en documenten waaruit blijkt welke organisatorische of technische maatregelen naar aanleiding van het datalek zijn genomen.
3. Interne audits, compliance-rapportages, controleverslagen en evaluaties waarin de naleving van de AVG binnen uw organisatie wordt beoordeeld.
4. Adviezen, rapportages en overige documenten van de Functionaris Gegevensbescherming betreffende de naleving van de AVG, voor zover deze niet reeds actief openbaar zijn gemaakt.
5. Documenten waarin structurele tekortkomingen, risico's, overtredingen of verbetermaatregelen met betrekking tot de verwerking van persoonsgegevens worden besproken.
6. Geanonimiseerde documenten betreffende interne onderzoeken naar mogelijke onrechtmatige verwerking van persoonsgegevens, waaronder de onderzoeksbevindingen, conclusies en eventuele verbetermaatregelen.
7. Documenten waaruit blijkt welke maatregelen zijn genomen naar aanleiding van constateringen van de Functionaris Gegevensbescherming, interne audits, datalekken of andere AVG-gerelateerde onderzoeken.
8. Managementrapportages, memo's, notities en evaluaties waarin de naleving van de AVG, de informatiebeveiliging of de bescherming van persoonsgegevens binnen uw organisatie wordt besproken.’

Besluit
Wij besluiten om uw verzoek toe te wijzen en de gevraagde documenten gedeeltelijk openbaar te maken. Hieronder lichten wij ons besluit toe.

Wettelijk Kader
Uitgangspunt van de Woo is dat er, in het belang van een goede en democratische bestuursvoering, voor degene die om informatie verzoekt, een recht op openbaarmaking van de informatie bestaat.
Artikel 1.1 Woo geeft het volgende aan: ‘Eenieder heeft recht op toegang tot publieke informatie zonder daartoe een belang te hoeven stellen, behoudens bij deze wet gestelde beperkingen.'

In de Woo en de daarop rustende bepalingen wordt verstaan onder document: ‘een door een orgaan, persoon of college opgemaakt of ontvangen schriftelijk stuk of ander geheel van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak' (artikel 2.1 Woo). Het moet gaan om bestaande documenten die daadwerkelijk fysiek aanwezig zijn. Er rust op een overheidsorgaan geen plicht om een document, zoals bijvoorbeeld een overzicht, aan te maken.

Onder 'naar zijn aard verband houdt met de publieke taak' heeft een brede betekenis. Het gaat hier om documenten die direct
of randvoorwaardelijk gerelateerd zijn aan het uitoefenen van publiek gezag of andere bestuurstaken.

Inventarisatie van de documenten
Er zijn 58 documenten gevonden die binnen de reikwijdte van uw verzoek vallen. Wij hebben bij deze inventarisatie de privacy officers en functionaris gegevensbescherming betrokken. In de bijlage bij dit besluit vindt u een toelichting op de inventarisatie per punt van uw verzoek.

Wij hebben een deel van de gevraagde informatie reeds geopenbaard vanwege een ander Woo-verzoek over de uitvoering van de AVG: Jaarrapportages en meldingen AP samengevoegd.

Motivering
Allereerst wijzen wij u op het volgende. Op grond van artikel 4.1 lid 7 Woo, wordt een verzoek om informatie ingewilligd met inachtneming van het bepaalde in hoofdstuk 5.

Het recht op openbaarmaking op grond van de Woo dient uitsluitend het publieke belang van een goede en democratische bestuursvoering. Het komt iedere burger in gelijke mate toe. De Woo kent daarnaast ook geen beperkte openbaarmaking.
Dit betekent dat openbaarmaking van de gevraagde documenten uitsluitend aan u op grond van de Woo niet mogelijk is. Wanneer de betreffende documenten aan u verstrekt worden, moeten wij deze ook aan anderen verstrekken indien zij daarom verzoeken.

Daarom kan ten aanzien van de openbaarheid de bedoeling of belangen van de verzoeker niet worden meegenomen in de te verrichten belangenafweging.

Bij de te verrichten belangenafweging worden dan ook betrokken het algemene belang bij openbaarmaking van de gevraagde informatie en de door de uitzonderingsgronden te beschermen belangen, maar niet het specifieke belang van de verzoeker.

Artikel 5.1 lid 1 van de Woo bevat absolute uitzonderingen. Het belang van openbaarheid moet te allen tijde wijken wanneer deze uitzonderingsgrond van toepassing is. Er wordt geen nadere belangenafweging gemaakt.
Artikel 5.1 lid 2 van de Woo bevat relatieve uitzonderingen. Bij relatieve uitzonderingsgronden maakt het bestuursorgaan een afweging tussen het algemene belang van openbaarheid en de door de uitzondering te beschermen belangen. Een beroep op een uitzonderingsgrond moet onderbouwd zijn.

De door u gevraagde documenten zijn deels openbaar gemaakt vanwege deze uitzonderingsgrondgronden. Hieronder leest u de motivering.

Persoonlijke levenssfeer
Op grond van artikel 5.1, tweede lid, onder e van de Woo zijn namen, directe telefoonnummers en e-mailadressen van personen niet zijnde leden van ons college, bijvoorbeeld medewerkers van onze organisatie, onleesbaar gemaakt. Deze personen treden naar de aard van hun werkzaamheden niet in de openbaarheid.

Naar onze mening weegt het belang van de persoonlijke levenssfeer van betrokkenen zwaarder dan het belang van openbaarheid. Wij wijzen daarbij op vaste jurisprudentie van de Afdeling bestuursrechtspraak van de Raad van State. Het belang van eerbiediging van de persoonlijke levenssfeer verzet zich tegen openbaarmaking van namen en contactgegevens van medewerkers binnen en buiten de organisatie die niet wegens hun functie in de openbaarheid treden, tenzij de indiener van het desbetreffende Woo-verzoek aannemelijk heeft gemaakt dat het belang van de openbaarheid in een concreet geval zwaarder weegt. Van dit laatste is niet gebleken.

Goed functioneren van de gemeente
Openbaarmaking van informatie blijft achterwege wanneer het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen, zwaarder weegt dan het belang van openbaarheid

Op grond van artikel 5.1, tweede lid, onder i van de Woo zijn melding- en registratienummers onleesbaar gemaakt. Met de melding- en registratienummers kun je zaken laten aanpassen in de meldingen van de AP. Bij openbaarmaking van deze gegevens zou dan ook het goed functioneren van de gemeente en de AP worden geschaad. Ook zijn interne e-mailadressen van de gemeente, niet zijnde persoonsgegevens afgelakt. Het openbaren van deze e-mailadressen zorgt voor mogelijke correspondentie via ongewenste kanalen. Tot slot zijn (voornamelijk in de DPIA’s) namen van leveranciers en applicaties geweigerd. Openbaarmaking van deze gegevens zou derden een inzicht verschaffen in de inrichting van het applicatie- en leverancierslandschap van de organisatie. Door deze informatie te combineren met publiek beschikbare informatie over softwareversies, bekende kwetsbaarheden, beheerrelaties en leveranciersketens kan een gerichter beeld worden verkregen van mogelijke aangrijpingspunten voor digitale aanvallen.

Gelet hierop zijn wij van mening dat het belang van de bescherming van het goed functioneren van de gemeente zwaarder weegt dan het belang van openbaarmaking.

Verstrekking
De te openbaren documenten worden samen met dit besluit verstuurd naar het bij ons bekende e-mailadres.

Bezwaar
Indien u het niet eens bent met dit besluit kunt u daartegen bezwaar maken. Wij verwijzen u kortheidshalve naar de bezwaarclausule bij dit besluit.

Vragen?
Bij vragen over deze brief kunt u contact met mij opnemen. Dat kan via telefoonnummer [redacted] en via woocontactpersoon@leeuwarden.nl onder vermelding van ons kenmerk.

Met vriendelijke groet,
Namens burgemeester en wethouders,

[redacted]

Onder deze brief treft u geen handtekening aan.
Meer informatie: https://www.leeuwarden.nl/digitalepost

BIJLAGE 1 Bezwaar maken

Bent u het niet eens met dit besluit?
Dan kunt u bezwaar maken. Dit doet u door binnen zes weken na de verzenddatum van dit besluit een brief (een 'bezwaarschrift') naar ons te sturen. In deze brief staan in ieder geval:

a uw naam en adres;
b de datum waarop u de brief heeft geschreven;
c. tegen welk besluit u bezwaar maakt;
d. het kenmerk/nummer van het besluit;
e. de reden van uw bezwaar;
f. uw handtekening.

U kunt het bezwaar digitaal indienen via www.leeuwarden.nl/bezwaarschrift of schriftelijk door het bezwaar te sturen naar de gemeente Leeuwarden, Postbus 21000, 8900 JA in Leeuwarden.

Besluit uitstellen?
Bij spoedeisende zaken kunt u vragen het besluit tijdelijk uit te stellen. Dit doet u door een 'voorlopige voorziening' aan te vragen bij Rechtbank Noord-Nederland. Hier zijn kosten voor u aan verbonden. Uiteraard is het aan de rechter om te beslissen of het besluit wel of niet kan worden uitgesteld. U kunt ook digitaal een verzoek om een voorlopige voorziening indienen bij de rechtbank via http://loket.rechtspraak.nl/bestuursrecht. Daarvoor moet u wel beschikken over een elektronische handtekening (DigiD). Kijk voor de precieze voorwaarden op de genoemde site.

Vorig jaar hebben we via dit Woo-besluit al aardig wat informatie geopenbaard over dit onderwerp:
Jaarrapportages en meldingen AP samengevoegd

Inventarisatie documenten
In het verzoek wordt gevraagd om verschillende zaken (zie ook de bijlage):
In het blauw staat aangegeven wat reeds openbaar is.

1. Alle gegevensbeschermingseffectbeoordelingen (DPIA's) die vanaf 1 januari 2024 zijn opgesteld of geactualiseerd, inclusief de daarbij behorende adviezen van de Functionaris Gegevensbescherming en de definitieve besluitvorming.	DPIA 5.1.2i voor MOL (2024-087311). DPIA digitale meldplicht (zaak Rex). DPIA Spraakassistent (2024-099354). DEPIA CT&R Herbeoordeling DEPIA gegevensdeling SD juni 2026 (2026-161857). DEPIA experiment minder typen meer luisteren (2026-088150)
2. Geanonimiseerde documenten betreffende datalekken, waaronder meldingen van datalekken, interne onderzoeksrapporten, evaluaties, conclusies en documenten waaruit blijkt welke organisatorische of technische maatregelen naar aanleiding van het datalek zijn genomen. We hebben eerder een overzicht van ons datalekregister en de integrale meldingen aan de AP gedeeld (zie gedeelde link naar openbare informatie). Deze informatie gaat tot mei 2025. Over de periode mei 2025 t/'m 26 juni 2026 moet nog geïnventariseerd worden.	register opgenomen. Meldingen AP toegevoegd
3. Interne audits, compliance-rapportages, controleverslagen en evaluaties waarin de naleving van de AVG binnen uw organisatie wordt beoordeeld.	onderzoek bij SD 1x, andere onderzoek opgenomen in herbeoordeling DEPIA gegevensdeling 5.1.2i
4. Adviezen, rapportages en overige documenten van de Functionaris Gegevensbescherming betreffende de naleving van de AVG, voor zover deze niet reeds actief openbaar zijn gemaakt. De FG jaarrapportages t/m 2024 zijn reeds openbaar.	jaarrapportage over 2025, adviezen vanuit 5.1.2i en opgeslagen in 5.1.2i toegevoegd.
5. Documenten waarin structurele tekortkomingen, risico's, overtredingen of verbetermaatregelen met betrekking tot de verwerking van persoonsgegevens worden besproken.	Geen documenten, wel email reacties op verbeteringen na datalekken
6. Geanonimiseerde documenten betreffende interne onderzoeken naar mogelijke onrechtmatige verwerking van persoonsgegevens, waaronder de onderzoeksbevindingen, conclusies en eventuele verbetermaatregelen.	zijn er niet.
7. Documenten waaruit blijkt welke maatregelen zijn genomen naar aanleiding van constateringen van de Functionaris Gegevensbescherming, interne audits, datalekken of andere AVG-gerelateerde onderzoeken.	informerende brief aan gemeenteraad bevat reactie van college op bevindingen; deze zijn al openbaar te vinden op website. Verder memo over update heraudit Wpg waarin acties zijn opgenomen.
8. Managementrapportages, memo's, notities en evaluaties waarin de naleving van de AVG, de informatiebeveiliging of de bescherming van persoonsgegevens binnen uw organisatie wordt besproken.	2026 begonnen met informeren teamleiders. Daarom nu reactie via mail opgenomen. Dashboards ontbreken, wordt na zomer 2026 start mee gemaakt via 5.1.2i 5.1.2i wordt binnen SSC-samenwerking aanbesteed. Dit loopt.

Aanlevering per punt
Wanneer mogelijk ontvang ik per punt de documenten. Als er van een bepaald punt geen documenten zijn, hoor ik dit ook graag.
Ik heb gebeld met verzoeker en vanwege de omvang van zijn verzoek, vakantieperiode en drukte omtrent Woo-verzoeken weet hij dat het verzoek langer zal duren dan de wettelijke termijn van 4 tot 6 weken.
Als het mogelijk is ontvang ik de documenten van jullie binnen 3 weken.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Inhoudsopgave

0001_0001_Register datalekken-Woo 17-05-2025 - 26-06-2026_Geanonimiseerd 3
0002_0002_Rapport Datalekken meldformulier_8-9-2025 13.15.41_Geanonimiseerd 12
0003_0003_Rapport Datalekken meldformulier_8-9-2025 12.30.54_Geanonimiseerd 20
0004_0004_Rapport Datalekken meldformulier_7-8-2025 9.08.15_Geanonimiseerd 28
0005_0005_Rapport Datalekken meldformulier_7-8-2025 11.48.10_Geanonimiseerd 36
0006_0006_Rapport Datalekken meldformulier_7-5-2026 10.03.11 (1)(1)_Geanonimiseerd 41
0007_0007_Rapport Datalekken meldformulier_31-3-2026 12.28.39_Geanonimiseerd 49
0008_0008_Rapport Datalekken meldformulier_29-1-2026 11.31.54_Geanonimiseerd 57
0009_0009_Rapport Datalekken meldformulier_28-11-2025 11.23.33 (voorlopige melding)_Geanonimiseerd 66
0010_0010_Rapport Datalekken meldformulier_27-11-2025 11.13.10 (aanvulling-definitief)_Geanonimiseerd 74
0011_0011_Rapport Datalekken meldformulier_24-6-2026 8.44.03_Geanonimiseerd 80
0012_0012_Rapport Datalekken meldformulier_23-12-2025 12.28.41 (definitieve melding)(1)_Geanonimiseerd 88
0013_0013_Rapport Datalekken meldformulier_22-5-2026 13.39.20_Geanonimiseerd 93
0014_0014_Rapport Datalekken meldformulier_22-5-2026 13.02.22(1)_Geanonimiseerd 101
0015_0015_Rapport Datalekken meldformulier_22-5-2025 11.40.00(1)_Geanonimiseerd 108
0016_0016_Rapport Datalekken meldformulier_21-7-2025 16.16.07_Geanonimiseerd 116
0017_0017_Rapport Datalekken meldformulier_21-7-2025 16.06.42(1)_Geanonimiseerd 120
0018_0018_Rapport Datalekken meldformulier_18-3-2026 16.13.03_Geanonimiseerd 128
0019_0019_Rapport Datalekken meldformulier_16-3-2026 15.29.08_Geanonimiseerd 133
0020_0020_Rapport Datalekken meldformulier_15-6-2026 10.48.53(1)_Geanonimiseerd 141
0021_0021_Rapport Datalekken meldformulier_15-1-2026 15.37.38_Geanonimiseerd 145
0022_0022_Rapport Datalekken meldformulier_13-11-2025 9.04.47_Geanonimiseerd 150
0023_0023_Rapport Datalekken meldformulier_12-12-2025 9.35.45_Geanonimiseerd 159
0024_0024_Rapport Datalekken meldformulier_12-12-2025 15.47.30_Geanonimiseerd 167
0025_0025_Rapport Datalekken meldformulier_12-1-2026 11.39.39_Geanonimiseerd 175
0026_0026_Rapport Datalekken meldformulier_1-10-2025 9.34.43_Geanonimiseerd 179
0027_0027_20250731 Melding AP datalek 20250729_Geanonimiseerd 187
0028_0028_19-06-20205 definitieve melding AP (22-05)_Geanonimiseerd 195
0029_2025-FG-Jaarverslag gemeente Leeuwarden_Geanonimiseerd 202
0030_9. Memo advies opname vergaderingen MS Teams_Geanonimiseerd 223
0031_Aanvulling DEPIA mbt data-ethiek_Geanonimiseerd (1) 230
0032_Aanvulling DEPIA mbt data-ethiek_Geanonimiseerd 239
0033_Advies dashboard Afas_Geanonimiseerd 248
0034_bijlage 1.1 - 20250310 FG-advies t.a.v. DPIA - OOV - Digitale Meldplicht V1.0 Definitief_Geanonimiseerd 251
0035_Controle deelproces team Inkomen en Zorg_Geanonimiseerd 256
0036_DEPIA [5.1.2.i] v4.5.1_Geanonimiseerd 260
0037_DEPIA - fase 1 experiment Digitale Meldplicht (def)_Geanonimiseerd 295
0038_DEPIA Spraakassistent versie getekend_Geanonimiseerd 322
0039_DPIAMA transcribeertool Gemeente Leeuwarden 1.0_Geanonimiseerd 338

0040_FW_ Aanvulling DEPIA mbt data-ethiek defintieve versie vanuit FG C2311 7797_Geanonimiseerd 377
0041_FW_ link_koppeling naar het register van verwerkingen (1)_Geanonimiseerd 379
0042_FW_ link_koppeling naar het register van verwerkingen_Geanonimiseerd 381
0043_GELWD-2023.1 Rapportage DPIA Meldpunt Overlast DEF (1) (1)_Geanonimiseerd 383
0044_herbeoordeling DEPIA _ 17 juni 2026_Geanonimiseerd 399
0045_Melding auteurnaam verwijderen uit metadata_Geanonimiseerd 410
0046_Memo datalekken bij online publicaties_Geanonimiseerd 415
0047_Memo Datalekken in raads- en informatiesystemen_Geanonimiseerd 419
0048_Memo Datalekken in raads- en informatiesystemen september 2024_Geanonimiseerd 422
0049_Memo inzetten dashboard bij MOR_Geanonimiseerd 426
0050_Memo SDF- gebruik Teams_Geanonimiseerd 429
0051_Memo update audit Wpg 2025_Geanonimiseerd 431
0052_printed_incident_M2511 4186_Geanonimiseerd 433
0053_RE_ contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen_Geanonimiseerd 438
0054_Re_ DPIAMA transcribeertool Gemeente Leeuwarden 1_0-12_Geanonimiseerd 442
0055_RE_ input rondom publicatietermijn vergunningen_Geanonimiseerd 447
0056_RE_ Memo datalekken bij online publicaties_Geanonimiseerd 449
0057_RE_ Werkwijze bij het testen van 'Meer luisteren_ minder typen'_Geanonimiseerd 451
0058_vervolg memo niet-geanonimiseerde metadata_Geanonimiseerd 454

Gemeld in	Datum incident	Aard van de inbreuk (categorieën AP)	Aard incident/oorzaak (categorieën AP)	Aantal betrokkenen	Melding AP? (ja/nee)	Korte toelichting niet melden AP	Categorie/soort persoonsgegevens	Maatregelen om datalek te beperken/weg te nemen
2025	1-1-2020	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	12) Persoonsgegevens per ongeluk gepubliceerd	medewerkers, max 10, externen onbekend.	ja		NAW, geslacht, handtekening	Documenten zijn verwijderd van internet en vervolgens juist geanonimiseerd terug geplaatst.
2025	Niet bekend	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	15) Overig, namelijk: medewerker heeft persoonlijke Downloads map per ongeluk versleept naar een afdelingsschijf.	Niet bekend	ja		NAW, geslacht, geboortedatum en/of leeftijd, BSN, e-mailadres, telefoonnummer, ras/etnische afkomst, lidmaatschap vakbond, gegevens gezondheid. Opsomming niet limitatief. In ieder geval ook gegevens die sollicitant op CV zet.	Toegang tot map voor onbevoegde ingetrokken
2025	5-8-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	ja		Naam en financiële gegevens.	Verkeerde ontvanger gevraagd mail te verwijderen. Tot op heden (7-8) nog geen bevestiging hiervan gehad. Daarom voorlopige melding eerst gedaan.
2025	1-9-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	15)overig, namelijk: document is aan een verkeerd document toegevoegd	1	ja		Naam, geboortedatum, BSN en gezondheidsgegevens	document is ingeleverd door de verkeerde ontvanger
2025	4-9-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	7) E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in de cc, in plaats van bcc	125	ja		mailadres	iedereen gevraagd de mail te verwijderen en er is een nieuwe mail verstuurd.
2025	1-3-2020	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	12) Persoonsgegevens per ongeluk gepubliceerd	9	ja		naam, adres, emailadres, telefoonnummer	document van internet gehaald en opnieuw correct geanonimiseerd
2025	4-11-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	13) Persoonsgegevens toegevoegd aan het verkeerde dossier	5	ja		naam, BSN, financiële gegevens	Nieuwe kopie dossier met excuusbrief, beveiligd verstuurd. Daarnaast onderzoek naar proces en nagaan of document in juiste dossier zit.
2025	28-2-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	15) Overig, namelijk: persoonsgegevens vrij toegankelijk op PC in publiekshal gemeente	1	ja		Geslacht, NAW, geboortedatum/leeftijd, BSN, financiële gegevens (bankrekeningnummer / IBAN, gegevens over uitkering)	Vooralsnog alleen informeren verantwoordelijken van het Meedenkpunt over risico's en tips/instructies meegeven over veilig werken.
2025	27-11-2025 en 09-12-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	5) Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)	2	ja		Naam, geslacht, geboortedatum, BSN.	Geadviseerd eigenaarsgegevens op te vragen via Kadaster. En en brief richting vakantieadres met verzoek de brieven te retourneren
2025	onbekend	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden;	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s).	3	ja		NAW, geslacht, geboortedatum en/of leeftijd, BSN, gegevens over gezondheid	foutieve domeinnaam is geblokkeerd door ICT.

2025	1-1-2021	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	13) Persoonsgegevens toegevoegd aan het verkeerde dossier;	1	nee	betreft eigen medewerker en interne afdeling. Beperkt aantal collega's hebben dit ingezien en zijn betrouwbare derde	NAW, geslacht, geboortedatum/leeftijd, BSN, financiële gegevens	Stukken zijn verwijderd uit dossier en gestuurd naar personeelszaken.
2025	4-6-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s).	Niet bekend	nee	Risico op misbruik gegevens is minimaal. Verkeerde ontvanger was medewerker van BV sport, semi-betrouwbare derde.	Naam, geslacht, e-mailadres, telefoonnummer	Verkeerde ontvanger gevraagd mail te verwijderen.
2025	Niet bekend	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	2) Autorisatie(s) van medewerker(s) verkeerd ingesteld;	Niet bekend	nee	Risico op misbruik gegevens is minimaal. Alleen collega's kunnen in TOPdesk en je moest echt goed zoeken, lek zat echt onderwater.	Naam, geslacht, mogelijk ook adressen en BSN	Functioneel beheerder heeft de filters aangepast. Onderzocht is of er andere 'fouten' in zaten, dat bleek niet het geval.
2025	11-6-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s).	1	nee	Gegevens betreffen vooral gegevens van overledene. Indien er een langstlevende was, is alleen een naam gelekt. Risico op misbruik is minimaal	Naam, geslacht	Verkeerde ontvanger gevraagd mail te verwijderen + te laten bevestigen.
2025	17-6-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	2) Autorisatie(s) van medewerker(s) verkeerd ingesteld;	7	nee	Intern datalek, betrouwbare ontvanger (medewerker). Risico op misbruik is minimaal	NAW, geslacht, geboortedatum en/of leeftijd, financiële gegevens, gegevens over gezondheid, daarnaast afspraken over condities om afscheid van elkaar te nemen bij langdurig verzuim of onenigheid tussen werkgever en werknemer.	Autorisatie is aangepast.
2025	22-6-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	2) Autorisatie(s) van medewerker(s) verkeerd ingesteld;	3	nee	Intern datalek, betrouwbare ontvanger (medewerker). Risico op misbruik is minimaal	Namen	Autorisatie is aangepast.
2025	25-6-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	150	nee	Verkeerde ontvanger is betrouwbare derde. Mail is ongelezen verwijderd. Risico op misbruik is dus nihil. Gegevens zijn dus niet ingezien door onbevoegden.	Namen + geldbedragen (financiële gegevens)	Mail is ongelezen verwijderd. Collega erop gewezen dat dit soort gegevens beveiligd en versleuteld verstuurd moeten worden.
2025	26-6-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: WhatsApp bericht verstuurd naar verkeerde persoon	4	nee	Verkeerde ontvanger heeft gemeld dat bericht niet voor hem/haar bestemd was. In bericht geen privacygevoelige gegevens of informatie. Risico op misbruik is nihil.	Naam, geslacht	Bericht is voor iedereen verwijderd. Advies aan melder: volgende keer bij eerste contact verifiëren of het nummer hoort bij de persoon die een bericht moet krijgen.
2025	2-7-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	2	nee	Verkeerde ontvanger is betrouwbare derde.	Naam, geslacht + financiele gegevens	Verkeerde ontvanger heeft direct na ontvangst contact opgenomen en mail verwijderd.

2025	22-4-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	2) Autorisatie(s) van medewerker(s) verkeerd ingesteld;	1	nee	Enkel SSC-partners konden erbij, allemaal ambtenaren, dus betrouwbare derden. Betreft enkel een gelekte naam, risico op misbruik is minimaal.	Naam.	Omgeving is meteen dicht gezet.
2025	14-7-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: document met persoonsgegevens op de printer blijven liggen	1	nee	Verkeerde ontvanger is betrouwbare derde. Document is in de daarvoor bestemde papiercontainers gedeponeerd.	Naam, adres, woonplaats, geslacht + geboortedatum.	Document is in de papiercontainer gedeponeerd. Hierdoor is het datalek weggenomen.
2025	4-7-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: Te veel persoonsgegevens inzichtelijk bij een bepaalde workflow in AFAS	onbekend	nee	Verkeerde ontvanger is collega, dus betrouwbare derde. Risico op misbruik van de gegevens is minimaal.	Naam, geslacht, geboortedatum/leeftijd, contactgegevens	Instellingen in de workflow zijn meteen aangepast, zodat deze in alle fasen gewoon AVG-proof zijn en er dus geen persoonsgegevens van derden te vinden zijn.
2025	11-8-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	5) Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)	1	nee	Verkeerde ontvanger kwam document meteen terugbrengen. Risico op misbruik van de gegevens is minimaal.	Naam, geslacht, geboortedatum/leeftijd, contactgegevens + adreshistorie.	Verkeerde ontvanger heeft document teruggebracht, daardoor is datalek niet meer actief.
2025	14-8-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	5) Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)	2	nee	Het ene document is ongeopend retour gekomen. Andere document is door CJIB geopend. Is een betrouwbare ontvanger. Risico op misbruik van de gegevens is minimaal, want is voor CJIB niet herleidbaar.	Voorletter, achternaam + laatste 3 cijfers BSN.	Poststukken opnieuw verstuurd + verzender geattendeerd op het juist sorteren/bezorgen van de post.
2025	29-8-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	5	nee	de mail is direct na ontvangst verwijderd. Persoonsgegevens van kandidaten zijn nooit ingezien	NAW, geslacht, geboortedatum	mail laten verwijderen.
2025	5-9-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: Brief door verwerker dubbelzijdig geprint door instellingen.	1	nee	Derde is betrouwbare derde: FIER!	Naam, contactgegevens, geldbedragen	brief is vernietigd en opnieuw verstuurd.
2025	18-1-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	nee	Alleen achternaam en geslacht, risico op misbruik is minimaal.	Achternaam, geslacht.	S&I heeft aan verkeerde ontvanger aangegeven dat ze de mail als niet verzonden kon beschouwen.
2025	6-8-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	2) Autorisatie(s) van medewerker(s) verkeerd ingesteld	Alle medewerkes gemeente LWD	nee	Datalek werd nog opgemerkt binnen de testfase, betrouwbare ontvangers.	Naam, aantal fte, loonschaal (geen bedrag), functienaam.	Autorisaties zijn juist ingesteld voordat de gebruikersinstructies verzonden zijn.

2025	6-10-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	11	nee	Mail betrof geen persoonsgegevens van andere inwoners. Verkeerde ontvanger heeft mails netjes verwijderd.	Zakelijke mailadressen van een aantal collega's, één privé mailadres van inwoner	Verkeerd ontvangen e-mails zijn verwijderd.
2025	8-10-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	12) Persoonsgegevens per ongeluk gepubliceerd	2	nee	Alleen enkele algemene gegevens die vrij kort niet juist geanonimiseerd online hebben gestaan.	Naam, geslacht, emailadres en telefoonnummer.	Document offline gehaald en juist geanonimiseerd weer gepubliceerd.
2025	13-10-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	nee	Verkeerde ontvanger is betrouwbare derde, datalek is meteen verholpen doordat verkeerde ontvanger meteen mail verwijderd had.	Naam, geslacht, adres, woonplaats, financiële gegevens.	Collega gewezen op het beveiligd mailen. Verkeerde ontvanger mail laten verwijderen + bevestigen.
2025	10-10-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	5) Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)	1	nee	Risico op misbruik van persoonsgegevens is minimaal, verkeerde ontvanger heeft toegezegd brief te vernietigen.	Naam, adres, woonplaats, geslacht, financiële gegevens	Verkeerde ontvanger heeft brief vernietigd.
2025	22-10-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	5) Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)	1	nee	Risico op misbruik van persoonsgegevens is minimaal, verkeerde ontvanger heeft toegezegd brief te vernietigen.	Naam, geslacht, adres, woonplaats, financiële gegevens.	Werkinstructie bij S&I over het melden van datalekken gaat aangepast worden. Hierover zijn al gesprekken met de kwaliteitsmedewerker van S&I.
2025	30-10-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	12) Persoonsgegevens per ongeluk gepubliceerd	1	nee	Hoewel vervelend dat onbekenden medewerker bellen, gaat het alleen om het telefoonnummer	Telefoonnummer	Document in offline gehaald, advies om aan ontvanger te vragen verkeerde document te vernietigen en dat te bevestigen + goed geanonimiseerd document verstrekken.
2025	12-11-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	2	nee	Verkeerde ontvanger is betrouwbare derde, risico op misbruik is minimaal, gegevens zijn al verwijderd.	Naam, geboortedatum	Verkeerde ontvanger gevraagd gegevens te verwijderen. Dit is gebeurd en bevestigd.
2025	18-11-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	nee	Alleen enkele algemene gegevens (niet mogelijk om persoon op basis hiervan te identificeren), verkeerde ontvanger heeft zelf gereageerd naar gemeente. Risico op misbruik minimaal.	Geslacht, achternaam	Aan verkeerde ontvanger is gevraagd mail te verwijderen (helaas niet bevestigd), verkeerde e-mailadres bij ontvanger is uit systeem verwijderd.

2025	21-11-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	nee	Er zijn alleen algemene gegevens gelekt. De verkeerde ontvanger is geen 'betrouwbare derde' maar heeft wel bevestigd dat zij de mail heeft verwijderd. Risico op misbruik is minimaal.	Geslacht, NAW, e-mailadres	Verkeerde ontvanger heeft mail verwijderd en dit bevestigd.
2025	29-10-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	2) Autorisatie(s) van medewerker(s) verkeerd ingesteld	Niet bekend	nee	Medewerker heeft alleen DAT-informatie gezien, geen WAT-informatie. Is betrouwbare ontvanger, risico op misbruik nihil.	Geslacht, naam, reden taak/signaal	Autorisatie is aangepast.
2025	27-11-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	12) Persoonsgegevens per ongeluk gepubliceerd	1	nee	Risico op misbruik van de gegevens is minimaal.	Naam	Geadviseerd een nieuwe mailing zonder persoonsgegevens te versturen, met verzoek de oude mail te verwijderen.
2025	16-11-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	5) Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)	2	nee	Bewindvoerderskantoor is aan te merken als betrouwbare derde. Ze hebben vermoedelijk de documenten ook vernietigd. Risico op misbruik van de gegevens is daardoor klein.	Naam, geslacht, adres, woonplaats, financiële gegevens.	Verzocht om contactgegevens van het bewindvoerderskantoor om uitvraag te doen. 2-12 verstuurd, nog even afwachten.
2025	2-12-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: persoonsgegevens laten liggen in openbaar gedeelte gemeentehuis	36	nee	Het gaat alleen om enkele algemene gegevens die voor een externe niet snel herleidbaar zijn naar individuele personen.	Naam, geslacht?, geboortedatum	Medewerker heeft op ons advies bericht op intranet gezet. Dag erna vernietigd omdat niemand de lijst heeft opghaald.
2025	19-12-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1 + ?	nee	Het gaat alleen om enkele algemene gegevens die deels openbaar / op internet te vinden zijn.	Geslacht, naam, e-mailadres	Medewerker heeft verkeerde ontvanger gevraagd mail te vernietigen en dit te bevestigen.
2026	12-3-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	5) Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)	1	ja		geslacht, NAW-gegevens	Verkeerde ontvanger heeft beschikking teruggestuurd
2026	10-1-2020	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	12) Persoonsgegevens per ongeluk gepubliceerd	1	ja		geslacht, NAW-gegevens, religieuze of levensbeschouwelijke overtuigingen, handtekening	Niet geanonimiseerde brief van website verwijderd, vervangen door geanonimiseerde versie, zoekresultaten via Google laten verwijderen
2026	6-5-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: Collega heeft via Whatsapp een video perongeluk in de "status" gezet waardoor deze in te zien was door haar contacten.	2	ja		Namen en adresgegevens van overlastmelder	Interne processen gaan bekeken worden om het gebruik van Whatsapp in de toekomst te verminderen.
2026	20-5-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	ja		Naam, adres, geslacht, email en financiële gegevens	Ontvanger is gevraagd de bijlage te verwijderen.

2026	21-5-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	7) E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in de cc, in plaats van bcc	453	ja		e-mailadres	Aan alle ontvangers is gevraagd de eerste mail te verwijderen.
2026	9-1-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	nee	Risico op misbruik van de gegevens is minimaal, verkeerde ontvanger is gevraagd gegevens te verwijderen (nog niet bevestigd).	Naam, mailadres en informatie over een aan te vragen uitkering.	Verkeerde ontvanger is gevraagd gegevens te verwijderen.
2026	20-1-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: persoonsgegevens zonder toestemming gedeeld met externe partij	1	nee	Alleen algemene persoonsgegevens, gedeeld met partij waarmee gemeente samenwerkt. Risico misbruik nihil.	Geslacht, NAW	Aan externe partij vragen gegevens te verwijderen en dit te bevestigen. Excuses aanbieden aan betrokkene.
2026	21-1-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	1) Apparaat, gegevensdrager (bijv. USB) en/of papier met persoonsgegevens kwijtgeraakt of gestolen	minimaal 1	nee	Risico op misbruik is minimaal, telefoon is volgende dag opgehaald.	Namen medewerkers	Telefoon is weer in bezit van collega.
2026	onbekend (gebeurd al enige tijd)	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: persoonsgegevens onbeveiligd/onversleuteld verstuurd.	onbekend	nee	Geen signalen dat persoonsgegevens bij onbevoegden zijn beland. Risico op misbruik is dus minimaal.	Naam, adres, woonplaats, rekeningnummer, geldbedragen (loon, IKB), loonschaal.	Werkprocessen worden aangepast om in de toekomst de laatste loonstroken op correcte wijze te verstrekken. Collega's hebben een poster gekregen met beslisboom wanneer wel en niet beveiligd te verstrekken via Cryptshare.
2026	9-2-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	7	nee	Alleen enkele algemene gegevens. Verkeerde ontvanger heeft mail verwijderd. Risico op misbruik nihil.	naam, geslacht, e-mailadres	Verkeerde ontvanger heeft de mailtjes verwijderd.
2026	onbekend	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: Documenten met persoonsgegevens lagen in een onafgesloten kast achter de beveiligde deuren.	Onbekend	nee	Betreft voor zover te beoordelen was algemene gegevens. Stukken zijn niet naar buiten gelekt, dus als ze zijn ingezien, enkel door betrouwbare derden.	Namen, adres, woonplaats, geboortedatum, mogelijk meer gegevens, maar niet duidelijk.	Opvolger van de teamleider heeft de stukken opgehaald en gaat na of de stukken vernietigd moeten worden of niet. Datalek is hiermee gedicht.
2026	9-2-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	12) Persoonsgegevens per ongeluk gepubliceerd	1	nee	Alleen enkele algemene gegevens voor zeer korte periode online. Risico op misbruik is nihil.	naam, geslacht (naam bedrijf, functie binnen bedrijf)	Nadat betrokkene heeft gebeld, is het document direct offline gehaald en geanonimiseerd weer gepubliceerd.

2026	1-1-2026	2) Persoonsgegevens per ongeluk of onopzettelijk gewijzigd	13) Persoonsgegevens toegevoegd aan het verkeerde dossier	5	nee	Gegevens zijn niet gelekt, risico op betrokkene is dus minimaal. Collega's hebben tijdig gesignaleerd dat de verkeerde persoonsgegevens waren toegevoegd en er zijn verder geen rechtshandelingen verricht.	Naam, contactgegevens, geboortedatum en/of leeftijd.	Juiste persoonsgegevens zijn toegevoegd.
2026	onbekend (25-2-2026 ontdekt)	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	2) Autorisatie(s) van medewerker(s) verkeerd ingesteld	onbekend	nee	Alleen medewerkers hebben toegang tot REX, dit zijn betrouwbare derden. Bovendien is risico op misbruik gegevens minimaal.	NAW, geslacht, gegevens over gebouwontzeggingen en mogelijk ook andere gegevens.	Betrof oude zaken. Huidige inrichting wordt rekening gehouden met vertrouwelijkheid en autorisaties.
2026	25-02-2026 (27-02-2026 ontdekt)	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	5) Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)	1	nee	Advocaat is betrouwbare derde (kantoor bovendien betrokken bij dossier), risico betrokkene is nihil.	NAW, geslacht, gegevens over afwijzing bijstand.	Advocatenkantoor heeft contact opgenomen met Bezwaar en beroep USD: zij hebben de envelop persoonlijk opgehaald. Stukken alsnog verstuurd naar rechtbank.
2026	5-6-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	9) Netwerkmappen of –locaties met persoonsgegevens zijn te breed toegankelijk ingesteld binnen de organisatie	niet bekend	nee	Alleen intern beschikbaar (betrouwbare ontvangers), kans is niet groot dat zij bestand daadwerkelijk geraadpleegd hebben.	NAW, geslacht, geboortedatum en/of leeftijd, BSN, financiële gegevens, toegangs- of identificatiegegevens, ras of etnische afkomst, lidmaatschap vakbond	Bestand van server verwijderd.
2026	23-3-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	nee	Verkeerde ontvanger was collega van andere afdeling. Heeft aangegeven meteen de mail te hebben verwijderd. Betrouwbare derde. Risico op misbruik van de gegevens is minimaal.	Naam, geslacht, adres, woonplaats, geboortedatum en/of leeftijd, BSN en gezondheidsgegevens.	Verkeerde ontvanger heeft de mail verwijderd.
2026	23-12-2025	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: rapportage met teveel persoonsgegevens gedeeld	4	nee	Gaat alleen om BSN waarbij verhuurder deze mogelijk al in zijn bezit heeft vanwege identificeren huurder. Risico op misbruik is klein.	BSN	Verhuurder een geanonimiseerde versie rapportage verzonden en verzocht 'verkeerde' rapportage te verwijderen
2026	31-3-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: persoonsgegevens naar verkeerde ontvanger gestuurd	1	nee	Bedrijf heeft zelf contact met gemeente opgenomen en mail verwijderd. Bovendien beperkt aantal gegevens waarbij alleen de financiële gegevens gevoelig zijn.	NAW, geslacht, financiële gegevens (IBAN	Verkeerde ontvanger heeft de mail verwijderd.

2026	27-3-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: zakelijke maildressen toegevoegd aan verkeerde omgeving.	37	nee	Risico op misbruik is minimaal, 3 personen hebben uberhaupt niet ingelogd. Betreffen zakelijke gegevens en de toegevoegde mensen zijn eigenlijk ook betrouwbare derden.	Namen en zakelijke mailadressen.	Leden zijn meteen de maandag weer verwijderd.
2026	1-4-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	2	nee	Verkeerde ontvanger heeft de mail verwijderd, is een betrouwbare derde (van een andere organisatie). Risico op misbruik is minimaal.	Namen en contactgegevens (mailadressen) van 2 medewerkers	Mail is verwijderd.
2026	7-4-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	nee	Collega heeft verkeerde ontvanger meteen opgebeld. Verkeerde ontvanger heeft mail ongelezen verwijderd. Datalek is hiermee gedicht en risico op misbruik is hiermee minimaal.	Naam, geslacht, geboortedatum en/of leeftijd, contactgegevens, financiële gegevens en kopie van buitenlands paspoort.	Betrokkene had zelf de kopie ID meegezonden, terwijl dit niet nodig was. Collega heeft meteen sjablonen aangepast waarin aangegeven wordt zulke stukken niet te sturen als dit niet gevraagd wordt. Daarnaast doorgegeven dat bij het doorsturen de bijlage verwijderd kan worden.
2026	5-4-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	2) Autorisatie(s) van medewerker(s) verkeerd ingesteld	Onbekend, betrof enkele	nee	Verkeerde ontvanger betrof betrouwbare derde, heeft meteen gehandeld toen bleek dat die verkeerde mails kreeg.	Naam, geslacht, feit dat iemand ziek is (want anders niet bekend dat diegene bij Zorgvandezaak loopt)	Autorisaties zijn naar verwachting goed ingeregeld, is nog uitgezocht of de fout bij ons zat of bij ZorgvandeZaak, die terugkoppeling is tot op heden niet geweest.
2026	7-4-2026	3) Persoonsgegevens permanent niet beschikbaar (verloren/vernietigd/verwijderd) en (vermoedelijk) 1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	8) Hacking, malware (bijv. ransomware) en/of phishing	12	nee	Op de gehackte website stonden alleen publieke/openbare gegevens, website is daarnaast uit de lucht gehaald. Doordat het enkel om publiekelijke gegevens gaat is er enkel een laag risico voor de betrokkenen.	Naam en emailadressen	Website is uit de lucht gehaald.
2026	18-5-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	13) Persoonsgegevens toegevoegd aan het verkeerde dossier	1	nee	Gaat enkel om een intern dossier, hierdoor zijn er betrouwbare ontvangers.	Naam, adresgegevens, geslacht, financiële gegevens	Mail uit dossier gehaald.
2026	21-5-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	15) Overig, namelijk: document met persoonsgegevens lag onbeheerd bij de printer	16	nee	Enkel collga's (betrouwbare ontvangers) konden het document mogelijk inzien.	Naam, financiële gegevens	Document vernietigd.
2026	10-6-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	nee	Enkel collga's (betrouwbare ontvangers) konden het document mogelijk inzien.	Naam, geslacht, financiële gegevens	Document vernietigd en manier van werken wordt geëvalueerd.

2026	16-6-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	3	nee	Gaat om betrouwbare ontvanger (uitvaartverzorger), geen risico voor betrokkenen en mail meteen verwijderd.	Naam, geslacht, geboortedatum, geboorteplaats	Document vernietigd en manier van werken wordt geëvalueerd.
2026	24-6-2026	1) Persoonsgegevens (mogelijk) ingezien door onbevoegden	6) E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)	1	nee	Gaat om betrouwbare ontvanger (bewindvoerder), geen risico voor betrokkenen en mail meteen verwijderd.	Naam, financiële gegevens,	Document vernietigd en manier van werken wordt geëvalueerd.

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 08 september 2025

Meldtijdstip: 13:15

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2i
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	FG
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Tweede telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	4-9-2025
(Mogelijke) einddatum van de inbreuk	4-9-2025
4.2 Wanneer is het incident ontdekt?	5-9-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	op 5 september is de melding gedaan van een datalek richting de privacy officer en de functionaris gegevensbescherming
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in de cc, in plaats van bcc

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	een uitnodiging voor een evenement is verstuurd aan 125 deelnemers met alle mailadressen in CC in plaats van in BCC

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Contactgegevens

[✓] E-mailadres

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	125
Geef een toelichting op bovengenoemd aantal:	Het betreft 125 genodigden voor het evenement.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Anders

Namelijk:	leden politieke partijen, inwoners
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	het is een groep die vaker uitgenodigd wordt voor dit evenement en bestaat uit een mix van leden politieke partijen, inwoners en werknemers. Daarbij zijn de mailadressen ook een mix van zakelijke en privé mailadressen.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	125

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	mailadressen kunnen onbehoorlijk gebruikt worden.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	De groep wordt vaker voor dit evenement uitgenodigd en zijn niet onbekend van elkaar. De mailadressen zijn echter voorheen niet eerder bekend gemaakt.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	125

Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	4-9-2025
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Er is een mail gestuurd volgend op de uitnodiging (naar aanleiding van een opmerking van één van de genodigden), met daarin aangegeven dat de mailadressen per abuis in CC zijn verstuurd in plaats van in BCC. Er is aan iedereen gevraagd de mail te verwijderen en er is gewezen op het risico van mogelijk misbruik van de mailadressen. Daarbij is de contactpersoon van de gemeente als contactpersoon aangewezen bij vragen etc. Deze schakelt met de FG indien nodig.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per e-mail

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Er is aan de ontvangers gevraagd om de mail te verwijderen en er is een nieuwe, juiste mail verstuurd.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Er is extra aandacht gevraagd voor het versturen van dergelijke mails in BCC. Ook is voorgesteld om een verzendlijst aan te maken, waardoor de zichtbaarheid van alle mailadressen is gegarandeerd.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: [redacted]

Melddatum: 08 september 2025

Meldtijdstip: 12:30

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	FG
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Tweede telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	1-9-2025
(Mogelijke) einddatum van de inbreuk	2-9-2025
4.2 Wanneer is het incident ontdekt?	4-9-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Op 4 september is er in de middag een melding van het datalek gedaan richting de privacy officer en de Functionaris gegevensbescherming.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja
Beschrijf hieronder waarom u de inbreuk later dan 72 uur na ontdekking meldt:	Door vergissing in de datum door de FG is de melding vandaag pas doorgegeven aan de AP. Het datalek zelf is de dag na het ontstaan van de melding afgehandeld en daarmee opgelost.

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Overig

Namelijk:	Na aangifte van erkenning is de betreffende akte in een envelop gedaan om mee te geven. Daarbij

is per abuis een zwangerschapsverklaring van een andere inwoner toegevoegd.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Na aangifte van erkenning is de betreffende akte in een envelop gedaan om mee te geven. Daarbij is per abuis een zwangerschapsverklaring van een andere inwoner toegevoegd en meegegeven aan derden.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geboortedatum en/of leeftijd

[✓] Burgerservicenummer (BSN)

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

[✓] Gegevens over iemands gezondheid

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Er zijn gegevens gelekt van 1 persoon

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	inwoners gemeente Leeuwarden
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	het betreft inwoners
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Identiteitsdiefstal of -fraude

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Naam en BSN zijn gelekt, alsmede gezondheidsgegevens. De onjuiste ontvangers hebben het document de volgende dag weer ingeleverd en daarmee is het risico beperkt.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	1
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	2-9-2025
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Er is aangegeven dat de verklaring per abuis is meegegeven aan andere inwoners, welke het document de volgende dag weer hebben teruggebracht. Er is uitgelegd wat het mogelijke risico is en de contactgegevens van de FG zijn doorgegeven.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Telefonisch

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Het document is de volgende dag door de verkeerde ontvanger terug gebracht.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Tijdens het teamoverleg is het incident besproken en aangegeven dat er extra gecontroleerd moet worden op de gegevens, voordat documenten worden meegegeven aan een inwoner.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 07 augustus 2025

Meldtijdstip: 09:08

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	FG 008121
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	privacy@leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	5-8-2025
4.2 Wanneer is het incident ontdekt?	6-8-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Collega heeft melding bij ons (privacy officers) gedaan. Verkeerde ontvanger heeft gereageerd dat betrokkene niet meer bereikbaar is via het mailadres waar de gegevens naartoe waren gestuurd.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd?	De verkeerde ontvanger heeft niet gereageerd

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Betreft een betalingsachterstand in het kader van de TOZO-regeling. Betrokkene heeft een mailadres bij aanmelden doorgegeven. Blijkbaar is het bedrijf overgedragen aan huidige eigenaren. Bij het aanschrijven van betrokkene omtrent de betalingsachterstand, is het mailadres dat bij ons bekend was gebruikt. Huidige eigenaren hebben ons erop geattendeerd dat betrokkene het bedrijf

heeft overgedragen en niet bereikbaar is via dat mailadres.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Financiële gegevens

[✓] Gegevens over (problematische) schulden

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Betreft 1 mail

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Betrokkene is (ex)ondernemer die gebruik heeft gemaakt van de TOZO-regeling.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Reputatieschade

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Het betreft informatie omtrent iemand zijn financiële situatie (schulden). Dit is erg vervelend voor betrokkene dat de huidige eigenaren van het bedrijf dit nu weten. Echter kan er weinig misbruik van de gegevens worden gemaakt, dus vandaar de keuze voor beperkt.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	1

Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	6-8-2025
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Betrokkene is gemeld dat de mail inzake betalingsachterstand per abuis naar verkeerd mailadres is gestuurd. Er is aangegeven welke maatregelen er zijn genomen om het datalek te beperken/te stoppen (verwijderen mail). Daarnaast vermeld dat er melding gedaan is van het datalek + contactgegevens van de FG gedeeld.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per e-mail

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Verkeerde ontvanger is verzocht de ontvangen mail te verwijderen. Hier tot op heden nog geen reactie op gehad. Daarom een voorlopige melding, in de hoop dat verkeerde ontvangers spoedig reageren dat de mail verwijderd is.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Collega erop gewezen dat financiële gegevens versleuteld verstuurd moeten worden + het wachtwoord via een ander kanaal. Hiermee had dit datalek voorkomen kunnen worden.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	22-8-2025

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: [redacted]

Melddatum: 07 augustus 2025

Meldtijdstip: 11:48

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	[redacted]

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	[redacted]
Functie	[redacted]
E-mailadres	privacy@leeuwarden.nl
Telefoonnnummer	[redacted]
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

[✓] Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	5-8-2025
(Mogelijke) einddatum van de inbreuk	7-8-2025

Wanneer heeft u het datalek voor het eerst aan de AP gemeld?	7-8-2025
4.2 Wanneer is het incident ontdekt?	6-8-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Collega heeft melding bij ons (privacy officers) gedaan. Verkeerde ontvanger heeft gereageerd dat betrokkene niet meer bereikbaar is via het mailadres waar de gegevens naartoe waren gestuurd.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	1
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	6-8-2025
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Betrokkene is gemeld dat de mail inzake betalingsachterstand per abuis naar verkeerd mailadres is gestuurd. Er is aangegeven welke maatregelen er zijn genomen om het datalek te beperken/te stoppen (verwijderen mail). Daarnaast vermeld dat er melding gedaan is van het datalek + contactgegevens van de FG gedeeld.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per e-mail

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Verkeerde ontvanger is gevraagd mail te vernietigen. Tijdens het maken van de voorlopige melding, nog geen reactie gehad. Inmiddels nu wel. Vandaar definitieve melding, omdat verkeerde ontvanger bevestigd heeft de mail vernietigd te hebben. Datalek is hiermee verholpen.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Bij collega aangegeven dat dergelijke gegevens beveiligd/versleuteld verstuurd moeten worden. En andere adviezen om dergelijke datalekken te voorkomen. Aangeraden dit in teamverband te bespreken.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 07 mei 2026

Meldtijdstip: 10:03

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	6-5-2026
(Mogelijke) einddatum van de inbreuk	6-5-2026
4.2 Wanneer is het incident ontdekt?	6-5-2026
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Collega heeft datalek gemeld via interne procedure nadat zij erop gewezen was door haar manager en twee andere contacten.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Overig

Namelijk:	Collega heeft via Whatsapp een video perongeluk in de "status" gezet waardoor deze in te zien was door haar contacten.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Collega heeft in het kader van overlast een video ontvangen via Whatsapp. Collega wilde deze doorsturen naar andere partijen en heeft tijdens het doorsturen per ongeluk de video inclusief begeleidend bericht met o.a. de naam van de overlastgever in de "status: gezet (soort story voor bij Whatsapp). Deze "status" heeft 20 minuten

"open" gestaan en is na kennisneming door twee contacten van collega en de betreffende manager meteen offline gehaald. Het is niet te herleiden	wie en hoeveel personen de "status" hebben ingezien.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Contactgegevens

[✓] Adres en woonplaats

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	2
Geef een toelichting op bovengenoemd aantal:	1 record voor de video en 1 record vanwege het doorgestuurde bericht.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Inwoners (overlastgever en melder).
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	In de video is de overlastgever te zien, in het bericht staat de naam van de melder en de naam van de overlastgever genoemd.

7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	2

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Reputatieschade

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Bericht heeft maar 20 minuten online gestaan en enkel voor de contacten van de collega. Van 3 personen is bevestigd dat zij de video hebben gezien, hierdoor is het risico voor de betrokken personen beperkt.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja

Aan hoeveel personen heeft u de inbreuk gemeld?	1
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	6-5-2026
Licht toe aan welke (groep) betrokkenen u de inbreuk heeft gemeld:	Het datalek is aan de melder (en zender van de video) gemeld. Het datalek is na belangenafweging van de sectormanager niet gemeld aan de overlastgever die in de video staat. Dit is gedaan omdat dit de relatie tussen melder en overlastgever (en de rest van de buurt) kan laten escaleren en daardoor de veiligheid in het geding kan komen.
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Collega heeft melder gebeld en hierbij aangegeven dat de video per ongeluk 20 minuten in de status stond, wat de gevolgen kunnen zijn en dat de video is verwijderd en dat we intern gaan kijken hoe we het proces kunnen verbeteren om dit soort dingen te voorkomen. Mogelijkheid tot vragen kan bij de betreffende privacy medewerkers. Melder reageerde positief.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Telefonisch

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Er is sprake van een zwaarwegend belang om de getroffen personen niet te informeren

Namelijk:	In verband de mogelijkheid tot escalatie tussen de melder, overlastgever en de buurt is door de sectormanager besloten om geen melding te doen aan de overlastgever.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	De video is offline gehaald en van de personen waarvan bekend is geweest dat zij de video hebben gezien is gevraagd ter bevestiging dat zij de status en het bericht niet hebben opgeslagen (dit is namelijk ook niet mogelijk bij statussen).
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Intern gaan we de processen nakijken om andere mogelijkheden tot het versturen en ontvangen van video's zodat Whatsapp minder meer gebruikt wordt.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i [redacted]

Melddatum: 31 maart 2026

Meldtijdstip: 12:28

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	FG 008121
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	10-1-2020
4.2 Wanneer is het incident ontdekt?	27-3-2026
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Betrokkene heeft contact met de gemeente opgenomen.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Nee
Wanneer heeft u kennis gekregen van het datalek?	30-3-2026

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Persoonsgegevens per ongeluk gepubliceerd

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Een brief met datum 9 januari 2020 aan de Burgemeester en Wethouders en de gemeenteraad van Leeuwarden is gepubliceerd op de website van de gemeente zonder dat de persoonsgegevens zijn geanonimiseerd. De brief betrof een protest tegen het verruimen van winkeltijden afkomstig van de protestantse wijkgemeente De Fontein te Leeuwarden.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] E-mailadres

[✓] Telefoonnummer

[✓] Anders

Namelijk:	Handtekening betrokkene

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

[✓] Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Eén brief met de gegevens.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Inwoner gemeente Leeuwarden, brief is geschreven vanuit zijn hoedanigheid als scriba bij de Protestantse wijkgemeente.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Stigmatisering (kerkenraad maakt protest tegen verruimen winkeltijden, betrokken schrijft de brief als scriba namens kerkenraad, met in de brief zijn privégegevens).

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar

Licht uw keuze toe:	Er zijn alleen algemene persoonsgegevens gelekt. De brief staat al ruim 6 jaar op de website van de gemeente. Als betrokkene hier nadelige gevolgen van heeft ondervonden, had hij dit waarschijnlijk ook in zijn melding aangegeven.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nee

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Betrokkene heeft het datalek zelf gemeld bij de gemeente. Uiteraard is ons advies wel om een excuusbrief naar betrokkene te sturen.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Niet geanonimiseerde brief verwijderen van website, inclusief uit zoekresultaten Google.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Bij eerdere, vergelijkbare datalekken is intern contact geweest met de betrokken medewerkers over het (op de juiste manier) anonimiseren van persoonsgegevens bij het publiceren van documenten op de website. Er is daarbij ook

geadviseerd om documenten die in het verleden zijn gepubliceerd alsnog te anonimiseren. We vragen nogmaals aandacht voor deze actie, het	kan zijn dat deze brief uit 2020 per abuis nog niet is geanonimiseerd.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 29 januari 2026

Meldtijdstip: 11:31

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2i
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	FG
E-mailadres	FG@leeuwarden.nl
Telefoonnummer	5.1.2e
Tweede telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	13-1-2026
4.2 Wanneer is het incident ontdekt?	19-1-2026
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Er is een klacht ingediend door client A, die via client B een afbeelding kreeg van een verslag waarin persoonsgegevens stonden van client A. Client A heeft een kind met de zoon van client B.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Nee
Wanneer heeft u kennis gekregen van het datalek?	27-1-2026

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Persoonsgegevens toegevoegd aan het verkeerde dossier

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Client A heeft bij standaard onderzoek verklaard 5.1.2e woonachtig is bij 5.1.2e 5.1.2e client B. Daarop is de uitkering van client B aangepast, waarop client B een bezwaarprocedure is gestart. De verklaring van

client A is in zijn geheel aan het bezwaardossier toegevoegd, als ondersteunend stuk. In dat document stond het hele verslag van het gesprek met client A en daarmee veel meer

persoonsgegevens of informatie over betrokkene, welke niet toegevoegd hadden moeten worden aan het bezwaardossier van client B.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Geboortedatum en/of leeftijd

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] E-mailadres

[✓] Telefoonnummer

[✓] Financiële gegevens

[✓] Gegevens over (problematische) schulden

[✓] Andere financiële gegevens

Namelijk:

Informatie over betalingen en leningen van anderen

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	2
Geef een toelichting op bovengenoemd aantal:	Het betreft allerlei persoonsgegevens over client A 5.1.2e

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Het betreft een inwoner van gemeente Leeuwarden met een uitkering
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	2

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Reputatieschade

[✓] Betrokkenen kunnen bijvoorbeeld (de verwerking van) hun persoonsgegevens niet inzien of op verzoek laten verwijderen (Uitoefening van rechten)

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Aanzienlijk
Licht uw keuze toe:	de onjuiste ontvanger is op dit moment niet genegen om de onterecht ontvangen documenten terug te geven danwel te vernietigen. De relatie tussen client A, client B 5.1.2e 5.1.2e is niet goed, waardoor niet na te gaan is, wat er met de gegevens van client A gaat gebeuren.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Ja
Aan hoeveel personen wilt u de inbreuk gaan melden?	2
Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?	30-1-2026
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	de klacht van client A wordt behandeld en aangegeven dat gemeente Leeuwarden dit beschouwd als een datalek. 29-1 wordt geprobeerd om bij client B de documenten op te halen en via een brief (waar client B om heeft gevraagd) aan te geven op grond waarvan de documenten moeten worden overhandigd. we geven daarbij dus aan wat we hebben gedaan om het datalek te beeindigen en welke risico's client A loopt. Contactgegevens van zowel de FG als van

de afdeling juridische zaken zullen worden	gedeeld, omdat client A gemeente Leeuwarden ook aansprakelijk heeft gesteld.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per brief

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	er wordt geprobeerd om de documenten op te halen bij client B. Deze heeft dit eerder geweigerd, omdat zij een brief wilde hebben van gemeente Leeuwarden, omdat zij wilde weten op welke grond zij de documenten zou moeten inleveren.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Er wordt kritischer gekeken naar de inhoud van de documenten die door de Adviescommissie Bezwaren worden opgevraagd en waar nodig geanonimiseerd.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk
Geef aan wanneer u (uiterlijk) een vervolgmelding doet	27-2-2026
Toelichting	Het staat nog niet vast, dat het datalek wordt gestopt; onbekend is of client B de documenten alsnog gaat inleveren.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2, 3, 5, 6
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 28 november 2025

Meldtijdstip: 11:23

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2i
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Onbekend
(Mogelijke) startdatum van de inbreuk	28-2-2025
4.2 Wanneer is het incident ontdekt?	27-11-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Collega informatiebeveiliging heeft contact opgenomen om te overleggen of een melding van beveiligingsincident tevens een datalek is.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Overig

Namelijk:	Persoonsgegevens vrij toegankelijk op PC in publiekshal gemeente.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	De gemeente Leeuwarden heeft een Meedenkpunt waar ze inwoners kunnen helpen met allerlei vragen. Het Meedenkpunt is in de publiekshal van de gemeente. Daar staan ook computers. Op één van de computers zag een medewerker twee bestanden met persoonsgegevens staan. De computers zijn op zich voor iedereen vrij toegankelijk. De medewerker heeft dit vervolgens gemeld bij de collega's van informatiebeveiliging; zij hebben weer contact opgenomen met Privacy

om te overleggen of er tevens sprake is van een datalek.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Geboortedatum en/of leeftijd

[✓] Burgerservicenummer (BSN)

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] Financiële gegevens

[✓] Bankrekeningnummer / IBAN

[✓] Gegevens over uitkering en/of toeslagen

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	2
Geef een toelichting op bovengenoemd aantal:	2 bestanden: een toekenning WW uitkering en een betaalspecificatie WW, beide afkomstig van het UWV.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Inwoner van gemeente Leeuwarden.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	stigmatisering.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt

Licht uw keuze toe:	Hoewel er ook gevoelige persoonsgegevens zijn gelekt (BSN en financiële gegevens) weten we niet of een onbevoegde de bestanden daadwerkelijk heeft geopend. Vandaar inschatting 'Beperkt'.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Het advies is betrokkene wel te informeren. Op dit moment is hier nog geen duidelijkheid over.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nog niet bekend
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nee, want:
Toelichting:	Aan melder geadviseerd om de bestanden z.s.m. veilig te stellen (i.v.m. afhandelen datalek, informeren betrokkene) en vervolgens te verwijderen van de desbetreffende computer. Ook gevraagd of gecontroleerd is dat de computers geen andere bestanden bevatten met persoonsgegevens. Hierover nog geen uitsluitsel gehad. Er zijn ook acties gestart om ervoor te zorgen dat de computers niet meer vrij toegankelijk zijn. Verder zal aan de

proceseigenaar worden geadviseerd om geen bestanden met persoonsgegevens op deze computers op te slaan of deze (als het wel nodig is) direct na contact met de inwoner te verwijderen.	

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	24-12-2025

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer [redacted]

Melddatum: 27 november 2025

Meldtijdstip: 11:13

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	[redacted]

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	[redacted]
Functie	Privacy Officer
E-mailadres	[redacted]@leeuwarden.nl
Telefoonnnummer	[redacted]
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

[✓] Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

[✓] Aantal personen die door de inbreuk zijn getroffen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	4-11-2025

(Mogelijke) einddatum van de inbreuk	25-11-2025
Wanneer heeft u het datalek voor het eerst aan de AP gemeld?	13-11-2025
4.2 Wanneer is het incident ontdekt?	10-11-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	5.1.2e 5.1.2e die kopie dossier van 5.1.2e 5.1.2e heeft ontvangen, heeft het datalek gemeld.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

7 Betrokkenen

7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	5

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nee

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	In het document (brief) over derdenbeslag staat alleen een naam van betrokkene. Hiermee is de

persoon niet herleidbaar voor de verkeerde ontvanger.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Verzoekers hebben nieuw kopie dossier ontvangen, zonder het verkeerde document, met excuusbrief. Na overleg met een vakjurist zijn nog 4 namen van medewerkers geanonimiseerd. Anonimiseren BSN van verzoekers is lastig omdat op sommige documenten alleen het BSN staat (dus geen andere identificerende persoonsgegevens). Geadviseerd om bij dit soort documenten alleen laatste vier cijfers van het BSN te laten staan.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	In aanvulling op eerdere melding: - Teamleider gaat proces onderzoeken (ontvangen en registreren van bestanden die een inwoner beveiligd naar de gemeente verstuurt, hoe het kan dat een document gekoppeld is aan een verkeerd dossier en waarom dit niet is opgemerkt). - Teamleider laat uitzoeken of het document ook in het juiste dossier is opgenomen (zo niet, dan alsnog in het dossier laten opnemen).

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

AP bescherming in een digitale wereld

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 3
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i [redacted]

Melddatum: 24 juni 2026

Meldtijdstip: 08:44

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Onbekend
(Mogelijke) startdatum van de inbreuk	22-6-2026
4.2 Wanneer is het incident ontdekt?	22-6-2026
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Inwoner heeft medewerkers van de gemeente op de hoogte gesteld van het datalek. Medewerker heeft datalek vervolgens conform de interne procedure gemeld.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd dat de persoonsgegevens vernietigd zijn, of zijn de persoonsgegevens teruggestuurd?	De verkeerde ontvanger heeft niet gereageerd

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Aanslag is naar verkeerde adres verstuurd. Betrokkene woont daar al geruime tijd niet meer, huidige bewoner heeft envelop geopend en datalek gemeld bij de gemeente.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] Financiële gegevens

[✓] Gegevens over uitkering en/of toeslagen

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Het gaat een verkeerd verstuurde brief van 1 persoon.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Inwoner gemeente
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Gaat om een verkeerd verstuurde brief van een inwoner van de gemeente.

7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Reputatieschade

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	Verkeerde ontvanger heeft zelf het datalek gemeld, staan alleen naam, geslacht (oude adres) en financiële gegevens in. Hierdoor is het risico op misbruik klein.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Het is nog niet duidelijk of de vakafdeling de betrokkene gaat informeren.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Inwoner is gevraagd om de brief te vernietigen, nog geen reactie van ontvangen.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nog niet bekend

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.

- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	24-7-2026
Toelichting	Inwoner moet nog bevestigen of de brief is vernietigd.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: [redacted]

Melddatum: 23 december 2025

Meldtijdstip: 12:28

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	[redacted]

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	[redacted]
Functie	Privacy Officer
E-mailadres	[redacted]@leeuwarden.nl
Telefoonnnummer	[redacted]
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

[✓] Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	28-2-2025
(Mogelijke) einddatum van de inbreuk	27-11-2025

Wanneer heeft u het datalek voor het eerst aan de AP gemeld?	28-11-2025
4.2 Wanneer is het incident ontdekt?	27-11-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Zie voorlopige melding: Collega informatiebeveiliging heeft contact opgenomen om te overleggen of de melding van dit beveiligingsincident tevens een datalek is.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nee

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Vanuit Privacy hebben we geadviseerd om betrokkene wel te informeren. De bestanden zijn ook direct na het ontdekken van het datalek op een beveiligde USB-stick bewaard (en verwijderd van de desbetreffende computer). Deze zijn echter op verzoek van de teamleiders verwijderd waardoor het niet meer mogelijk is betrokkene te informeren.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Bestanden zijn direct veiliggesteld op een USB-stick met een wachtwoord en verwijderd van de desbetreffende computer. Er is verder gecontroleerd of de desbetreffende computers nog meer bestanden met persoonsgegevens bevatten. Dit bleek niet het geval.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	De huidige computers vervangen door dockingstations. Medewerkers kunnen deze alleen gebruiken in combinatie met hun eigen laptop. Zo zijn de computers niet meer onbeveiligd toegankelijk voor iedereen en is het dus niet meer mogelijk om bestanden op te slaan die onbevoegden zouden kunnen raadplegen.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 22 mei 2026

Meldtijdstip: 13:39

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Onbekend
(Mogelijke) startdatum van de inbreuk	20-5-2026
4.2 Wanneer is het incident ontdekt?	21-5-2026
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Collega heeft het datalek via de interne procedure gemeld, nadat de inwoner een mail had gestuurd dat er een verkeerde bijlage was gestuurd.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd?	De verkeerde ontvanger heeft niet gereageerd

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Een inwoner heeft een verkeerde bijlage ontvangen. De bijlage was een ontvangstbevestiging van een ingezonden administratief beroep voor kwijtschelding. In de bijlage stond alleen een voornaam, achternaam, email, adres, geslacht en het feit dat het beroep op de kwijtschelding was ontvangen. De inwoner heeft een mail gehad of deze de bijlage wilde verwijderen, maar hier hebben we nog geen reactie gehad. Verder hebben we de betreffende

vakafdeling geadviseerd om de betrokkene te informeren.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] E-mailadres

[✓] Financiële gegevens

[✓] Gegevens over (problematische) schulden

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Het gaat om de gegevens van 1 persoon.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Inwoner gemeente
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Gaat om een inwoner van onze gemeente.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Reputatieschade

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	De bijlage gaat enkel over het feit dat iemand een administratief beroep voor kwijtschelding heeft gedaan. Verder staan er geen andere financiële gegevens in de bijlage, hierdoor is het risico verwaarloosbaar voor de betrokkene.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Betrokken vakafdeling geadviseerd om de betrokkene te informeren. Hier nog geen reactie op ontvangen.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Interne procedures aanscherpen.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	De interne procedures gaan aangescherpt worden.

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	22-6-2026
Toelichting	Wanneer we reactie hebben van de inwoner met betrekking tot het verwijderen van de bijlage en we antwoord hebben van de betrokken vakafdeling zal de vervolgmelding worden gedaan.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 22 mei 2026

Meldtijdstip: 13:02

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Onbekend
(Mogelijke) startdatum van de inbreuk	21-5-2026
4.2 Wanneer is het incident ontdekt?	21-5-2026
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De medewerker die de mail had verstuurd ging aan het eind van de dag de mailbox controleren op ingekomen mail en toen zag ze de reacties op de verstuurde mail.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in de cc, in plaats van bcc

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Er is een mail verstuurd vanuit de mailbox omgevingsvisie met algemene informatie (uitslag van een enquête). De mail moest naar een grote groep personen en is in vier etappes verstuurd (in Outlook is ingesteld dat een mail naar maximaal 500 personen verstuurd kan/mag worden). Bij drie mailtjes zijn alle e-mailadressen in de BCC gezet, bij de vierde mail is dat per ongeluk niet gedaan. Deze mail is naar 453 e-mailadressen verstuurd waarbij iedereen dus kon zien aan wie de mail verstuurd was.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Contactgegevens

[✓] E-mailadres

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	453
Geef een toelichting op bovengenoemd aantal:	De mail is naar 453 e-mailadressen verstuurd.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Inwoners/burgers die hebben deelgenomen aan een online enquête.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	453

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Misbruik van ontvangen e-mailadressen

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Het gaat alleen het e-mailadres. Ernst van mogelijke gevolgen voor betrokkenen is daarom verwaarloosbaar tot beperkt.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	453
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	22-5-2026
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	De oorspronkelijke mail is nogmaals naar de geadresseerden verstuurd, dit keer in de BCC, met daarbij de vermelding dat de eerste mail per

ongeluk niet via de BCC is verstuurd. Tevens excuses, verzoek om die mail te verwijderen en dat het datalek gemeld is aan de	privacymedewerkers die het volgens de interne procedure gaan afhandelen.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per e-mail

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Mail naar alle betrokkenen met verzoek de oorspronkelijke mail van 21 mei 2026 met alle e-mailadressen erin te verwijderen.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Het is bekend dat dergelijke mailtjes via de BCC verstuurd moeten worden. Helaas is dat in dit geval bij één van de vier mailtjes per ongeluk niet goed gegaan.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 22 mei 2025

Meldtijdstip: 11:40

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2i
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	FG
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Tweede telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	1-1-2020
4.2 Wanneer is het incident ontdekt?	22-5-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Via een brief van Geonovum, waarin wordt aangegeven dat er mogelijk persoonsgegevens in de metadata staat van gepubliceerde documenten. Daarop zijn we gaan controleren op de publicatie-website en vonden we documenten die niet-geanonimiseerd gepubliceerd zijn.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Persoonsgegevens per ongeluk gepubliceerd

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Documenten in verband met omgevingsplannen en bestemmingsplannen zijn niet-geanonimiseerd gepubliceerd en daarmee online toegankelijk.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] E-mailadres

[✓] Anders

Namelijk:	handtekening van ondertekenaars van de brieven

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	100
Geef een toelichting op bovengenoemd aantal:	Het aantal records is een schatting; er staan documenten vanuit zeker 2020, die nog gecontroleerd moeten worden op de mate van anonimisering.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Het betreft zowel werknemers als in behandelend ambtenaar als ondertekenaar en klanten als in aanvragers van vergunningen en mogelijk ook insprekers bij bespreken van bestemmingsplannen.
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	100

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Identiteitsdiefstal of -fraude

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt

Licht uw keuze toe:

het aantal belangstellenden voor dergelijke documenten is laag, evengoed is er een risico op	misbruik van persoonsgegevens

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Er wordt een inventarisatie gemaakt van het aantal documenten, het aantal betrokkenen en dan wordt besloten of deze wel/niet en hoe worden geinformeerd.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nee, want:
Toelichting:	Het is een grote klus om alle documenten te verwijderen en geanonimiseerd terug te plaatsen. Er wordt bekeken of de toegang tot de website tijdelijk geblokkeerd kan worden om het risico te beperken.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nog niet bekend

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	19-6-2025
Toelichting	de proceseigenaar is ingeschakeld om te komen tot een inventarisatie van het probleem, de vervolgacties te bepalen en ook om herhaling te voorkomen.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: [redacted]

Melddatum: 21 juli 2025

Meldtijdstip: 16:16

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	[redacted]

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	[redacted]
Functie	Privacy Officer
E-mailadres	[redacted]@leeuwarden.nl
Telefoonnnummer	[redacted]
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	1
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	18-7-2025

Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Wat er is gebeurd, welke maatregelen getroffen zijn, datalek gemeld bij de AP, mogelijkheid tot het indienen van een klacht bij zowel gemeente als AP.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Telefonisch

[✓] Per e-mail

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 21 juli 2025

Meldtijdstip: 16:06

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	12-6-2025
4.2 Wanneer is het incident ontdekt?	16-7-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Collega heeft melding datalek gedaan. Kwam erachter nadat een document dat fysiek is afgegeven niet in het dossier is gevoegd, omdat wettelijk vertegenwoordiger een dwangsom bij niet tijdig beslissen had ingediend.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Nee
Wanneer heeft u kennis gekregen van het datalek?	21-7-2025

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

[✓] Persoonsgegevens permanent niet beschikbaar (verloren/verwijderd)

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Brief of postpakket met persoonsgegevens kwijtgeraakt

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Wettelijk vertegenwoordiger van betrokkene heeft fysiek op het gemeentehuis een document m.b.t. de aanvraag/verlenging van het PGB ingediend. Dit document is kwijtgeraakt. Collega kwam hierachter omdat wettelijk vertegenwoordiger een dwangsom bij niet tijdig beslissen heeft ingediend. Bij raadplegen van het dossier bleek

dat het stuk niet is toegevoegd en dus kwijt is	geraakt. Document is nog steeds niet terecht gekomen.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Geboortedatum en/of leeftijd

[✓] Burgerservicenummer (BSN)

[✓] Contactgegevens

[✓] Adres en woonplaats

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

[✓] Gegevens over iemands gezondheid

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Betreft 1 brief.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Minderjarigen

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Betrokkene is minderjarig.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Reputatieschade

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Aanzienlijk
Licht uw keuze toe:	Door verlies van het document is er niet tijdig beslist op een aanvraag voor betrokkene. PGB wordt aangevraagd met als doel zorg in te kunnen kopen waar betrokkene afhankelijk van is. Dit kon nu niet.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	1
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	18-7-2025
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Verteld wat is gebeurd, welke maatregelen er genomen zijn, wat we gaan doen om dit in de toekomst te voorkomen, dat we datalek melden bij de AP, dat betrokkene mogelijkheid heeft tot het indienen van een klacht.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Telefonisch

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nee, want:
Toelichting:	Document is gewoonweg kwijt. Vermoedelijk papiercontainer, maar dat weten we niet zeker.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Collega die het stuk heeft ingenomen wordt op de hoogte gebracht van de processen, om soortgelijke gevallen in de toekomst te voorkomen.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	31-7-2025

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: [redacted]

Melddatum: 18 maart 2026

Meldtijdstip: 16:13

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	[redacted]

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	[redacted]
Functie	FG
E-mailadres	[redacted]@leeuwarden.nl
Telefoonnnummer	[redacted]
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	1

Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	27-2-2026
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Er is aangegeven wat er precies is gebeurd en welke gevolgen dat mogelijk kan hebben. Ook zijn de gegevens van de FG medegedeeld en van de medewerker Verzekeringen. De ene betrokkene was inmiddels op de hoogte en had een klacht ingediend. Naar aanleiding van het datalek heeft zij gemeente Leeuwarden aansprakelijk gesteld.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per brief

[✓] Per e-mail

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Er is op 30-1 een brief persoonlijk overhandigd aan de persoon die een bezwaarprocedure had lopen. op 18 maart is een 2e verzoek gestuurd (omdat het eerste verzoek niet formeel genoeg was), om de ongelakte documenten terug te sturen. Ook zijn de zwartgelakte documenten per mail en per post naar de persoon gestuurd.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	er is met de betreffende medewerkers gesproken over het toesturen van gevraagde documenten door de bezwaarcommissie. De afspraak is dat er nu (nog meer dan eerder) wordt gecontroleerd op de relevantie van aanwezige persoonsgegevens van derden in dergelijke stukken. En dat er advies kan worden gevraagd aan de privacy officers, voordat de documenten worden verstuurd naar de secretaris van de Bezwaarcommissie.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 16 maart 2026

Meldtijdstip: 15:29

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	12-3-2026
(Mogelijke) einddatum van de inbreuk	16-3-2026
4.2 Wanneer is het incident ontdekt?	16-3-2026
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Verkeerde ontvanger heeft beschikking teruggestuurd naar de gemeente.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd dat de persoonsgegevens vernietigd zijn, of zijn de persoonsgegevens teruggestuurd?	Ja

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Een beschikking met afwijzing aanvraag bijzondere bijstand is per ongeluk naar verkeerde inwoner verstuurd. Gaat om NAW-gegevens, geslacht en privacygevoelige inhoud. Verkeerde ontvanger heeft beschikking teruggestuurd naar de gemeente.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Contactgegevens

[✓] Adres en woonplaats

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Eén beschikking (brief)

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Inwoner van de gemeente Leeuwarden.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	stigmatisering

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	Er zijn alleen NAW-gegevens gelekt en de verkeerde ontvanger heeft beschikking teruggestuurd naar de gemeente. Wel gemeld vanwege de privacygevoelige inhoud van de beschikking (namelijk afwijzing aanvraag bijzondere bijstand).

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	1

Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	16-3-2026
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	De medewerker die het datalek bij Privacy heeft gemeld, heeft betrokkene telefonisch geïnformeerd over het datalek en excuses aangeboden.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Telefonisch

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Beschikking is alsnog naar juiste persoon verstuurd.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nee, want:
Toelichting:	Betrof een vergissing van een medewerker waarbij een eerder besluit is 'hergebruikt' voor een andere inwoner. Medewerker vond het zelf ook heel vervelend dat het was gebeurd, dus zij zal voortaan zeker beter opletten.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

AP bescherming in een digitale wereld

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: [redacted]

Melddatum: 15 juni 2026

Meldtijdstip: 10:48

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	[redacted]

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	[redacted]
Functie	Privacy Officer
E-mailadres	[redacted]@leeuwarden.nl
Telefoonnnummer	[redacted]
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	1
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	2-6-2026

Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Door middel van onze standaardbrief is de betrokkene geïnformeerd. In deze brief staat aangegeven wat er is gebeurd, wat de gevolgen zijn, welke maatregelen we hebben getroffen en contactgegevens van de FG.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per brief

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: [redacted]

Melddatum: 15 januari 2026

Meldtijdstip: 15:37

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	[redacted]

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	[redacted]
Functie	FG
E-mailadres	[redacted]@leeuwarden.nl
Telefoonnnummer	[redacted]
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

[✓] Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

[✓] Aantal personen die door de inbreuk zijn getroffen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Onbekend
(Mogelijke) startdatum van de inbreuk	13-11-2025

Wanneer heeft u het datalek voor het eerst aan de AP gemeld?	12-12-2025
4.2 Wanneer is het incident ontdekt?	10-12-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Via de politie is de melding binnen gekomen dat een mail naar een verkeerd mailadres is gestuurd vanuit het Zorg- en Veiligheidshuis Fryslan
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

7 Betrokkenen

7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	10

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Er is nog niet besloten of de betrokkenen wel of niet worden geïnformeerd. Ten eerste is nog niet

bekend om hoeveel betrokkenen het gaat en of er mogelijk zwaarwegende belangen zijn om de getroffen personen niet te informeren. Dit wordt	nog besproken vanuit het ZVHF en de overige betrokken partners.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nog niet bekend
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nog niet bekend

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk
Geef aan wanneer u (uiterlijk) een vervolgmelding doet	12-2-2026
Toelichting	Het onderzoek naar oorzaak en impact is nog altijd in onderzoek bij een externe informatiebeveiligingspartij. Dat is ook de reden dat de datalek melding nog niet definitief gemaakt kan worden.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 13 november 2025

Meldtijdstip: 09:04

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	4-11-2025
4.2 Wanneer is het incident ontdekt?	10-11-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	5.1.2e 5.1.2e die kopie dossier van 5.1.2e heeft ontvangen, heeft datalek gemeld.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Persoonsgegevens toegevoegd aan het verkeerde dossier

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Inwoners hebben een kopie van hun dossier van werk & inkomen opgevraagd. Dit is in drie e-mails (onbeveiligd) verstuurd. Hiertussen zat een document over loonbeslaglegging van een andere persoon. Ook waren namen van medewerkers niet geanonimiseerd en was hun eigen BSN zichtbaar. De 5.1.2e van de aanvragers heeft hun dossier ontvangen. Hij heeft het datalek ontdekt en gemeld. Onderzoek is nog gaande over hoe het document van een andere persoon in het verkeerde dossier terecht is gekomen. Verder is nog niet duidelijk of er meer namen van medewerkers geanonimiseerd hadden moeten worden. Het BSN is bekend bij

aanvragers maar in dit geval onbeveiligd gemaild (extra risico).

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Burgerservicenummer (BSN)

[✓] Financiële gegevens

[✓] Andere financiële gegevens

Namelijk:	loonbeslaglegging / derdenbeslag

[✓] Anders

Namelijk:	handtekening directeur bedrijf die brief voor rechtshandeling heeft ondertekend.

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	3
Geef een toelichting op bovengenoemd aantal:	Eén document (brief) over derdenbeslag, mogelijk namen van medewerkers, BSN van aanvragers.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Document derdenbeslag van klant (cliënt) werk & inkomen, aanvragers zijn klant (cliënt) werk & inkomen, mogelijk medewerkers gemeente Leeuwarden.
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	4
Het maximum aantal betrokkenen is:	10

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Mogelijk stigmatisering, hoewel in het document derdenbeslag alleen een naam staat.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	Persoon die datalek heeft ontdekt, heeft gemeente geïnformeerd. Hoewel het document over derdenbeslag gaat, staan er alleen enkele algemene gegevens in. Als de namen van medewerkers onvoldoende zijn geanonimiseerd gaat het alleen om algemene gegevens. T.a.v. BSN: documenten zijn onbeveiligd gemaild maar wel naar het juiste e-mailadres.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Aan vakafdeling geadviseerd om betrokkene wel te informeren. Uitsluitsel hierover nog ontvangen.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nee, want:
Toelichting:	Er vindt nog onderzoek plaats naar hoe het document in het verkeerde dossier is opgenomen en of er meer namen van medewerkers geanonimiseerd hadden moeten worden. Een nieuw (juist) geanonimiseerde kopie van het

dossier moet nog worden verzonden met het	verzoek het verkeerde dossier te vernietigen en dat te bevestigen.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Instructie over goed/beter opletten bij anonimiseren, dit soort documenten altijd beveiligd mailen (en wachtwoord via ander kanaal). Handleiding/instructie/factsheet opstellen over anonimiseren om alle medewerkers te informeren.

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	11-12-2025
Toelichting	-

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

AP bescherming in een digitale wereld

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2, 3
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 12 december 2025

Meldtijdstip: 09:35

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2i
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	FG
E-mailadres	FG@leeuwarden.nl
Telefoonnummer	5.1.2e
Tweede telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	27-11-2025
4.2 Wanneer is het incident ontdekt?	10-12-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De beoogd ontvangers hebben gemaild naar de afdeling dat zij nog altijd geen bevestiging van inschrijving en hun BSN niet hadden ontvangen. Toen is ontdekt dat de brieven naar een verkeerd adres gestuurd waren, omdat betrokkenen op een verkeerd adres waren ingeschreven. Daarop is direct een melding van het datalek opgemaakt.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd dat de persoonsgegevens vernietigd zijn, of zijn de persoonsgegevens teruggestuurd?	De verkeerde ontvanger heeft niet gereageerd

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	betrokkenen zijn bij burgerzaken op het verkeerde huisnummer ingeschreven, waardoor de bevestiging van de 1e vestiging en toekenning van hun BSN-nummer naar het verkeerder huisnummer zijn gestuurd. Dit betreft een vakantiewoning, waarvan de eigenaar nog niet gereageerd heeft op de ontvangst van de brieven.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Geboortedatum en/of leeftijd

[✓] Burgerservicenummer (BSN)

[✓] Contactgegevens

[✓] Adres en woonplaats

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	2
Geef een toelichting op bovengenoemd aantal:	het gaat om twee afzonderlijke brieven, met daarin persoonsgegevens van 2 personen

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	nieuwe inwoners van de gemeente vanuit het buitenland
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Het betreft 2 vestigingen vanuit het buitenland
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	2

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Identiteitsdiefstal of -fraude

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Hoewel er een aantal belangrijke persoonsgegevens in de bevestiging van inschrijving staan, gaat het om verzending

daarvan naar een vakantiewoning. Aangezien er momenteel nog geen contact is geweest met de eigenaar, lijkt het erop dat de brieven wel bezorgd	zijn, maar nog niet gevonden. Daarmee is het risico op misbruik minimaal.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	2
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	10-12-2025
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Er is aangegeven dat de inschrijving per abuis op het verkeerde huisnummer is gedaan, waardoor ook de bevestiging van inschrijving naar het verkeerde huisnummer is gestuurd. Er is aangegeven dat dit als datalek is beschouwd en dat deze gemeld wordt aan de AP. Contactgegevens van de medewerker van burgerzaken is bekend en ook de gegevens van de FG zijn doorgegeven. Er is aangegeven dat we via de eigenaar van de woning de brieven proberen te achterhalen en uitleg gegeven over het risico van de bezorging van de brieven op het verkeerde huisnummer.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Per e-mail

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nee, want:
Toelichting:	de eigenaar van de woning heeft nog niet gereageerd.

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	voorafgaand aan de definitieve registratie van de personen op het adres wordt de inschrijving samen met de betrokkene doorgelopen.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk
Geef aan wanneer u (uiterlijk) een vervolgmelding doet	12-1-2026
Toelichting	Omdat de brieven nog niet zijn achterhaald en dat mogelijk nog gaat lukken, wordt de melding naar aanleiding daarvan aangevuld.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 12 december 2025

Meldtijdstip: 15:47

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2i
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	FG
E-mailadres	FG@leeuwarden.nl
Telefoonnummer	5.1.2e
Tweede telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja

Geef aan welke andere organisaties betrokken waren bij de inbreuk?

Naam	Op welke wijze betrokken	Toelichting (optioneel)
Nog niet bekend, wordt aangevuld		

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	9-12-2025
4.2 Wanneer is het incident ontdekt?	10-12-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Via de politie is de melding binnen gekomen dat een mail naar een verkeerd mailadres is gestuurd vanuit het Zorg- en Veiligheidshuis Fryslan
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd?	Nee

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Er is een typefout gemaakt in het emailadres, waardoor de mail naar een heel andere partij is gestuurd. Dit maildomein is in bezit van een stichting, die de ontvangst van de mail gemeld heeft aan de politie.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

- [✓] Naam
- [✓] Geslacht
- [✓] Geboortedatum en/of leeftijd
- [✓] Burgerservicenummer (BSN)
- [✓] Contactgegevens
- [✓] Adres en woonplaats
- [✓] Anders

Namelijk:	Wordt nog onderzocht welke andere gegevens

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

- [✓] Gegevens over iemands gezondheid

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	2

Geef een toelichting op bovengenoemd aantal:

het gaat om een email met daarin informatie over mogelijk 2 betrokkenen

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Patiënten

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Het betreft informatie over personen die binnen de casuistiek van het Zorg- en Veiligheidshuis wordt besproken met verschillende partijen
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	3

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Ja, namelijk: versleuteld (encryptie)

Welke versleutelingstechniek heeft u toegepast (indien bekend)?	Nog onbekend
8.2 Als de persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt waren, om welk deel gaat dat dan?	Alle gegevens waren vooraf onbegrijpelijk of ontoegankelijk gemaakt

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Reputatieschade

[✓] Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	de gegevens zijn ontvangen door een stichting die een relatie lijkt te hebben met mishandeling. De ontvangst van de mail is gemeld aan de politie.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Het onderzoek naar de oorzaak en ontvangst van de mail door de derde partij wordt op dit moment nog onderzocht. Zodra daarover meer bekend is, zal besloten worden of informeren van de betrokkenen mogelijk is.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nog niet bekend
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nog niet bekend

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	12-1-2026
Toelichting	Er loopt nog een onderzoek naar de ontvangst van de foutief geadresseerde mail. Zodra daarover meer bekend is, zal deze melding worden aangevuld

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer [redacted]

Melddatum: 12 januari 2026

Meldtijdstip: 11:39

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	[redacted]

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	[redacted]
Functie	FG
E-mailadres	[redacted]@leeuwarden.nl
Telefoonnnummer	[redacted]
Tweede telefoonnummer	[redacted]
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Maatregelen om de inbreuk aan te pakken?

10 Vervolgacties naar aanleiding van de inbreuk

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Er is contact opgenomen met de eigenaar van de woning. Inmiddels is 1 van de brieven ongeopend retour gekomen, met daarop de vermelding dat er geen brievenbus was. De verwachting is dan ook, dat de andere brief ook retour afzender gaat

komen. Ofwel via PostNL, ofwel via de eigenaar van de woning.

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	voorafgaand aan de definitieve registratie van de personen op het adres wordt de inschrijving samen met de betrokkene doorgelopen.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 01 oktober 2025

Meldtijdstip: 09:34

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2i
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Functionaris Gegevensbescherming
E-mailadres	fg@leeuwarden.nl
Telefoonnummer	5.1.2e
Tweede telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	5-3-2020
(Mogelijke) einddatum van de inbreuk	30-9-2025
4.2 Wanneer is het incident ontdekt?	29-9-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	er is een melding gedaan door betrokkene dat zijn naam en van andere betrokkenen niet juist geanonimiseerd zijn gepubliceerd op internet.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Persoonsgegevens per ongeluk gepubliceerd

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	documenten zijn onjuist geanonimiseerd gepubliceerd. Daardoor zijn de gegevens bij kopiëren en plakken in een ander document zichtbaar te maken en opgenomen in de zoekresultaten van Google. Betrokkene kwam hierachter, doordat hij bij het invoeren van zijn

naam bij een zoekresultaat in Google zijn adresgegevens zag staan.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] E-mailadres

[✓] Telefoonnummer

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	9
Geef een toelichting op bovengenoemd aantal:	Bij doornemen van het bestand zijn gegevens van 9 personen in het document aangetroffen, variërend van naam en emailadres en naam en adres tot naam en telefoonnummer.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	inwoners

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	het betreft inwoners van gemeente Leeuwarden, welk gebruik hebben gemaakt van hun inspreekrecht.
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	9

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Ja, namelijk: op een andere manier onbegrijpelijk of ontoegankelijk gemaakt

Op welke manier waren de gegevens onbegrijpelijk of ontoegankelijk gemaakt (indien bekend)?	zwart weggelakt, maar niet correct weggelakt
8.2 Als de persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt waren, om welk deel gaat dat dan?	Alle gegevens waren vooraf onbegrijpelijk of ontoegankelijk gemaakt

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Reputatieschade

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt

Licht uw keuze toe:	Voor de meeste betrokkenen geldt, dat hun gegevens pas herkenbaar gemaakt kunnen worden, als deze worden gekopieerd vanuit Adobe naar een ander document. Voor 1 betrokkene geldt, dat zijn adres via het invoeren van zijn naam verscheen via de zoekresultaten van Google.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Ja
Aan hoeveel personen wilt u de inbreuk gaan melden?	9
Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?	1-10-2025
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Via een brief laten we de betrokkenen weten, dat hun gegevens niet correct geanonimiseerd op internet waren gepubliceerd. Daarbij geven we aan dat de gegevens alleen zichtbaar waren door te kopiëren naar een ander document. We geven aan dat het document inmiddels van internet is gehaald en correct wordt geanonimiseerd. De gegevens van de FG worden daarin opgenomen voor vragen of opmerkingen. De persoon wiens gegevens via de zoekmachine zichtbaar waren, is ook nog gebeld.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Telefonisch

[✓] Per brief

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	document is van internet verwijderd en wordt opnieuw geanonimiseerd. De zoekmachine geeft daardoor nu ook geen resultaten meer weer.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Er wordt niet meer gebruik gemaakt van deze manier van anonimiseren, maar een aparte anonimiseer-tool.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 31 juli 2025

Meldtijdstip: 09:27

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2i
KvK-nummer	59734817
Naam van het bedrijf of de organisatie	Gemeente Leeuwarden
Adres	Oldehoofsterkerkhof 2
Postcode	8911 DH
Plaats	Leeuwarden

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	Privacy Officer
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	1-1-2025
(Mogelijke) einddatum van de inbreuk	30-7-2025
4.2 Wanneer is het incident ontdekt?	25-7-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Medewerker (melder) is gebeld en heeft een mail ontvangen van een collega over het datalek.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Nee
Wanneer heeft u kennis gekregen van het datalek?	29-7-2025

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Overig

Namelijk:	Medewerker heeft persoonlijke Downloads map per ongeluk versleept naar een afdelingsschijf.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Een medewerker heeft per ongeluk de persoonlijke Downloads map versleept naar de afdelingsschijf. Hierdoor hadden circa 300 medewerkers toegang tot de bestanden. Het is niet te herleiden wanneer de map is versleept en in hoeverre medewerkers bestanden hebben

geopend. In de map staan ook vertrouwelijke documenten met persoonsgegevens. Het is niet exact duidelijk om welke persoonsgegevens het gaat. Een ISO heeft contact gehad met een TISO en de ICT-afdeling. Zij hebben de map direct	ontoegankelijk gemaakt. De medewerker die de map per ongeluk verplaatst heeft, heeft momenteel vakantie. Toegang tot de map is voor deze persoon dus op dit moment niet noodzakelijk.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Geboortedatum en/of leeftijd

[✓] Burgerservicenummer (BSN)

[✓] Contactgegevens

[✓] Adres en woonplaats

[✓] E-mailadres

[✓] Telefoonnummer

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

[✓] Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt

[✓] Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt

[✓] Gegevens over iemands gezondheid

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	145
Geef een toelichting op bovengenoemd aantal:	Er staan 145 bestanden in de map.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Klanten (huidig en potentieel)

[✓] Anders

Namelijk:	Sollicitanten
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	In de map staan allerlei bestanden, deze kunnen gaan over medewerkers, klanten (inwoners/burgers) en in ieder geval ook sollicitanten. Dit laatste blijkt uit de bestandsnaam van diverse bestanden.
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	145

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Misschien stigmatisering i.v.m. inzage in gegevens over collega's en sollicitanten.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	Medewerkers zijn betrouwbare ontvangers, zij hebben allen de eed of gelofte afgelegd en een integriteitsverklaring ondertekend. Niettemin wel gemeld omdat het in ieder geval om vertrouwelijke persoonsgegevens gaat.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nee

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Medewerkers zijn betrouwbare ontvangers. Risico op misbruik van persoonsgegevens is minimaal/vrijwel uitgesloten.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Na melding en onderzoek is de map direct ontoegankelijk gemaakt.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	In overleg met ICT, TISO's en ISO's wordt bekeken of het mogelijk is het per ongeluk verslepen van een dergelijke persoonlijke map naar een afdelingsschijf te voorkomen.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.2i

Melddatum: 19 juni 2025

Meldtijdstip: 14:56

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	5.1.2i

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	5.1.2e
Functie	FG
E-mailadres	5.1.2e @leeuwarden.nl
Telefoonnnummer	5.1.2e
Tweede telefoonnummer	5.1.2e
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

[✓] Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

[✓] Welke persoonsgegevens

7. Getroffen personen

[✓] Aantal personen die door de inbreuk zijn getroffen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja

(Mogelijke) startdatum van de inbreuk	1-1-2020
Wanneer heeft u het datalek voor het eerst aan de AP gemeld?	22-5-2025
4.2 Wanneer is het incident ontdekt?	22-5-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Via een brief van Geonovum, waarin wordt aangegeven dat er mogelijk persoonsgegevens in de metadata staat van gepubliceerde documenten. Daarop zijn we gaan controleren op de publicatiewebsite en werden documenten gevonden die niet geanonimiseerd gepubliceerd zijn
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

6 Betrokken persoonsgegevens

6.1 Persoonsgegevens in het algemeen

- [✓] Naam
- [✓] Geslacht
- [✓] Contactgegevens
- [✓] E-mailadres
- [✓] Anders

Namelijk:	handtekening van ondertekenende ambtenaren bij besluiten

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

7 Betrokkenen

7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	10
Het maximum aantal betrokkenen is:	100

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	10
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	23-5-2025
Licht toe aan welke (groep) betrokkenen u de inbreuk heeft gemeld:	Intern is iedereen op de hoogte gesteld, dus alle collega's zijn op de hoogte. Externe betrokkenen hebben we niet geinformeerd, omdat dit alleen de naam van contactpersonen van organisaties betreft.
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	We hebben de situatie uitgelegd en wat de mogelijke risico's zijn. contactgegevens van de FG zijn gedeeld.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Telefonisch

[✓] Per e-mail

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Ik heb na de inbreuk maatregelen genomen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkene(n)

Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?	Het merendeel van de documenten (vanaf 2024, welke het grootste mogelijke risico zouden kunnen vormen) zijn inmiddels verwijderd en alsnog geanonimiseerd terug geplaatst. Een klein deel van de documenten is nog niet geanonimiseerd, doordat dit andere bestandstypen zijn, die niet direct door de anonimiseringssoftware kan worden herkend. Dit is voorgelegd aan de leverancier.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	de documenten zijn (en worden voor een deel) verwijderd, geanonimiseerd en weer terug geplaatst.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Alle medewerkers betrokken bij het publiceren van dergelijke dossiers, zijn hierover geïnformeerd en hebben instructie ontvangen over het anonimiseren van de documenten.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP


AP
bescherming in een
digitale wereld

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Gemeente Leeuwarden

JAARVERSLAG GEGEVENSBESCHERMING GEMEENTE LEEUWARDEN 2025



Functionaris
Gegevensbescherming
maart 2026

Gemeente Leeuwarden

Inhoudsopgave

INHOUDSOPGAVE **2**

INLEIDING **4**

LEESWIJZER **4**

FG JAARRAPPORTAGE 2025 ..... **5**

DEEL 1. TERUGBLIK OP 2025 ..... **6**

BELEID 7
PROCESSEN 7
ORGANISATIE 7
RECHTEN VAN BETROKKENE 8
SAMENWERKING 8
BEVEILIGING 8
VERANTWOORDING 9
WPG 10
OVERIG 10

DEEL 2. VOORUITKIJKEN NAAR 2026 ..... **11**

BIJLAGE 1 - STAND VAN ZAKEN AVG PER ONDERWERP **14**

BIJLAGE 2 - OVERZICHT HERZIENING EN NIEUWE DEPIA'S **15**

BIJLAGE 3 - OVERZICHT RECHTEN VAN BETROKKENEN **17**

BIJLAGE 4 - OVERZICHT DATALEKKEN **17**

BIJLAGE 5 – RESULTATEN EXTERNE AUDIT WPG **18**

Samenvatting

Als onafhankelijk toezichthouder van de gemeente constateert de Functionaris Gegevensbescherming (FG) dat de gemeente Leeuwarden in 2025 vorderingen heeft gemaakt wanneer het gaat om het voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg). Hieronder volgt een korte samenvatting van wat in de rest van het verslag verder wordt uitgewerkt.

Wat de gemeente in 2025 heeft bereikt:

- Naar aanleiding van de geconstateerde achterstanden bij de afronding van de Data en Data-ethische Protectie Impact Assessments (DEPIA's) is er extra financiële ruimte gecreëerd voor de inzet van een tijdelijke privacy officer die de organisatie zou gaan helpen bij het wegwerken van de achterstanden. Deze tijdelijke ondersteuning is aangetrokken, maar heeft de organisatie inmiddels weer verlaten.
- De privacy verklaring is herzien en opgesteld in B1. Naar aanleiding hiervan is ook informatie over AVG en privacy op de website van de gemeente geactualiseerd en aangevuld.
- Na de in werkingtreding van de Wet Gegevensdeling door Samenwerkingsverbanden (Wgs) is de FG van gemeente Leeuwarden aangewezen als de FG met coördinerende taken voor alle samenwerkende partners binnen het RIEC NN en ZVHF.
- Eveneens naar aanleiding van de Wgs is een contactpunt opgericht voor zowel het RIEC NN als voor het ZVHF. Dit contactpunt is weliswaar gemandateerd aan resp. RIEC NN en ZVHF, maar taken als inrichten van de website en opstellen van processen en procedures is mede door de privacy officers van gemeente Leeuwarden uitgevoerd.

Acties die in 2025 zijn gestart en in 2026 voortlopen:

- In afstemming met het Collectief Management Team (CMT) is een kaderdocument opgesteld, welke een vooruitlopend onderdeel is van een later op te stellen algemene directielijn. In dit kaderdocument zijn de taken, rollen en verantwoordelijkheden opgenomen die betrokken zijn bij gegevensbescherming.
- Naar aanleiding van dit kaderdocument gaat de FG in gesprek met de leidinggevenden, om hen meer te betrekken bij de verschillende verplichte vereisten vanuit de AVG en Wpg, waardoor werk-processen beter aan gaan sluiten op de verschillende privacy wetgevingen.
- Er is een start gemaakt met het herzien van het register van verwerkingen. Dit wordt verder uitgewerkt in 2026.
- Het inventariseren en beoordelen van samenwerkingsverbanden: deze opnemen in het verwerkingsregister en daarbij onder andere vastleggen welke gegevens worden verwerkt en op basis van welke grondslag.
- De externe Wpg audit is in 2025 uitgevoerd. De bevindingen daaruit hebben geleid tot het aantrekken van extra ondersteuning bij de domeinen van Handhaving, Leerplicht en Sociale Recherche. De heraudit wordt in 2026 uitgevoerd, waarbij de verwachting is, dat deze goede resultaten gaat opleveren.
- Verder werken aan het afronden van de werkvoorraad aan DEPIA's. Hiervoor is aandacht en zeker tijd nodig vanuit de verschillende sectoren, onder wiens verantwoordelijkheid de afronding valt. Het afgelopen jaar is geconstateerd dat de inzet daarvoor te weinig is geweest om een verschil te maken.

Inleiding

Met het jaarverslag van de Functionaris Gegevensbescherming (FG) van gemeente Leeuwarden wordt beoogd verantwoording af te leggen van de taak van de FG zoals vastgelegd in de AVG (art. 39 AVG en art. 36 Wpg) en daarmee een beeld te scheppen over waar de gemeente staat wanneer het gaat om het verwerken van persoonsgegevens conform de verschillende privacywetten zoals de AVG, UAVG en de Wpg.

De belangrijkste taak van de FG is dat deze onafhankelijk toezicht en controle houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming en de Wet politiegegevens door de gemeente als organisatie.

Dit jaarverslag gaat in op het algemene beeld van de compliance ten aanzien van de AVG, de bevindingen over het jaar 2025 en de aandachtspunten voor 2026. Dit verslag wordt jaarlijks opgesteld en aangeboden aan het college van Burgermeester en wethouders omdat zij eindverantwoordelijk is voor de verwerking van persoonsgegevens. Daarna kan het college via een informerende brief de gemeenteraad informeren en deze publiceren op de website van de gemeente. Het jaarverslag wordt ook aangeboden aan de Gemeentesecretaris en aan de Directie, aangezien zij inhoudelijk verantwoordelijk zijn voor de verwerking van persoonsgegevens binnen de gemeentelijke organisatie.

Leeswijzer

Dit verslag bestaat uit twee onderdelen. In het eerste deel wordt teruggekeken naar 2025. Wat heeft de gemeente bereikt op het gebied van gegevensbescherming? Welke maatregelen zijn genomen om te voldoen aan de privacywetgeving?
In het tweede deel staan aanbevelingen om gegevensbescherming vanaf 2026 naar een hoger niveau te tillen.

De algehele AVG-compliance wordt gemeten aan het hand van onderstaande thema's uit het AVG borgingsproduct 3.0 van de VNG:[1] Hierbij wordt (nog) geen onderscheid gemaakt tussen de verschillende sectoren binnen de gemeente.

- Beleid
- Processen
- Organisatie
- Rechten van betrokkene
- Samenwerking
- Gegevensbescherming
- Verantwoording

Het borgingsproduct bevat thema's, criteria en maatregelen die de AVG vertalen naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen. In bijlage 1 staat per thema aangegeven in hoeverre de gemeente in algemene zin de criteria heeft geïmplementeerd.

Daarnaast is een apart deel gewijd aan de Wet Politiegegevens (Wpg) en bevat bijlage 5 de resultaten van de externe audit die in juli 2025 is uitgevoerd voor de Wpg-domeinen I (Handhaving Openbare Orde en Veiligheid), III (Leerplicht) en V (Sociale Recherche).

[1] Zie het document 'Criteria borging AVG / Borgingsproduct gegevensbescherming in de gemeentelijke organisatie', link.

Gemeente Leeuwarden

FG Jaarrapportage 2025
Totaaloverzicht van de kaders



	2024 Resultaten	2025 Resultaten
Beleid		
Processen		
Organisatie		
Betrokkene		
Samenwerking		
Gegevensbescherr		
Verantwoording		
Wpg		

Deel 1. Terugblik op 2025

In 2025 zijn twee wetten in werking getreden, welke de nodige inspanningen hebben gekost:

- Op 1 maart 2025 is de Wet gegevensverwerking door samenwerkingsverbanden (Wgs) en het daarop gebaseerde Besluit gegevensverwerking door samenwerkingsverbanden (Bgs) in werking getreden. De Wgs en de Bgs bieden een wettelijke kader voor de verwerking van persoonsgegevens door de regionale samenwerkingsverbanden RIEC NN en ZVHF.

Gemeente Leeuwarden is hier op verschillende manieren bij betrokken:

- Als zelfstandige deelnemer in de samenwerkingsverbanden RIEC NN en ZVHF. Dit geldt zowel voor de burgemeester als het college.
- Als Wgs-contactpunt voor de naleving van de verplichtingen door alle deelnemers aan deze samenwerkingsverbanden. Deze verplichtingen bestaan uit het behandelen van AVG-verzoeken en datalekken en het voldoen aan de informatieverplichtingen namens alle deelnemers aan RIEC NN en ZVHF.
- De FG van gemeente Leeuwarden is aangewezen voor het uitvoeren van de coördinerende FG-taken. Deze taken bestaan uit het coördineren van het toezicht door de FG's van de gezamenlijk verwerkingsverantwoordelijke deelnemers aan het samenwerkingsverband.

Om de werkzaamheden die voortvloeien uit de Wgs en de Bgs uit te voeren, is in april 2025 een kwartiermaker ingehuurd voor deze cFG-taken. De kosten hiervoor zijn vanuit RIEC NN en ZVHF vergoed. De kwartiermaker heeft in 2025 deze uren gebruikt om de samenwerking te bevorderen tussen RIEC NN en de FG's van de deelnemers van RIEC NN.

RIEC NN heeft voor deze FG's een informatiepositie gebouwd, informatiebijeenkomsten georganiseerd en een communicatiekanaal ingericht. Er is nog geen overlegstructuur ingericht voor de FG's binnen het ZVHF. Het informeren van deze FG's loopt vooralsnog via de informatieverstrekking aan de RIEC-FG's.

Om de informatievoorziening vanuit RIEC NN en ZVHF richting FG's te optimaliseren, verdient het aanbeveling een regionaal online samenwerkingsplatform, zoals Pleio, in te richten bij het contactpunt in Leeuwarden. Deze Pleio-omgeving kan worden gebruikt voor de informatievoorziening vanuit RIEC NN en ZVHF. Daarnaast kan er een afgeschermde ruimte komen voor de onderlinge communicatie tussen de RIEC-FG's en de ZVHF-FG's. Dat laatste is noodzakelijk om het toezicht van deze FG's te coördineren.

Voor 2026 is voorzien dat de FG-werkzaamheden die voortvloeien uit de Wgs en de Bgs een extra investering in FG-uren vergen. Het verdient aanbeveling hiervoor een structurele oplossing te vinden.

- Per 1 juli 2025 is de **Wet Persoonsgerichte Aanpak Radicalisering en Terroristische Activiteiten (PARTA)** in werking getreden. Daarmee vervangt deze wet de persoonsgerichte aanpak radicalisering, die is gebaseerd op het modelconvenant. Deze wet vraagt nog wel de nodige uitwerking rondom de casusbesprekingen en eventuele verzoeken van betrokkenen.

- Ook is in 2025 de **AI Act (AIA)** meer van invloed; zo is vanaf 2 februari 2025 een aantal bepalingen op verboden AI in werking getreden en zijn vanaf 2 augustus 2025 eisen voor AI-modellen voor algemene doeleinden (*general purpose AI*) in werking getreden. Voor 2026 en verder gelden nadere uitbreidingen voor de AIA.

Verder stond 2025 in het teken van het verder verstevigen van de basis, verbeteringen en werken aan de komende ontwikkelingen. Dit deel van het verslag geeft een terugblik op wat gemeente Leeuwarden in 2025 heeft bereikt. In algemene zin valt op, dat de scores op groen staan, met uitzondering van het resultaat voor de Wpg. Op onderdelen is dan ook de nodige extra inzet gepleegd, wat direct terug te zien is in de scores van het Borgingsproduct. Daar mag de organisatie dan ook met tevredenheid op terugzien!



Beleid

Het privacybeleid is een kader waarin gemeente Leeuwarden aangeeft aan welke principes zij zich houdt bij het verwerken van persoonsgegevens. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving.

De gemiddelde score op Beleid in het borgingsproduct is 83%, 19% hoger dan in 2024. Dit heeft vooral te maken met het bespreken van het kaderdocument rondom gegevensbescherming in het Collectief Management Team (CMT). De uiteenzetting van de taken, rollen en verantwoordelijkheden op het gebied van privacy heeft het gevoel van eigenaarschap bij privacy wel duidelijk gemaakt. Doel voor 2026 is om de verschillende sectoren te onderzoeken op compliance aan het privacybeleid.



Processen

Het verwerken van persoonsgegevens van gemeente Leeuwarden moet voldoen aan de AVG. Dit houdt in dat de gemeente de werkprocessen, waarbinnen met persoonsgegevens wordt gewerkt, moet inrichten volgens de beginselen vanuit de AVG: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast is de gemeente bij risicovolle verwerkingen verplicht om een DEPIA[2] uit te voeren.

In 2024 was de achterstand op de uitvoering van de DEPIA's dermate groot, dat er besloten is om er extra inhuur in te zetten. Helaas heeft de inzet van de inhuur niet aan de verwachtingen voldaan en wordt op dit moment de data-ethiek officer hierop ingezet. Toch laat de inzet verbetering zien; hoewel het aantal afgeronde DEPIA's weinig is toegenomen, is het proces aangepast, waardoor de doorlooptijd verkort wordt. De echte inhaalslag wordt dan ook vanaf 2026 verwacht, op voorwaarde dat er vanuit de teams ook de nodige tijd en aandacht aan wordt gegeven.

De totale score op dit onderdeel is hoger uitgekomen; 78%, waar dat in 2024 71% was. De uitvoering van de pre-DEPIA, de DEPIA's en het bijwerken van het register van verwerkingen zijn onderdelen die scherp in de gaten gehouden moeten worden.



Organisatie

Voor een goede en juiste uitvoering is het van belang dat iedereen binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van privacy. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren.

De score op Organisatie is 84%. Door de verantwoordelijkheden vast te leggen, ontstaat nog meer eigenaarschap. Hiermee wordt gegevensbescherming een vast onderdeel van het werk. Vanaf 2026 wordt een leerlijn voor leidinggevenden ingezet op het gebied van privacy. Het bewustzijnsprogramma is daarmee, naast ARDA en de AVG in Vogelvlucht, compleet.

Punt van aandacht is, dat de deelname aan de geboden leerlijnen voldoende moet zijn. De mens is de zwakste schakel als het gaat om het voorkomen van datalekken. De deelname aan bijvoorbeeld ARDA zal onderwerp van gesprek moeten zijn met het management en vervolgens met de eigen medewerkers. Daarnaast zal de organisatie moeten bepalen wat het gewenste resultaat is in de deelnamegraad. Deelname aan de elearning kan ook iets zeggen over houding en gedrag van het personeel.

[2] DEPIA is een Data en Data-Ethische Protectie Impact Assessment: een onderzoek om de privacy risico's én ethische dilemma's van gegevensverwerkingen in kaart te brengen. En de maatregelen om deze risico's en dilemma's weg te nemen of te verkleinen.

Ook is er een lage score op het deel “privacyteam”; dat komt omdat daarin wordt gevraagd om een functionaris die verantwoordelijk is voor het tijdig inschatten van de gevolgen voor de organisatie van ontwikkelingen op het gebied van privacywetgeving en jurisprudentie. Dit is nog niet concreet belegd.



Rechten van betrokkene

Gemeente Leeuwarden informeert degene waarover zij de persoonsgegevens verwerkt (de betrokkene) zowel actief als passief over het verwerken, de grondslag en de maatregelen tegen onrechtmatige toegang en verwerking. Daarnaast faciliteert de gemeente de betrokkenen in het uitoefenen van hun rechten op bijvoorbeeld inzage, correctie en verwijderen van hun persoonsgegevens. De score op Rechten van betrokkene is 94%. Net als in 2024 is dat een uitstekend resultaat.

In bijlage 3 is een overzicht opgenomen van het aantal verzoeken van betrokkenen in 2025.



Samenwerking

Gemeente Leeuwarden werkt op meerdere beleidsterreinen, in diverse rollen en hoedanigheden samen met (mede) overheden en private organisaties. Vaak is er sprake van het verwerken van persoonsgegevens tussen partijen: ontvangen, verzenden, maar ook het opslaan en raadplegen van persoonsgegevens valt hieronder. De gemeente moet dan ook afspraken vastleggen hierover met deze andere partijen.

De score op Samenwerking in het toetsingsproduct is van 82% naar 97% gegaan. Dat heeft vooral te maken met de toename in gestructureerde aandacht voor de opslag en actualiteit van de verschillende overeenkomsten. Hierdoor is het overzicht verbeterd en kan er beter toezicht gehouden worden.

Voor het komende jaar wil de FG de samenwerkingsverbanden inzichtelijk krijgen, deze op laten nemen in het verwerkingsregister en dat deze periodiek worden geëvalueerd en waar nodig herzien. Samenwerkingen veranderen in de loop van de tijd, gegevensuitwisselingen veranderen, soms op basis van behoefte, soms op basis van veranderende wet- en regelgeving.



Beveiliging

Vanuit het algemene behoorlijkheids-, het integriteits- en het vertrouwelijkheidsbeginsel is het essentieel dat gemeente Leeuwarden passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er een meldplicht datalekken. Dit houdt in dat de gemeente incidenten op het gebied van informatieveiligheid onder bepaalde omstandigheden moet melden aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).

In 2025 is verdere invulling gegeven aan het BIO-normenkader (Baseline Informatiebeveiliging Overheid). Met name op beleidsmatig vlak is aandacht besteed aan het opstellen en actualiseren van diverse beleidsdocumenten, waaronder het cryptografiebeleid, het back-up- en restorebeleid en het Suwinetbeveiligingsbeleid. Momenteel scoort gemeente Leeuwarden op alle onderdelen in de BIO een voldoende.

Daarnaast is in 2025 een TPM-verklaring (Third Party Memorandum) afgegeven voor de SSC-werkplek. Hierbij zijn de BIO-normen, welke behoren bij de SSC-werkplek, getoetst op Opzet, Bestaan maar ook de Werking. Deze TPM-verklaring wordt inmiddels door samenwerkingspartners gebruikt voor hun ENSIA-verantwoording binnen het BIO-normenkader. Tevens wordt de TPM-verklaring door de accountants van deze partners benut om de mate van volwassenheid van de informatiebeveiliging van de SSC-werkplek te toetsen.

De ICT-omgeving is in 2025 door een externe partij onderzocht, waarbij zowel de vanaf het internet bereikbare systemen als de interne systemen zijn gecontroleerd op kwetsbaarheden.
Ook is aandacht besteed aan het vergroten van het informatiebeveiligingsbewustzijn. Dit is onder meer gedaan door het uitvoeren van phishingcampagnes, de inzet van een mystery guest en verlenging van het contract met ARDA (E-learning).

Wat datalekken betreft, zijn alle gemelde incidenten op de juiste manier behandeld en afgehandeld. In een aantal situaties heeft een datalek ertoe geleid, dat werkprocessen zijn herbeoordeeld en aangepast. Het aantal datalekken is gedaald ten opzichte van 2024. Dat kan een positief resultaat zijn, maar kan dat evengoed niet zijn, gezien de grootte van de organisatie en de hoeveelheden persoonsgegevens die worden verwerkt via de verschillende applicaties.

Er is in ieder geval te merken, dat de impact van datalekken groter wordt; de ransomeware aanval bij Omrin waarbij niet alleen alle gegevens van personeelsleden van Omrin waren betrokken, maar ook een bestand van gemeente Schiermonnikoog, is daar een goed voorbeeld van.

Ook publicatie van documenten die niet juist of niet volledig zijn geanonimiseerd, hebben veel impact en kennen soms een lange periode van oplossen; vaak is de hulp van zoekmachines als Google nodig om gegevens definitief te laten verwijderen van het internet. Dat maakt dan ook, dat voortdurend aandacht voor het voorkomen van datalekken nodig blijft.

In bijlage 4 is een overzicht opgenomen van het aantal datalekken in 2025, afgezet tegen het aantal datalekken in 2024.



Verantwoording

De gemeente zelf is verantwoordelijk voor het aantonen dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht, levert gemeente Leeuwarden een belangrijke bijdrage aan de bescherming van betrokkenen op het gebied van privacy. Dit betekent dat het college van B&W, de burgemeester en de gemeenteraad moeten kunnen aantonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en aan de relevante andere wet- en regelgeving.

De werkzaamheden die worden verricht op het vlak van privacy worden gedocumenteerd. Denk aan de wekelijkse werkoverleggen en de verzoeken en meldingen van collega's die via Topdesk worden afgehandeld. Daarnaast heeft de FG periodieke overleggen met de Gemeentesecretaris en de portefeuille houdende wethouder. Deze overleggen zijn ingepland per kwartaal en worden tevens spontaan belegd waar nodig.

De score op Verantwoording in het toetsingsproduct is 86%; een lichte stijging ten opzichte van de score van 82 % in 2024. De stijging heeft te maken met het toezicht plan dat is opgesteld en waarmee de FG aan de slag is gegaan. Het laatste onderdeel van dit punt heeft te maken met de periodieke controle die onder aansturing van het management moet worden gedaan. Door dit in brede zin te koppelen aan al bestaande controles, voldoet gemeente Leeuwarden aan de verantwoordingsplicht.

Wpg



Op grond van artikel 36 van de Wet politiegegevens (Wpg) houdt de Functionaris Gegevensbescherming toezicht op de naleving van de Wpg. Gemeenten (en andere werkgevers) die buitengewoon opsporingsambtenaren (boa's) in dienst hebben en gegevens verwerken op grond van de Wpg, zijn op grond van deze wet verplicht om jaarlijks een interne audit uit te voeren. De Wpg is binnen gemeente Leeuwarden van toepassing op de strafrechtelijke handhaving in het kader van:

1) openbare ruimte	2) onderwijs	3) werk, inkomen en zorg

Eens in de vier jaar moet daarnaast een externe audit worden uitgevoegd. In 2022 is deze externe audit uitgevoerd en de rapportage daarvan is ingediend bij de Autoriteit Persoonsgegevens. In februari 2024 is een externe hercontrole uitgevoerd op de punten uit de rapportage van 2022 waarbij de gemeente nog niet geheel aan de criteria van de Wpg voldeed of waar nog verbeteringen mogelijk waren. Deze rapportage is aangeboden aan de Autoriteit Persoonsgegevens (AP).

In 2025 is een externe audit uitgevoerd, welke wederom een afkeurend oordeel kreeg. Hieruit zijn dan ook de nodige actiepunten voortgekomen. De noodzaak voor het aanpakken van deze bevindingen is gevoeld bij de betreffende afdelingen; naast eigen inzet is er een extern bureau aangetrokken om hen te ondersteunen bij het uitvoeren van het verbeterplan.

De resultaten van deze externe audit moeten gedeeld worden met de AP. Dit is begin februari 2026 uitgevoerd. De AP heeft daarop ook het verbeterplan opgevraagd, zodat bij de heraudit kan worden gecontroleerd in hoeverre de uitvoering van het verbeterplan tot een uiteindelijke verbetering heeft geleid. Dit geeft aan, dat de AP verscherpte aandacht heeft voor de uitkomsten van de Wpg audit.

Vanaf medio 2025 is besloten om voor domein 3, (werk, inkomen en zorg) alleen nog toezicht uit te voeren op grond van de Awb. Daarmee zal voor de komende audits dit domein niet langer meegenomen worden.

In bijlage 5 zijn de resultaten per domein opgenomen van de externe Wpg audit van 2025.

Overig

De FG heeft ook in 2025 adviezen gegeven aan de organisatie ten aanzien van onderwerpen die aandacht vroegen of waarbij twijfels waren over de juiste aanpak met aandacht voor het verantwoord omgaan met persoonsgegevens. Een aantal voorbeelden daarvan:

- Mag het dashboard vanuit AFAS informatie op persoonsniveau geven aan alle leidinggevenden?
- Mag er een Teamsomgeving worden ingericht voor het delen van (persoons)gegevens tussen verschillende gemeentelijke onderdelen en organisaties?
- Mogen gegevens intern worden gedeeld, welke vallen onder belastingwetgeving?

De FG heeft dit jaar deelgenomen aan periodieke overleggen met de privacy officers, de data-ethisch officer, de CISO, record manager, de regionale experttafel en het regionale FG-overleg. Verder heeft er afstemming plaatsgevonden met externe partijen zoals FG's/PO's van andere gemeenten of van samenwerkingspartners.

De FG heeft daarnaast deelgenomen aan diverse (digitale) bijeenkomsten van VNG/IBD zoals bijeenkomsten rondom de Wams (Wet aanpak meervoudige problematiek sociaal domein), kennissessies over de Wpg en de Wgs (wet gegevensdeling samenwerkingsverbanden.

Ten aanzien van kennisbevordering heeft de FG deelgenomen aan diverse (bij-)scholingsactiviteiten en cursussen.

Deel 2. Vooruitkijken naar 2026

Op basis van de bevindingen over 2025 doet de FG de hieronder beschreven aanbevelingen. De aanbevelingen zijn ‘risico gebaseerd’. Deze worden aangevuld met ontwikkelingen op het gebied van digitalisering en wetgeving, waar dit jaar aandacht aan gegeven moet worden.

Aanbevelingen

- **Aandacht blijven houden voor de uitvoering van de DEPIA’s**

Ten aanzien van het uitvoeren van DEPIA’s is er afgelopen jaar licht vooruitgang geboekt, mede door de extra inzet vanuit de privacy officers en de data-ethiek officer. Maar dit is nog steeds slechts het begin. Er zijn veel DEPIA’s gestart, maar sommige processen lopen erg lang en is de voortgang soms traag. Daarnaast is het nog niet volledig transparant voor welke processen een DEPIA verplicht is (hier moet nog een scan voor worden uitgevoerd op alle processen die zijn opgenomen in het verwerkingsregister).

Aangezien veel processen en gebruikte systemen bij gegevens verwerkingen in veel gemeenten identiek zijn, kan hiervoor de samenwerking gezocht worden met andere gemeenten of gebruik te maken van de DEPIA-bibliotheek van de IBD/VNG.

Verder adviseert de FG om de uitvoering van DEPIA’s op te nemen in de jaarlijkse werkzaamheden van de verschillende teams.

- **Aandacht blijven houden voor privacy onder medewerkers**

De mens is de belangrijkste schakel in het vertrouwelijk houden van persoonsgegevens en voorkomen van datalekken. Het creëren van meer bewustwording zal sterk bijdragen aan een informatieveilig werken. Een van de manieren waarop dit vormgegeven wordt is via de e-learning ARDA. Maar daarvoor is wel een hogere deelname-graad nodig. Aandacht daarvoor vanuit leidinggevenden is cruciaal hierin.

Maar er is meer nodig. Medewerkers hebben, afhankelijk van hun functie, ook kennis nodig over specifieke onderwerpen zoals wanneer een verwerkersovereenkomst nodig is of wanneer informatie wel of niet gedeeld mag worden. Dit zal niet alleen helpen bij de uitvoering van DEPIA’s, het actueel houden van het verwerkingsregister en het (tijdig) melden van datalekken, maar vooral ook bij het zo veel mogelijk veilig en privacy bewust werken.

Daarnaast maakt de gemeente ook meer en meer gebruik van Algoritmen en AI. Ook hierbij spelen AVG en privacy een rol, met name wanneer bij de inzet daarvan persoonsgegevens worden gebruikt en vooral wanneer de uitkomsten van deze AI-tools gevolgen voor individuele betrokkenen kunnen hebben.

Medewerkers hebben hierbij ook meer kennis nodig om op basis daarvan ook meer risicobewustzijn te ontwikkelen en te weten wanneer bij het gebruik van Algoritmes extra onderzoek nodig is naar risico's. En of er naast de DEPIA nog een ander onderzoek nodig is: de IAMA ofwel 'Impact Assessment Mensenrechten en Algoritmes'. De FG beveelt aan om na te gaan hoe het proces van de IAMA gecombineerd kan worden met die van de DEPIA.

- **Aandacht hebben voor het Algoritmeregister**

Hoewel het register nog niet verplicht is, zal dat niet zo lang meer duren. Gemeente Leeuwarden is aangesloten op het landelijk format van het algoritmeregister, maar het register is niet volledig gevuld en daarmee niet actueel. Het probleem ligt hierbij in het eigenaarschap. Niemand is of voelt zich verantwoordelijk voor dit register. Het is zaak dit zo snel als mogelijk toe te wijzen en actie hierop in te zetten. Zeker nu er diverse ontwikkelingen zijn op het gebied van digitalisering en AI.

Ontwikkelingen op het gebied van digitalisering en wetgeving

Voor het komende jaar zijn er ontwikkelingen die gegevensbescherming raken en daarmee de nodige aandacht vragen. Het algoritmeregister, de AI Act en de daarmee samenhangende digitale weerbaarheid en tenslotte de Wet gegevensdeling door samenwerkingsverbanden zijn daar voorbeelden van. Ook de AP noemt een aantal van deze zaken in haar jaarplan. Het is goed om een aantal van deze punten mee te nemen in het eigen jaarplan.

Jaarplan AP:

De AP heeft haar jaarplan voor 2026 gepubliceerd, waarin drie thema's centraal: massasurveillance, AI en digitale weerbaarheid:

1. **Massasurveillance: inclusief tracking**

De AP kijkt bij massasurveillance niet alleen naar cameratoezicht of opsporingspraktijken, maar ook naar de manier waarop mensen online gevolgd worden. Tracking en cookies worden daarbij ook geplaatst onder het bredere begrip surveillance.

2. **AI: regels moeten vooraf duidelijk zijn**

De AP ziet dat AI zich razendsnel ontwikkelt en steeds vaker invloed heeft op beslissingen die mensen direct raken. Denk aan selectie, beoordeling, risicoprofilering of geautomatiseerde dienstverlening. Dat brengt reële risico's mee, zoals discriminatie, desinformatie en verlies van menselijke autonomie. Ingrijpen achteraf bij AI-systemen is vaak moeilijk of zelfs onmogelijk. Zodra systemen eenmaal draaien en persoonsgegevens zijn verwerkt, zijn fouten en ongewenste effecten niet eenvoudig terug te draaien.

Duidelijke kaders vooraf zijn effectiever dan correcties achteraf. Transparantie, uitlegbaarheid en het voorkomen van structurele bias, ofwel vooringenomenheid of vooroordeel, worden daarbij steeds belangrijker. Deze preventieve insteek sluit aan bij de Europese AI-wetgeving, waarin risicogericht toezicht en waarborgen aan de voorkant centraal staan. AI-governance is dan ook geen toekomstvraag meer. Wanneer AI wordt ingezet in processen waar persoonsgegevens een rol spelen, moet vooraf nagedacht worden over controle, verantwoording en waarborgen, voordat toezicht, klachten of maatschappelijke discussie volgen.

3. **Digitale weerbaarheid: grip op digitale afhankelijkheden**

Burgers en organisaties worden steeds afhankelijker van digitale diensten en infrastructuren, juist ook bij essentiële publieke processen. Die afhankelijkheid vergroot de impact van verstoringen, datalekken of misbruik van persoonsgegevens. Digitale weerbaarheid gaat verder dan technische beveiliging

alleen. Het raakt aan de vraag hoe je omgaat met leveranciers, ketens en data en hoe zij zorgen dat digitale dienstverlening betrouwbaar blijft. Vertrouwen in digitale systemen wordt een structurele randvoorwaarde.

Dit is dan ook hét moment om privacy en AI-governance vooraf in te bouwen. Door nu al na te denken over transparantie, verantwoord datagebruik en digitale weerbaarheid, voorkom je reputatierisico's en ingrijpend toezicht achteraf.

Gemeente Leeuwarden

Bijlage 1 - Stand van zaken AVG per onderwerp

Dit is het dashboard dat voortkomt uit het invullen van het Borgingsproduct van de VNG. Het Borgingsproduct beschrijft precies wat geregeld moet zijn om als organisatie aan de AVG te voldoen.

Per onderdeel leidt het antwoord op de vragen tot een percentage. Dat percentage geeft vervolgens aan in hoeverre de organisatie voldoet aan dat specifieke onderdeel. Op dit moment wordt de vragenlijst gemeentebreed ingevuld door de privacy officers, de information security officer en de record manager. Om tot een score te komen die inzage geeft in een sector of zelfs een team, zouden de hoofdstukken 2, 4, 5 en 6 door de verschillende managers ingevuld moeten worden. Dit staat voor komend jaar op de planning.

Paragraaf	Titel	Percentage
1.	Beleid	83%
1.1	Beleid vaststellen	100%
1.2	Privacybeleid	78%
1.3	Verantwoordelijkheden	83%
2.	Processen	78%
2.1	Werkprocessen	86%
2.2	Verwerkingsregister	95%
2.3	Pre-DEPIA's	**58%**
2.4	DEPIA's	65%
2.5	Bewaar- en vernietigingsbeleid	71%
3.	Organisatorische inbedding	84%
3.1	Privacyteam	**25%**
3.2	Aanstelling, positie en taken FG	95%
3.3	Informeren OR	100%
3.4	Bewustwording	75%
4.	Rechten van betrokkenen	94%
4.1	Recht op informatie	95%
4.2	Processen rechten van betrokkenen	94%
4.3	Toestemming	100%
4.4	Geautomatiseerde individuele besluitvorming	80%
4.5	Websites en applicaties	100%
4.6	Technische ondersteuning	100%
5.	Samenwerking	97%
5.1	AVG rollen	97%
5.2	Gegevensverstrekking	96%
6.	Gegevensbescherming	79%
6.1	Risico's	**50%**
6.2	Gegevensbescherming door ontwerp	88%
6.3	Gegevensbescherming door standaardinstellingen	75%
6.4	Informatiebeveiliging	64%
6.5	Privacyincidenten en datalekken	96%
7.	Verantwoording	86%
7.1	Evaluatie naleving AVG	75%
7.2	Evaluatie informatiebeveiliging	100%
7.3	Rapportage	100%

Bijlage 2 - Overzicht Herziening en nieuwe DEPIA's

Herziening van bestaande DEPIA's, stand van zaken per 31-12-2025:

	Naam DEPIA	Omschrijving	Startdatum	Status
1.	Bodycams	Camera's die door BOA's worden gebruikt bij incidenten of escalatie, ter voorkoming of in ieder geval registratie daarvan	09-06-2023	In behandeling bij afdeling
2.	Uitvoering dagelijkse politietaak door Boa's	Een all-in platform dat voorziet in verzameling, verkrijging en opvolging van (algemene, strafrechtelijke of bestuursrechtelijke) informatie	09-06-2023	In behandeling bij afdeling (ondersteund door externe partij)
3.	Rittenregistratie	Aanpassing van het systeem voor registratie van gebruik dienstauto's in de buitendienst.	12-03-2024	In behandeling bij afdeling (eigenaarschap onbekend)
4.	Kentekenparkeren/ ANPR-camera's	Controle van het geldig parkeerrecht door het gebruik van batch-gewijs scanning of inzet van scanvoertuigen	20-06-2024	In behandeling bij afdeling
5.	CCTV	De beveiliging van personen, gebouwen, terreinen en zaken die aan de zorg van Gemeente Leeuwarden zijn toevertrouwd. Meer specifiek ook ter handhaving van gebouwverboden van personen en ter bescherming van publieke personen	27-09-2024	In behandeling bij afdeling
6.	Datawarehouse	Gegevens uit meerdere bronnen opslaan. Door het in de tijd vaker opslaan van hetzelfde type gegevens kunnen analyses en rapportages worden gemaakt / het koppelen van (reeds bekende) gegevens op het gebied van Wmo, Wet Gemeentelijke Schuldhulpverlening, Jeugdwet, Onderwijs en Participatiewet zou kunnen leiden tot een (kosten)efficiëntere zorgverlening	24-04-2024	In behandeling bij afdeling
7.	Webcrawler Voyager	Gebruik webcrawler Voyager tbv de handhaving van de niet vergunde sector prostitutie in de gemeente Leeuwarden	Herziening nodig per juni 2024	Nog niet uitgezet door privacy
8.	Gezichtsherkenning RNI	Toepassen van gezichtsherkenning ter vergelijking met identiteitsdocumenten.	Herziening per 01-2025	Nog niet uitgezet door privacy
9.	Bestuurlijke aanpak ondermijnende criminaliteit Leeuwarden	Bijeenbrengen van ondermijningssignalen die zich organisatiebreed voordoen en het opstellen van een plan van aanpak om ondermijning tegen te gaan door onder meer gegevens te delen met de politie of het RIEC Noord.	Herziening per 02-2025	Nog niet uitgezet door privacy
10.	Camerahandhaving autoluwe binnenstad	Inzetten van camera's om ervoor te zorgen dat de binnenstad autoluw blijft.	Herziening per 04-2025	Nog niet uitgezet door privacy
11.	Zaakgericht werken	Zaakgericht werken via Rex	Herziening per 05-2025	Nog niet uitgezet door privacy
12.	Journalistiek	Advies over gebruik beeldmateriaal.	Herziening per 06-2025	Nog niet uitgezet door privacy

Gemeente Leeuwarden

Nieuwe DEPIA's, stand van zaken per 31-12-2025:

	Naam DEPIA	Omschrijving	Startdatum	Status
1.	DEPIA en actualiseren convenanten OOV	Actualiseren diverse documenten en convenanten	12-01-2024	In behandeling bij afdeling, voorlopig gestaakt
2.	Inzet van drones	In algemene zin inzetten van drones binnen gemeentelijke vraagstukken	05-04-2024	In behandeling bij afdeling, voorlopig gestaakt
3.	Opvang Oekraïners	In kaart brengen van processen en risico's signaleren	13-02-2024	In behandeling bij afdeling
4.	MS 365	Overzicht maatregelen vanuit DEPIA het Rijk op MS 365	30-11-2024	In behandeling bij afdeling
5.	Mens en Organisatie	Alle processen van Mens en Organisatie beoordelen op risico's en maatregelen	04-07-2024	In behandeling bij afdeling
6.	Urgentieverordening	Toevoegen DEPIA aan verordening	05-08-2024	In behandeling bij afdeling
7.	Gebouwontzeggingen	Proces van inzetten en bijhouden van gebouwontzeggingen	11-07-2024	In behandeling bij afdeling
8.	Zwerfafvaldetectie	Proces van detecteren van zwerfafval en daarop actie inzetten	31-07-2024	In behandeling bij afdeling, voorlopig gestaakt
9.	Spookbewoning	Proces spookbewoning dmv tool van TNO	27-09-2024	In behandeling bij privacy
10.	Uitvoering Sociaal Domein (w.o. Life Coaching jongerenteam & Handhaving SD	Alle processen van Uitvoering Sociaal Domein beoordelen op risico's en maatregelen	11-09-2024	In behandeling bij afdeling
11.	Opnemen telefoongesprekken	Opnemen van telefoongesprekken binnen organisatie	28-10-2024	In behandeling bij afdeling
12.	Platform woningverduurzaming	Platform voor bij elkaar brengen vraag en aanbod bij verduurzamen woningen	22-11-2024	In behandeling bij afdeling
13	Bibob	Uitvoeren van DEPIA op proces Bibob	12-11-2024	In behandeling bij ondersteunende beleidsafdelingen
14	E-mail archivering	Bevriezen van e-mail in outlook om de juiste bewaartermijnen te hanteren.	06-08-2025	In behandeling bij afdeling
15.	Bezorgen reisdocumenten en rijbewijzen	Bezorgen van reisdocumenten en rijbewijzen door Dynasure	14-11-2024	In behandeling bij privacy, vervolg is voorleggen FG
16.	Vraagstuk soevereinen	Onderzoeken van proces rondom soevereinen	20-09-2024	In behandeling bij privacy, vervolg is voorleggen FG
17.	Aanvraag Levensonderhoud (ALO)	Proces aanvraag Levensonderhoud toevoegen aan MijnLeeuwarden.nl	22-10-2024	In behandeling bij privacy, vervolg is voorleggen FG
18.	DEPIA & AIIA Project OmgevingsChat, route kaart verantwoorde AI	Opzetten chatbot voor vragen binnen Omgevingswet	24-12-2024	Afronding door behandeling bij afdeling, vervolg is voorleggen FG
19.	Spraak assistent Service & Informatie	Via spraaktechnologie meldingen woon-werk- en leefomgeving doen	05-02-2024	Afgerond
20.	Anonimiseren en waarmerken documentatie	Proces van anonimiseren van documenten vóór publicatie	08-03-2024	Gestaakt. Wordt via Woo-verzoek of publicatieproces opgepakt.

Bijlage 3 - Overzicht rechten van betrokkenen

Type verzoek AVG recht	Aantal 2024	Aantal 2025
Inzage	6	7
Inzage/kopie dossier	0	4
Bezwaar op inzageverzoek	2	1
Verwijdering	7	1
Verwijdering (Amaryllis)	4	0
Bezwaar op verwerking	0	1
Correctie	3	0
Klacht	2	2
Totaal	**24**	**16**

Type verzoek Wpg recht	Aantal 2024	Aantal 2025
Inzage	1	3

Ondersteuning bij kopie dossier (Woo/Wmo/Jeugd/Participatiewet/MOL)	Aantal 2024	Aantal 2025
Verzoek kopie dossier	11	23

Ondersteuning bij kopie dossier vanuit RIEC en/of ZVHF	Aantal 2024	Aantal 2025
Verzoek kopie dossier	3	2

Bijlage 4 - Overzicht datalekken

Type datalekken	2024	2025
Interne datalekken, die niet gemeld hoeven te worden aan de Autoriteit Persoonsgegevens	47	47
Datalekken die gemeld zijn aan de Autoriteit Persoonsgegevens	33	15
Datalekken waarbij een partner verwerkersverantwoordelijk is en het datalek behandelt	3	3
Totaal aantal datalekken	83	**65**

Hieronder in percentages het type datalekken. Net als te zien is in de landelijke trend, zijn de meeste datalekken ontstaan bij de verzending en bezorging van fysieke post en emails.

Soort	percentage	Type datalek
Email	39%	Email naar verkeerde persoon gestuurd
		Email verstuurd met ontvangers in CC in plaats van in BCC
		Email met persoonsgegevens onbeveiligd verstuurd
Fysieke post	32%	Brief ontvangen door verkeerde ontvanger
		Brief geopend retour ontvangen
Publicatie	10%	Niet volledig geanonimiseerd online publiceren van stukken, vergunningen etc
Overig	19%	Bijvoorbeeld: toegang tot netwerk, gegevens toevoegen aan verkeerde dossier

Bijlage 5 – Resultaten externe audit Wpg

Sub oordelen domein I Openbare ruimte

Domein	Verwerking
I	**Gemeente - Openbare Ruimte**
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de APV van de gemeente.
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot parkeeroverlast en -excessen
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot het Vuurwerkbesluit en de Wet Milieubeheer
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de verwijzing voor vuurwerkoverlast door minderjarigen.
☒	Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de Alcoholwet 2021.

Tabel Verwerkingen domein I

Wpg onderwerpen	Oordelen		
	Opzet	Bestaan	Werking
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Data protection impact assessment (DPIA)			
9. Bijzondere politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen			
12. Onderscheid tussen verschillende categorieën van betrokkenen			
13. Verwerker en verwerkersovereenkomst			
14. Geheimhoudingsplicht			
15. Geautomatiseerde individuele besluitvorming **			
16. Uitvoering van de dagelijkse politietaak			
17. Ter beschikking stellen van politiegegevens binnen het WPG-domein			
18. Geautomatiseerd vergelijken en in combinatie zoeken **			
19. Ondersteunende taken **			
20. Bewaartermijnen, verwijderen en vernietigen			
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee			

Wpg onderwerpen	Oordelen		
	Opzet	Bestaan	Werking
22. Doorgiften aan derde landen **			
23. Verstrekking aan derden structureel voor samenwerkingsverbanden			
24. Rechtstreekse verstrekking			
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering			
26. Register			
27. Documentatie			
28. Logging			
29. Audits			
30. Melding datalekken			
31. Functionaris voor Gegevensbescherming			

Tabel Sub oordelen domein I

Technische en organisatorische maatregelen	Oordelen		
	Opzet	Bestaan	Werking
1. GITC1. Wijzigingsbeheer			
2. GITC2. Logische toegangsbeveiliging			
3. GITC3. Beheer van kwetsbaarheden (patchmanagement			
4. GITC4. Cryptografie			
5. GITC5. Vulnerability scans en penetratietesten			

Tabel Sub oordelen technische en organisatorische maatregelen domein I

Gemeente Leeuwarden

Sub oordelen domein III Onderwijs

Verwerking
Verwerken van politiegegevens in verband met de opsporing en vervolging van strafbare feiten met betrekking tot de leerplichtwet en alle daaraan gerelateerde wet- en regelgeving.

Tabel Verwerkingen domein III

Wpg onderwerpen	Oordelen		
	Opzet	Bestaan	Werking
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Data protection impact assessment (DPIA)			
9. Bijzondere politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen **			
12. Onderscheid tussen verschillende categorieën van betrokkenen			
13. Verwerker en verwerkersovereenkomst			
14. Geheimhoudingsplicht			
15. Geautomatiseerde individuele besluitvorming **			
16. Uitvoering van de dagelijkse politietaak			
17. Ter beschikking stellen van politiegegevens binnen het WPG-domein			
18. Geautomatiseerd vergelijken en in combinatie zoeken **			
19. Ondersteunende taken **			
20. Bewaartermijnen, verwijderen en vernietigen			
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee			
22. Doorgiften aan derde landen **			
23. Verstrekking aan derden structureel voor samenwerkingsverbanden			
24. Rechtstreekse verstrekking **			
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering			
26. Register			
27. Documentatie			
28. Logging			
29. Audits			
30. Melding datalekken			
31. Functionaris voor Gegevensbescherming			

Technische en organisatorische maatregelen	Oordelen		
	Opzet	Bestaan	Werking
1. GITC1. Wijzigingsbeheer			
2. GITC2. Logische toegangsbeveiliging			
3. GITC3. Beheer van kwetsbaarheden (patchmanagement			
4. GITC4. Cryptografie			
5. GITC5. Vulnerability scans en penetratietesten			

Tabel Sub oordelen technische en organisatorische maatregelen domein III

Gemeente Leeuwarden

Sub oordelen domein V Werk, inkomen en zorg

Wpg onderwerpen	Oordelen		
	Opzet	Bestaan	Werking
1. Reikwijdte			
2. Doelbinding			
3. Noodzakelijkheid & rechtmatigheid, vermelding herkomst			
4. Juistheid en volledigheid politiegegevens			
5. Onderscheid feiten en oordeel			
6. Gegevensbescherming door beveiliging en ontwerp			
7. Gegevensbescherming door standaardinstellingen			
8. Data protection impact assessment (DPIA)			
9. Bijzondere politiegegevens			
10. Autorisaties en toegang tot politiegegevens			
11. Autorisaties: aanwijzen functionarissen			
12. Onderscheid tussen verschillende categorieën van betrokkenen			
13. Verwerker en verwerkersovereenkomst			
14. Geheimhoudingsplicht			
15. Geautomatiseerde individuele besluitvorming **			
16. Uitvoering van de dagelijkse politietaak			
17. Ter beschikking stellen van politiegegevens binnen het WPG-domein			
18. Geautomatiseerd vergelijken en in combinatie zoeken **			
19. Ondersteunende taken **			
20. Bewaartermijnen, verwijderen en vernietigen			
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee			
22. Doorgiften aan derde landen **			
23. Verstrekking aan derden structureel voor samenwerkingsverbanden **			
24. Rechtstreekse verstrekking			
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering			
26. Register			
27. Documentatie			
28. Logging			
29. Audits			
30. Melding datalekken			
31. Functionaris voor Gegevensbescherming			

Tabel Sub oordelen domein V

Technische en organisatorische maatregelen	Oordelen		
	Opzet	Bestaan	Werking
1. GITC1. Wijzigingsbeheer			
2. GITC2. Logische toegangsbeveiliging			
3. GITC3. Beheer van kwetsbaarheden (patchmanagement			
4. GITC4. Cryptografie			
5. GITC5. Vulnerability scans en penetratietesten			

Tabel Sub oordelen technische en organisatorische maatregelen domein V

De Dienst
Noardwest Fryslân
zo werkt het sociaal

Memo

Aan: 5.1.2e
Van 5.1.2e, Functionaris Gegevensbescherming
Datum: 13 januari 2022

Onderwerp: Opname vergaderingen Microsoft Teams

☒ Geheim document ☐ Openbaar document

Sedert meer dan een jaar worden bij de gemeente Leeuwarden initiatieven ontwikkeld om de functionaliteit van Microsoft Teams uit te breiden met het opnemen van beeld en geluid in online bijeenkomsten als vergaderingen, cursussen, instructies, etc.

Omdat het opnemen van bijeenkomsten een verwerking van persoonsgegevens is, zoals bedoeld in de AVG, moet het gebruik van deze functionaliteit worden getoetst aan de AVG. Het gebruik voor instructies en cursussen stuit naar het zich laat aanzien niet op bezwaren vanuit de AVG. Voor vergaderingen ligt dit anders.

Ook voor vergaderingen moet worden beoordeeld of er een rechtmatige grondslag is voor de verwerking van persoonsgegevens en of recht wordt gedaan aan de beginselen van proportionaliteit, subsidiariteit, dataminimalisatie en het noodzakelijkheidsvereiste in relatie tot een vooraf duidelijk omschreven doel. In voorbereidende documenten en besprekingen is gesteld dat het doel van het opnemen van vergaderingen is gelegen in het niet hoeven notuleren. Ook kunnen genodigden die verhinderd waren de vergadering op een later tijdstip afspelen.

Toestemming van de deelnemers kan niet als rechtmatige grondslag dienen omdat er geen sprake is van vrije toestemming in verband met de ongelijkwaardige verhouding tussen werkgever en werknemer. Als rechtmatige grondslag zou alleen een gerechtvaardigd belang van de werkgever in aanmerking kunnen komen. Tot op heden is een gerechtvaardigd belang niet duidelijk aangetoond. Als er al sprake van een gerechtvaardigd belang zou zijn voor het opnemen van vergaderingen, dan moet dit worden afgewogen tegen de inbreuk op de privacy van de deelnemers aan de vergaderingen.

Met het opnemen van vergaderingen wordt door de verwerking van persoonsgegevens een aanzienlijke inbreuk op de privacy gemaakt. Het gaat daarbij niet alleen om vastlegging van wat er inhoudelijk wordt gezegd maar ook om persoonsgegevens als uiterlijk, stem, gelaatsuitdrukking, motoriek, houding, fysionomie, gebreken, etc. Bij het vergaderen vanaf de thuislocatie wordt ook de privéomgeving gefilmd, tenzij een standaard achtergrond wordt gekozen. De inbreuk op de privacy weegt dan ook niet op tegen het doel “niet hoeven notuleren”. Het opnemen van vergaderingen is daarom niet proportioneel. Daarnaast worden gegevens als stemgeluid, uiterlijk, etc. verwerkt die niet nodig zijn voor de verslaglegging van vergaderingen. Ook aan de eisen van dataminimalisatie en noodzakelijkheid wordt derhalve niet voldaan. Overigens kan er geen noodzaak voor het opnemen van vergaderingen ontstaan omdat Microsoft nieuwe functionaliteit heeft ontwikkeld.

Er is niet gezocht naar alternatieven, bijvoorbeeld het blijven notuleren zoals dat al sinds jaar en dag wordt gedaan. Er is nooit gebleken dat dit een probleem vormt. Er bestaat ook

software voor het omzetten van spraak naar tekst. Deze mogelijkheid die minder inbreuk op de privacy maakt, is niet onderzocht. Het beginsel van subsidiariteit wordt dus niet toegepast.

Voor de invoering van opnamefunctionaliteit is instemming van de Ondernemingsraad vereist op grond van WOR artikel 27 lid 1 sub l (bijlage 1) nu daarmee stelselmatige monitoring mogelijk is. Ook als de opnamefunctionaliteit niet voor monitoring wordt gebruikt is instemming vereist, de mogelijkheid alleen is hiervoor reeds voldoende.

Bovenstaande argumenten zijn door Functionarissen Gegevensbescherming eerder ingebracht in commentaren op een memo van het Projectteam Digitale Werkomgeving MS 365 aan de Stuurgroep Digitale Werkomgeving MS 365 van de gemeente Leeuwarden en de uitgevoerde DPIA. Zie ook bijlage 2.

Conclusie en advies

Het gebruik van de opnamefunctionaliteit in Microsoft Teams voor vergaderingen is in strijd met de AVG.

Advies:
- Het gebruik van Microsoft Teams niet toestaan voor het opnemen van vergaderingen;
- Dit onderwerp bespreken met de Ondernemingsraad van de Dienst;
- De gemeente Leeuwarden er op wijzen dat de opnamefunctionaliteit niet mag worden gebruikt voor vergaderingen waar medewerkers van de Dienst bij betrokken zijn;

www.sozawe-nw-fryslan.nl

Bijlage 1 Wet op de ondernemingsraden

Artikel 27

1 De ondernemer behoeft de instemming van de ondernemingsraad voor elk door hem voorgenomen besluit tot vaststelling, wijziging of intrekking van:
l. een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen;

www.sozawe-nw-fryslan.nl

Bijlage 2 Eerder aangeleverd commentaar

Selectie commentaren op een memo van het Projectteam Digitale Werkomgeving MS 365 aan de Stuurgroep Digitale Werkomgeving MS 365 van de gemeente Leeuwarden:

Leeuwarden

Toestemming is een middel wat moeilijk kan worden gebruikt in een werknemer/werkgever situatie. Er is namelijk nooit sprake van vrijelijke toestemming. Daarom willen we juist een andere grondslag vinden zodat het mag zonder toestemming. De afweging per situatie waarin de gemeente opname wil inzetten is daarom van belang.

Noardeast Fryslân

Ik denk dat we grondslag juist niet in toestemming moeten vinden, maar in het gerechtvaardigd belang van de werkgever en wellicht ook het belang van andere deelnemers aan een vergadering.

Waadhoeke

Eens met hierboven. Toestemming kan niet de grondslag zijn. Er is niet alleen sprake van een hiërarchische verhouding, maar ook van groepsdruk wanneer het in een vergadering zelf wordt gevraagd.

Grondslag gerechtvaardigd belang (maar het echte belang is m.i. nog niet volledig aangetoond). Met de kanttekening dat iemand zich kan en mag verzetten tegen de opname. Artikel 18 AVG.

De Dienst

Verzet moet kunnen, maar In de praktijk zal dit niet werken. Gerechtvaardigd belang is inderdaad niet duidelijk. Verder moeten beginselen van proportionaliteit, subsidiariteit (gewoon notuleren zoals dat sinds jaar en dag gebeurt) en dataminimalisatie in acht worden genomen. Zolang die afweging niet glashelder is geen opname vergaderingen

Commentaar op de DPIA:

Een ander kan privacygevoelig zijn. De AVG is dan ook onverkort van toepassing. Voor bewustmakingsmateriaal en cursussen ligt het minder gevoelig, het doel is duidelijk en er is expliciete toestemming van de deelnemers, althans de docenten, misschien niet van de cursisten (tenzij vooraf toestemming wordt gevraagd).

Bij vergaderingen ligt het anders. Het doel van opname en/of verspreiding is niet altijd duidelijk. Dit moet per vergadering vastgesteld worden en aan de deelnemers worden medegedeeld. Vervolgens moet aan iedere deelnemer toestemming worden gevraagd en vastgelegd, bijvoorbeeld in de notulen. Aan het eind van de vergadering moet de toestemming voor opname en verspreiding ook weer kunnen worden ingetrokken. Het weigeren of intrekken van toestemming hoeft niet te worden gemotiveerd. Als toestemming

www.sozawe-nw-fryslan.nl

wordt gegeven moet ook duidelijk zijn naar wie de opname zal worden verspreid. Dan is het ook nog zo dat de ontvanger iedereen kan laten meekijken, tenzij daar duidelijke regels voor zijn die kunnen worden gehandhaafd. Bij het opnemen en verspreiden van een opname moet ook rekening worden gehouden met proportionaliteit (het gaat om een aanzienlijke inbreuk op de privacy) en subsidiariteit (notulen verspreiden) in relatie tot het doel. Dan is het de vraag of de opname functionaliteit alleen voor geplande afspraken in de agenda beschikbaar is of bij ieder Teams gesprek kan worden ingeschakeld. Mogelijk ontstaat er dan een oncontroleerbare situatie. Verder moet ook de relatie met het portretrecht worden onderzocht.

Van: 5.1.2e <5.1.2e @noardeast-fryslan.nl>
Verzonden: vrijdag 4 september 2020 11:36
Aan: 5.1.2e <5.1.2e @noardeast-fryslan.nl>; 5.1.2e <M.Post@noardeast-fryslan.nl>
Onderwerp: RE: MS Stream - Vragen & Antwoorden

Ik zie dat de FG's (5.1.2e voor Leeuwarden en 5.1.2e voor Waadhoeke) ook niet in de mail zijn meegenomen, maar ik zie wel dat 5.1.2e als voormalig FG wel een paar AVG-vragen heeft gesteld. De vragen zijn "met verschillende vakspecialisten besproken", maar het is niet duidelijk met wie en of daar FG's bij zijn geweest. Ik vermoed, gelet op de antwoorden, dat dat niet zo is…

Ik heb nog niet helemaal duidelijk in beeld wat Streams precies is, maar ik begrijp dat er beeld- en geluidsopnamen van bijeenkomsten tussen werknemers -en mogelijk externe partijen- worden gemaakt en opgeslagen/bewaard. Op basis van de WP29-richtlijnen en het besluit van de Autoriteit Persoonsgegevens kan daarvoor een DPIA verplicht omdat er sprake is van de volgende verwerkingen:
- Stelselmatige monitoring (WP29-3): verwerking die wordt gebruikt voor het observeren, monitoren of controleren van betrokkenen;
- Op grote schaal verwerkte gegevens: in de AVG wordt niet gedefinieerd wat grootschalig is, al worden in overweging 91 enkele richtsnoeren gegeven. *In ieder geval raadt de WP29 aan om met name de volgende factoren in aanmerking te nemen bij het bepalen of een verwerking op grote schaal wordt uitgevoerd;*
a. het aantal betrokkenen, hetzij als een specifiek aantal hetzij als een deel van de relevante populatie;
Op de totale schaal van het aantal werknemers kan deze verwerking voor al die werknemers gelden, en dan is er sprake van grootschaligheid.
- Controle werknemers (AP-11): grootschalige verwerking van persoonsgegevens en-of stelselmatig monitoring van activiteiten van werknemers

En omdat je ook over de toepasselijkheid van deze categorieën nog wel een discussie kan voeren, het volgende advies van de WP29: "In gevallen waarin het niet duidelijk is of een [DPIA] vereist is, raadt de WP29 aan om deze toch uit te voeren omdat een [DPIA] een nuttig instrument is dat verwerkingsverantwoordelijken helpt om aan de wetgeving inzake gegevensbescherming te voldoen." Dus zelfs al zou een DPIA niet verplicht hoeven te zijn, dan lijkt me toch verstandig om er een uit te laten voeren om je als werkgever tegenover je

www.sozawe-nw-fryslan.nl

werknemers te kunnen verantwoorden. Wellicht kunnen de DPIA's die door het Rijk op Windows10 en Office365 zijn uitgevoerd hierbij betrokken worden.

Ik zou een paar vragen uit de AVG toch nog wel beantwoord willen zien:
- Op welke grondslag is/wordt deze verwerking gebaseerd. Er is sprake van een hiërarchische werkgever-werknemerrelatie, dus toestemming kan en mag nooit als grondslag gelden (de toestemming kan namelijk niet in vrijheid gegeven worden). Het antwoord op de tweede vraag van 5.1.2e ("De toestemming/melding is formeel niet per se nodig aangezien zij leden van de vergadering zijn en dit hebben geaccepteerd") vind ik daarom (veel) te kort door de bocht. De werkgever zal zich vermoedelijk op zijn gerechtvaardigd belang beroepen, laat dat dan maar uitleggen waarom dat belang zwaarder weegt dan de rechten en vrijheden van de werknemers.
- Het antwoord op de derde vraag van 5.1.2e (AVG-rechten beperking, wissen, etc) waarin gezegd wordt dat "de oplossing [...] hier volgens 5.1.2e niet in [hoeft] te voorzien. In zo'n geval gaat er een verwijderingsverzoek naar FG@leeuwarden.nl. Dit zal dan per geval worden beoordeeld" is ook te kort door de bocht. De AVG schrijft voor dat je de risico's aan de voorkant zoveel mogelijk moet beperken. Gewoon doen en reageren als zich iets voordoet is niet conform AVG. Bovendien heb je als verwerkingsverantwoordelijke de plicht om betrokkene vooraf te informeren over de verwerking. Heel strikt genomen zou de werkgever als verwerkingsverantwoordelijk dan ook de huisgenoten van thuiswerkers die in beeld kunnen komen moeten informeren over het feit dat hun gegevens mogelijk door de werkgever verwerkt kunnen worden...
- Ook het antwoord op de vierde vraag van 5.1.2e (datalek) is veel te kort door de bocht. "Dit risico bestaat, echter komt de data in handen van een betrouwbare relatie *[dus? RC]*. Dit hoeft dan niet altijd bij de autoriteit persoonsgegevens gemeld te worden. Het verkeerd delen is dan wel een datalek, maar niet altijd meldingsplichtig." Ieder datalek moet individueel beoordeeld worden, en een datalek zoals genoemd in het voorbeeld (een casusbespreking van een gebiedsteam WMO/Jeugd) kan zeker een hoog risico inhouden en daarmee meldingsplichtig zijn aan zowel de AP als aan de betrokkenen.
- Bij de eerste vraag van 5.1.2e wordt het opslaan en delen als doel genoemd, maar dat is natuurlijk een middel om het doel "interne communicatie, training en bewustmaking" te bereiken. Het doel zal bij de grondslagbeoordeling van het gerechtvaardigd belang aangetoond moeten worden.
- Ik begrijp dat iedere deelnemer aan een overleg een opname kan starten. Wat gebeurt er als een van de andere deelnemers bezwaren tegen een opname heeft, bijvoorbeeld als deze een beroepsgeheim heeft of er zeer vertrouwelijke gegevens worden gedeeld. Is het bijvoorbeeld mogelijk om niet de opname van een heel overleg, maar fragmenten daarvan te delen?
- Als er bij een overleg externe partijen aanwezig zijn, hoe zit het dan met bijvoorbeeld de beschikbaarheid van de opname. Is die ook voor die externe partijen beschikbaar?
- De opnames zijn beschikbaar in MP4-formaat. Is het mogelijk om een opname lokaal te bewaren zodat deze via een USB-stick of vergelijkbaar kan worden gedeeld?

Eerst maar even tot zover…

www.sozawe-nw-fryslan.nl

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 5, 6

AANVULLING DEPIA MBT DATA-ETHIEK : 5.1.2i

Wie zijn betrokken bij DEPIA vanuit expertise
(bijv. ISO, juridische expertise, inkoop, procesontwerper etc.)

Functie	**Naam**
Projectleider	5.1.2e
Proceseigenaar	5.1.2e
Privacy Officer	5.1.2e
Inkoop	?
ISO	5.1.2e
FG	5.1.2e
Adviseur data-ethiek	5.1.2e
Informatieadviseur(s)	5.1.2e en 5.1.2e

Planning
Vul in wat van toepassing is voor het betreffende project.

	Taak	**Datum gereed**
Fase 1	Uitvoeren Pre-DEPIA	
	Beoordelen Pre-DEPIA door FG	
	Voorafgaande raadpleging van AP (indien van toepassing)	
Fase 2	Uitvoeren DEPIA; invullen door projectleider/beleidsmedewerker	
	Uitvoeren DEPIA; raadplegen PO	
	Uitvoeren DEPIA; raadplegen ISO	
	Uitvoeren DEPIA; raadplegen Adviseur data-ethiek	
Fase 3	Beoordeling door FG en Adviseur Data-ethiek	
	Indien van toepassing; uitvoeren moreel beraad of inzetten data-ethische commissie.	
	Reflectie op de data-ethische waarden vanuit moreel beraad of data-ethische commissie toevoegen aan DEPIA	
	Indien van toepassing; aanpassen DEPIA	
	Beoordeling door FG en Adviseur Data-ethiek	09-04-2024
Fase 4	Eindbeoordeling bestuur/MT/Proceseigenaar	
	Opslaan documenten (Pre-DPIA, DEPIA)	
	Bepalen mate van vertrouwelijkheid documenten	
	Toesturen documenten naar FG	
	Herziening DEPIA inplannen (3 jaar na datum definitieve versie DEPIA)	

1. Baten

Bij baten kun je denken aan vrijheid, welzijn, welvaart, duurzaamheid, inclusiviteit en diversiteit, gelijkheid, efficiëntie en kostenreductie. (Deze brede benadering is belangrijk, omdat ethische en juridische aspecten invloed kunnen hebben op de relatie tussen onze organisatie en de omgeving)

1.1: Wat zijn de baten voor gemeente Leeuwarden als organisatie?

In vergelijking met 5.1.2i heeft 5.1.2i verschillende functionaliteiten die het MOL-meldingsproces verbeteren en dat zijn de volgende drie factoren: 1. 5.1.2i kan meer gestroomlijnde en efficiënte workflow bieden voor het verwerken van meldingen, waardoor de reactietijd van de gemeente op overlast en problemen wordt verkort. 2. Het is gebruiksvriendelijker dan 5.1.2i, waardoor de medewerker en stakeholders gemakkelijker meldingen kunnen maken, beheren en opvolgen. 3. Een overzicht van alle meldingen en de status ervan, waardoor de gemeente beter geïnformeerd is over de situatie in onze gemeente. Al deze aspecten leveren een bijdrage aan een efficiënter en effectiever meldingsproces vergeleken met 5.1.2i.
Advies FG: Akkoord
Adviseur data-ethiek: Geen toevoegingen verder

1.2: Wat zijn de baten voor het individu?

Vergeleken met 5.1.2i kan de burger de volgende voordelen ervaren wanneer wij gebruik van 5.1.2i maken voor het melden van overlast: - Met 5.1.2i kunnen wij meldingen sneller opvolgen en oplossen, wat resulteert in een snellere reactie op overlastsituaties. Dit betekent dat burgers minder lang hoeven te wachten voordat hun meldingen worden behandeld, waardoor ze zich sneller geholpen voelen. Het bevordert een veiligheidsgevoel. - Wanneer het mol-team optimaal 5.1.2i weet in te zetten, kan de burger geüpdatet worden van de status van de meldingen, om eventuele vragen of zorgen te bespreken. Hierdoor wordt het gevoel van betrokkenheid en transparantie vergroot bij de burgers. - Doordat 5.1.2i de taakefficiëntie van het MOL-team verbetert, kunnen meldingen sneller worden verwerkt en opgelost. Dit betekent dat burgers minder lang hoeven wachten op een reactie of oplossing voor hun meldingen.
Advies FG: Akkoord
Adviseur data-ethiek: Geen toevoegingen verder

1.3: Wat zijn de baten voor de Leeuwarder samenleving als geheel?

- De taakefficiëntie die 5.1.2i biedt aan het MOL-team helpt bij het verbeteren door het meldingsproces te stroomlijnen en te automatiseren. Hierdoor kunnen medewerkers hun tijd effectiever besteden aan het oplossen van overlastsituaties, waardoor er minder personeelsuren nodig zijn voor het afhandelen van meldingen. - De administratieve lasten kunnen beter worden georganiseerd door het hebben van een meldingsbeheersysteem, waardoor de administratieve lasten voor het beheren en verwerken van meldingen worden verminderd. Minder tijd besteed aan administratieve taken kan resulteren in lagere operationele kosten voor de gemeente. - Door sneller te kunnen reageren op meldingen van overlast, kan 5.1.2i helpen bij het voorkomen van langdurige en ernstigere overlastsituaties. Dit kan uiteindelijk leiden tot kostenbesparingen (bijvoorbeeld doordat er minder middelen nodig zijn voor herstelwerkzaamheden), een groter gevoel van veiligheid en een groter gevoel van betrokkenheid bij onze inwoners.
Advies FG: Akkoord
Adviseur data-ethiek: Geen toevoegingen verder

2. Verantwoording; Is het doel en hoe het doel wordt bereikt juridisch en ethisch verantwoord?

Beschrijf de invloed die het gebruik van gegevens of techniek heeft/kan hebben op menselijke en maatschappelijke waarden en belangen.

Wanneer de verwerking invloed heeft op de data-ethische waarden, betekent dit vaak dat de belangen van stakeholders geschaad worden. Dit kan richting geven aan de beoordeling of een toepassing data-ethisch verantwoord is. Hieronder staan de ethische waarden, die voor gemeente Leeuwarden van belang zijn.

- ***Rechtvaardigheid:***
  We dragen bij aan rechtvaardigheid, gelijke kansen en inclusiviteit. Onze digitale oplossingen zijn laagdrempelig en waardevol voor iedereen. We zijn alert op het voorkomen van ongewenste vooringenomenheid bij de selectie van data. Ook letten we erop dat er geen discriminatie, stereotypering of vooroordelen in algoritmes zit (bias).

- ***Menselijke waardigheid:***
  We behandelen bewoners, ondernemers en bezoekers als mensen, niet als 'nummer'. Onze digitaliseringstrajecten sluiten aan bij de leefwereld en behoeften van de mensen in onze gemeente. De mens is altijd leidend , niet de techniek/data.

- ***Privacy:***
  We beschermen de privacy van inwoners, ondernemers en bezoekers. Data van inwoners worden geanonimiseerd gebruikt en zijn niet herleidbaar tot een persoon. We gebruiken 'Privacy by design' en doen onderzoek naar de impact van digitaliseringstrajecten op de privacy.

- ***Veiligheid:***
  We waarborgen de openbare orde en veiligheid, zodat iedereen zich veilig voelt in onze gemeente. We beveiligen onze data. Via cybersecurity bereiden we ons voor op digitale aanvallen.

- ***Autonomie:***
  We respecteren menselijke autonomie (vrijheid). We vermijden onbewuste beïnvloeding, manipulatie en stimulering van dwangmatig gedrag of overheidstoezicht ('Big Brother'). We zijn terughoudend met het gebruik van data waarmee we gebruikers kunnen volgen, hun reputatie schaden of hun toekomst negatief kunnen beïnvloeden.

- ***Controle over technologie:***
  We controleren op natuurlijke momenten of onze digitaliseringstrajecten nog goed werken. Door open en transparant om te gaan met data en informatie, kan iedereen deelnemen op basis van dezelfde kennis en inzichten.

- ***Kwaliteit van leven/duurzaamheid:***
  We vinden gezond en duurzaam leven belangrijk in Leeuwarden. We zoeken naar duurzame oplossingen waarbij de gezondheid van inwoners, ondernemers en bezoekers voorop staat. We toetsen of digitale oplossingen echt meerwaarde hebben voor de gemeente.

- ***Mienskip:***
  We vinden de bescherming van de gemeenschap belangrijk. We zorgen ervoor dat onze digitale toepassingen aansluiten op het gevoel van mienskip. We streven ernaar dat groepen inwoners en ondernemers vertrouwen hebben in de gemeente en onze digitaliseringstrajecten.

2.1: Welke van de eerder genoemde waarden worden beïnvloed of geraakt door het project/proces? (bespreek alle bovenstaande waarden. En benoem bij 3.3 de risico en de maatregelen.)
Beoordeel in de onderstaande vragen of er één of meerdere waarden zijn die mogelijk geraakt worden door het project/proces. (Als de waarde negatief wordt geraakt, neem deze dan op in de risico's bij vraag 11.3 en 11.4)

Veiligheid en Rechtvaardigheid Veiligheid: Dit wordt bevorderd door middel van snellere respons op veiligheidsmeldingen, zoals defecte straatverlichting, of in de toekomst straatintimidatie. Rechtvaardigheid: Draagt bij aan gelijke toegang tot diensten, aangezien meldingen vanuit verschillende wijken op een dezelfde manier wordt behandeld. Menselijke waardigheid: bij valse meldingen (dit staat los van 5.1.2i, maar heeft te maken met proces van doen van meldingen. Voor de aandacht voor privacy wordt verwezen naar de DPIA, voor risico's zie vraag 3.3.
Advies FG: Akkoord
Adviseur data-ethiek: Geen toevoegingen, als in 3.3 de risico's zijn opgenomen.

3. Afweging;

Afweging van alle onderdelen in het kader van ethiek, privacy en informatieveiligheid.

3.1: Kan hetzelfde doel op een andere manier worden bereikt (subsidiariteit)? Leg uit waarom wel/niet.

Nee, niet op dezelfde wijze. Hoewel de binnen Leeuwarden gebruikte applicatie '5.1.2i' ook een deel van de functionaliteiten als 5.1.2i heeft, sluit dit onvoldoende aan op de eisen en werkwijze van MOL ten aanzien van het organiseren van haar processen en het uitvoeren van de werkzaamheden.
Advies FG: Akkoord

3.2: Kan hetzelfde doel met minder gegevens worden bereikt (proportionaliteit)? Leg uit waarom wel/niet.

De vastlegging van informatie in 5.1.2i en gedurende het proces is beperkt tot dat wat noodzakelijk en ter zake dienend is ter uitvoering van de werkzaamheden van MOL. Het is belangrijk om te benadrukken dat de verzameling van deze gegevens beperkt blijft tot wat strikt noodzakelijk of anderszins ter zake dienend is voor de behandeling van de melding. Hieronder vallen ook foto's of video's. Hoewel hieruit mogelijk meer gegevens af te leiden zijn dan een melder in reguliere zin dient in te vullen via het meldformulier, is deze informatie uiterst relevant voor het beoordelen van overlastmeldingen, de ernst daarvan, en het aan de hand daarvan afstemmen of escaleren met andere afdelingen of partijen. De beelden worden op eenzelfde wijze beschermd als andere persoonsgegevens en ook enkel gebruikt voor de doeleinden zoals hierboven beschreven.
Advies FG: Helder omschreven, de overige zaken rondom bewaren en bewaartermijnen komen terug in de DPIA.

3.3: Wat zijn de negatieve gevolgen en de genomen maatregelen voor de betrokkenen (Benoem de gevoel van een inwoner en de gevolgen. Bedenk dingen op de proces op de waarde en rechtvaardig)

Beschrijf en beoordeel risico's van de voorgenomen gegevensverwerkingen voor de de waarden vanuit vraag 2.1;

Negatieve gevolgen	Oorzaak hiervan	Kans op gevolgen	Impact van gevolgen	Maatregel	Geïmplementeerd door
1.Privacy gevolgen	Het delen van locatiegegevens	Midden	Hoog	Toegang alleen voor team-MOL.	Gemeente Leeuwarden
2.Weerstand burgers delen van gegevens	Digitale onzekerheid	Laag	Laag	Anoniem meldingen doen	Gemeente Leeuwarden
3. Mogelijke weerstand tegen verandering	Gebrek aan training en ondersteuning	Midden: weerstand tegen verandering is dat medewerkers niet goed worden betrokken bij het implementatieproces van 5.1.2i	Midden: weerstand tegen verandering kan leiden tot vertragingen in het meldingsproces en verminderde productiviteit van medewerkers, waardoor de voordelen van 5.1.2i niet volledig worden gerealiseerd	De gemeente kan ervoor zorgen dat medewerkers voldoende training en ondersteuning krijgen bij het gebruik van 5.1.2i, zodat ze zich comfortabel voelen bij de nieuwe technologie.	Gemeente Leeuwarden en Leverancier 5.1.2i
4. Technische problemen	Een gebrek aan geschikte IT-infrastructuur	Midden: technische problemen zijn mogelijk, vooral tijdens de initiële implementatie van 5.1.2i of bij updates van het systeem.	Hoog: technische problemen kunnen de efficiëntie van het meldingsproces verminderen en de reactietijd van de gemeente op overlastmeldingen vertragen, wat de tevredenheid van burgers kan verminderen.	Het verbeteren van de IT-infrastructuur kan helpen om technische problemen met 5.1.2i te voorkomen en een soepele implementatie en werking van het systeem te garanderen.	Leverancier 5.1.2i
5. Doen van valse meldingen	Dit kan gedaan worden als grap, uit wraak of om anderen te schaden	laag	Hoog	Melders dienen achternaam, postcode en telefoonnummer door te geven. Aan de hand van deze gegevens kan het MOLteam een verificatie doen	Gemeente Leeuwarden

				in de BRP(andere bron). Ook vind er altijd een eerste gesprek plaats alvorens een melding wordt omgezet tot een aanpak.	
6. Meldingen worden gebruikt om bepaalde groepen te discrimineren of te stigmatiseren, wat kan leiden tot onrechtvaardige behandeling.	Melders melden vanuit een discriminerende gedachtegang.	Midden	Hoog	Beleid doorvoeren dat discriminatie verbiedt en procedures voor het onderzoeken en behandelen van meldingen waarbij sprake is van discriminatie. In 5.1.2i werken wij met een persoonsgerichte aanpak. MOL selecteert hierin op gedrag en niet op eigenschappen waarop gediscrimineerd kan worden.	Gemeente Leeuwarden
7. Het verwerken van meldingen kan mogelijk leiden tot inbreuken op de privacy van individuen, vooral als persoonlijke gegevens onjuist worden gebruikt of gedeeld	De meldingen die ontvangen worden, worden direct als waarheid beschouwd en daarop ook als zodanig gehandeld.	Laag	Hoog	Wij delen sfeerbeelden met bijv. ketenpartners. Meldingen zijn niet op feitelijkheden gebaseerd, maar deze sfeerbeelden kunnen wel door ketenpartners gecheckt worden op feitelijkheden.	Gemeente Leeuwarden
8. Het verwerken van meldingen kan mogelijk leiden tot inbreuken op het gevoel van privacy, als het persoonlijke meldingen betreft)	Benoeming van gedragingen van een beklaagde in de AVG brief	Midden	Midden	Zo feitelijk mogelijk benoemen van de gemelde overlast.	Gemeente Leeuwarden
Advies FG: Akkoord.					
Adviseur data-ethiek: Goede aanvullingen.					

3.4: Zijn er rest-risico's en zo ja, welke? Leg ook uit waarom.

N.v.t.
Advies FG: Akkoord
Adviseur data-ethiek: Akkoord

Datum: 09-04-2024
Eindoordeel Functionaris voor Gegevensbescherming: De combinatie van de risico's en maatregelen uit de extern uitgevoerde DPIA en deze aanvulling op data-ethiek geeft een goed beeld van het proces en de maatregelen die ingezet worden om de risico's te beperken.

Graag ontvang ik het zaaknummer van de defintieve versie (en de verwerking in het register zal ook aangepast moeten worden). Voor de duidelijkheid; de definitieve versie is dan dit document en het document van Waker.

Beoordeling (door management/bestuur)	**Is de beoordeling openbaar, vertrouwelijk, zeer vertrouwelijk of geheim**

Waar wordt de beoordeling opgeslagen

Startdatum verwerkingen (indien van toepassing)	**Wanneer bijwerken register (indien van toepassing)**	**Datum herziening DEPIA (indien van toepassing)**

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2, 4, 5, 6

AANVULLING DEPIA MBT DATA-ETHIEK : 5.1.2i

Wie zijn betrokken bij DEPIA vanuit expertise
(bijv. ISO, juridische expertise, inkoop, procesontwerper etc.)

Functie	**Naam**
Projectleider	5.1.2e
Proceseigenaar	5.1.2e
Privacy Officer	5.1.2e
Inkoop	?
ISO	5.1.2e
FG	5.1.2e
Adviseur data-ethiek	5.1.2e
Informatieadviseur(s)	5.1.2e en 5.1.2e

Planning
Vul in wat van toepassing is voor het betreffende project.

	Taak	**Datum gereed**
Fase 1	Uitvoeren Pre-DEPIA	
	Beoordelen Pre-DEPIA door FG	
	Voorafgaande raadpleging van AP (indien van toepassing)	
Fase 2	Uitvoeren DEPIA; invullen door projectleider/beleidsmedewerker	
	Uitvoeren DEPIA; raadplegen PO	
	Uitvoeren DEPIA; raadplegen ISO	
	Uitvoeren DEPIA; raadplegen Adviseur data-ethiek	
Fase 3	Beoordeling door FG en Adviseur Data-ethiek	
	Indien van toepassing; uitvoeren moreel beraad of inzetten data-ethische commissie.	
	Reflectie op de data-ethische waarden vanuit moreel beraad of data-ethische commissie toevoegen aan DEPIA	
	Indien van toepassing; aanpassen DEPIA	
	Beoordeling door FG en Adviseur Data-ethiek	
Fase 4	Eindbeoordeling bestuur/MT/Proceseigenaar	
	Opslaan documenten (Pre-DPIA, DEPIA)	
	Bepalen mate van vertrouwelijkheid documenten	
	Toesturen documenten naar FG	
	Herziening DEPIA inplannen (3 jaar na datum definitieve versie DEPIA)	

1. Baten

Bij baten kun je denken aan vrijheid, welzijn, welvaart, duurzaamheid, inclusiviteit en diversiteit, gelijkheid, efficiëntie en kostenreductie. (Deze brede benadering is belangrijk, omdat ethische en juridische aspecten invloed kunnen hebben op de relatie tussen onze organisatie en de omgeving)

1.1: Wat zijn de baten voor gemeente Leeuwarden als organisatie?

In vergelijking met 5.1.2i heeft 5.1.2i verschillende functionaliteiten die het MOL-meldingsproces verbeteren en dat zijn de volgende drie factoren: 1. 5.1.2i kan meer gestroomlijnde en efficiënte workflow bieden voor het verwerken van meldingen, waardoor de reactietijd van de gemeente op overlast en problemen wordt verkort. 2. Het is gebruiksvriendelijker dan 5.1.2i, waardoor de medewerker en stakeholders gemakkelijker meldingen kunnen maken, beheren en opvolgen. 3. Een overzicht van alle meldingen en de status ervan, waardoor de gemeente beter geïnformeerd is over de situatie in onze gemeente. Al deze aspecten leveren een bijdrage aan een efficiënter en effectiever meldingsproces vergeleken met 5.1.2i.
Advies FG: Akkoord
Adviseur data-ethiek: Geen toevoegingen verder

1.2: Wat zijn de baten voor het individu?

Vergeleken met 5.1.2i kan de burger de volgende voordelen ervaren wanneer wij gebruik van 5.1.2i maken voor het melden van overlast: - Met 5.1.2i kunnen wij meldingen sneller opvolgen en oplossen, wat resulteert in een snellere reactie op overlastsituaties. Dit betekent dat burgers minder lang hoeven te wachten voordat hun meldingen worden behandeld, waardoor ze zich sneller geholpen voelen. Het bevordert een veiligheidsgevoel. - Wanneer het mol-team optimaal 5.1.2i weet in te zetten, kan de burger geüpdatet worden van de status van de meldingen, om eventuele vragen of zorgen te bespreken. Hierdoor wordt het gevoel van betrokkenheid en transparantie vergroot bij de burgers. - Doordat 5.1.2i de taakefficiëntie van het MOL-team verbetert, kunnen meldingen sneller worden verwerkt en opgelost. Dit betekent dat burgers minder lang hoeven wachten op een reactie of oplossing voor hun meldingen.
Advies FG: Akkoord
Adviseur data-ethiek: Geen toevoegingen verder

1.3: Wat zijn de baten voor de Leeuwarder samenleving als geheel?

- De taakefficiëntie die 5.1.2i biedt aan het MOL-team helpt bij het verbeteren door het meldingsproces te stroomlijnen en te automatiseren. Hierdoor kunnen medewerkers hun tijd effectiever besteden aan het oplossen van overlastsituaties, waardoor er minder personeelsuren nodig zijn voor het afhandelen van meldingen. - De administratieve lasten kunnen beter worden georganiseerd door het hebben van een meldingsbeheersysteem, waardoor de administratieve lasten voor het beheren en verwerken van meldingen worden verminderd. Minder tijd besteed aan administratieve taken kan resulteren in lagere operationele kosten voor de gemeente. - Door sneller te kunnen reageren op meldingen van overlast, kan 5.1.2i helpen bij het voorkomen van langdurige en ernstigere overlastsituaties. Dit kan uiteindelijk leiden tot kostenbesparingen (bijvoorbeeld doordat er minder middelen nodig zijn voor herstelwerkzaamheden), een groter gevoel van veiligheid en een groter gevoel van betrokkenheid bij onze inwoners.
Advies FG: Akkoord
Adviseur data-ethiek: Geen toevoegingen verder

2. Verantwoording; Is het doel en hoe het doel wordt bereikt juridisch en ethisch verantwoord?

Beschrijf de invloed die het gebruik van gegevens of techniek heeft/kan hebben op menselijke en maatschappelijke waarden en belangen.

Wanneer de verwerking invloed heeft op de data-ethische waarden, betekent dit vaak dat de belangen van stakeholders geschaad worden. Dit kan richting geven aan de beoordeling of een toepassing data-ethisch verantwoord is. Hieronder staan de ethische waarden, die voor gemeente Leeuwarden van belang zijn.

- ***Rechtvaardigheid:***
  We dragen bij aan rechtvaardigheid, gelijke kansen en inclusiviteit. Onze digitale oplossingen zijn laagdrempelig en waardevol voor iedereen. We zijn alert op het voorkomen van ongewenste vooringenomenheid bij de selectie van data. Ook letten we erop dat er geen discriminatie, stereotypering of vooroordelen in algoritmes zit (bias).

- ***Menselijke waardigheid:***
  We behandelen bewoners, ondernemers en bezoekers als mensen, niet als 'nummer'. Onze digitaliseringstrajecten sluiten aan bij de leefwereld en behoeften van de mensen in onze gemeente. De mens is altijd leidend , niet de techniek/data.

- ***Privacy:***
  We beschermen de privacy van inwoners, ondernemers en bezoekers. Data van inwoners worden geanonimiseerd gebruikt en zijn niet herleidbaar tot een persoon. We gebruiken 'Privacy by design' en doen onderzoek naar de impact van digitaliseringstrajecten op de privacy.

- ***Veiligheid:***
  We waarborgen de openbare orde en veiligheid, zodat iedereen zich veilig voelt in onze gemeente. We beveiligen onze data. Via cybersecurity bereiden we ons voor op digitale aanvallen.

- ***Autonomie:***
  We respecteren menselijke autonomie (vrijheid). We vermijden onbewuste beïnvloeding, manipulatie en stimulering van dwangmatig gedrag of overheidstoezicht ('Big Brother'). We zijn terughoudend met het gebruik van data waarmee we gebruikers kunnen volgen, hun reputatie schaden of hun toekomst negatief kunnen beïnvloeden.

- ***Controle over technologie:***
  We controleren op natuurlijke momenten of onze digitaliseringstrajecten nog goed werken. Door open en transparant om te gaan met data en informatie, kan iedereen deelnemen op basis van dezelfde kennis en inzichten.

- ***Kwaliteit van leven/duurzaamheid:***
  We vinden gezond en duurzaam leven belangrijk in Leeuwarden. We zoeken naar duurzame oplossingen waarbij de gezondheid van inwoners, ondernemers en bezoekers voorop staat. We toetsen of digitale oplossingen echt meerwaarde hebben voor de gemeente.

- ***Mienskip:***
  We vinden de bescherming van de gemeenschap belangrijk. We zorgen ervoor dat onze digitale toepassingen aansluiten op het gevoel van mienskip. We streven ernaar dat groepen inwoners en ondernemers vertrouwen hebben in de gemeente en onze digitaliseringstrajecten.

2.1: Welke van de eerder genoemde waarden worden beïnvloed of geraakt door het project/proces? (bespreek alle bovenstaande waarden. En benoem bij 3.3 de risico en de maatregelen.)
Beoordeel in de onderstaande vragen of er één of meerdere waarden zijn die mogelijk geraakt worden door het project/proces. (Als de waarde negatief wordt geraakt, neem deze dan op in de risico's bij vraag 11.3 en 11.4)

Veiligheid en Rechtvaardigheid Veiligheid: Dit wordt bevorderd door middel van snellere respons op veiligheidsmeldingen, zoals defecte straatverlichting, of in de toekomst straatintimidatie. Rechtvaardigheid: Draagt bij aan gelijke toegang tot diensten, aangezien meldingen vanuit verschillende wijken op een dezelfde manier wordt behandeld. Menselijke waardigheid: bij valse meldingen (dit staat los van 5.1.2i, maar heeft te maken met proces van doen van meldingen. Voor de aandacht voor privacy wordt verwezen naar de DPIA, voor risico's zie vraag 3.3.
Advies FG: Akkoord
Adviseur data-ethiek: Geen toevoegingen, als in 3.3 de risico's zijn opgenomen.

3. Afweging;

Afweging van alle onderdelen in het kader van ethiek, privacy en informatieveiligheid.

3.1: Kan hetzelfde doel op een andere manier worden bereikt (subsidiariteit)? Leg uit waarom wel/niet.

Nee, niet op dezelfde wijze. Hoewel de binnen Leeuwarden gebruikte applicatie 551122i ook een deel van de functionaliteiten als 5.1.2i heeft, sluit dit onvoldoende aan op de eisen en werkwijze van MOL ten aanzien van het organiseren van haar processen en het uitvoeren van de werkzaamheden.
Advies FG: Akkoord

3.2: Kan hetzelfde doel met minder gegevens worden bereikt (proportionaliteit)? Leg uit waarom wel/niet.

De vastlegging van informatie in 5.1.2i en gedurende het proces is beperkt tot dat wat noodzakelijk en ter zake dienend is ter uitvoering van de werkzaamheden van MOL. Het is belangrijk om te benadrukken dat de verzameling van deze gegevens beperkt blijft tot wat strikt noodzakelijk of anderszins ter zake dienend is voor de behandeling van de melding. Hieronder vallen ook foto's of video's. Hoewel hieruit mogelijk meer gegevens af te leiden zijn dan een melder in reguliere zin dient in te vullen via het meldformulier, is deze informatie uiterst relevant voor het beoordelen van overlastmeldingen, de ernst daarvan, en het aan de hand daarvan afstemmen of escaleren met andere afdelingen of partijen. De beelden worden op eenzelfde wijze beschermd als andere persoonsgegevens en ook enkel gebruikt voor de doeleinden zoals hierboven beschreven.
Advies FG: Helder omschreven, de overige zaken rondom bewaren en bewaartermijnen komen terug in de DPIA.

3.3: Wat zijn de negatieve gevolgen en de genomen maatregelen voor de betrokkenen (Benoem de gevoel van een inwoner en de gevolgen. Bedenk dingen op de proces op de waarde en rechtvaardig)

Beschrijf en beoordeel risico's van de voorgenomen gegevensverwerkingen voor de de waarden vanuit vraag 2.1;

Negatieve gevolgen	Oorzaak hiervan	Kans op gevolgen	Impact van gevolgen	Maatregel	Geïmplementeerd door
1.Privacy gevolgen	Het delen van locatiegegevens	Midden	Hoog	Toegang alleen voor team-MOL.	Gemeente Leeuwarden
2.Weerstand burgers delen van gegevens	Digitale onzekerheid	Laag	Laag	Anoniem meldingen doen	Gemeente Leeuwarden
3. Mogelijke weerstand tegen verandering	Gebrek aan training en ondersteuning	Midden: weerstand tegen verandering is dat medewerkers niet goed worden betrokken bij het implementatieproces van 5.1.2i	Midden: weerstand tegen verandering kan leiden tot vertragingen in het meldingsproces en verminderde productiviteit van medewerkers, waardoor de voordelen van 5.1.2i niet volledig worden gerealiseerd	De gemeente kan ervoor zorgen dat medewerkers voldoende training en ondersteuning krijgen bij het gebruik van 5.1.2i, zodat ze zich comfortabel voelen bij de nieuwe technologie.	Gemeente Leeuwarden en Leverancier 5.1.2i
4. Technische problemen	Een gebrek aan geschikte IT-infrastructuur	Midden: technische problemen zijn mogelijk, vooral tijdens de initiële implementatie van 5.1.2i of bij updates van het systeem.	Hoog: technische problemen kunnen de efficiëntie van het meldingsproces verminderen en de reactietijd van de gemeente op overlastmeldingen vertragen, wat de tevredenheid van burgers kan verminderen.	Het verbeteren van de IT-infrastructuur kan helpen om technische problemen met 5.1.2i te voorkomen en een soepele implementatie en werking van het systeem te garanderen.	Leverancier 5.1.2i
5. Doen van valse meldingen	Dit kan gedaan worden als grap, uit wraak of om anderen te schaden	laag	Hoog	Het invoeren van een verificatieproces om de authenticiteit van meldingen te verifiëren voordat ze worden verwerkt. Dit kan bijvoorbeeld	Gemeente Leeuwarden

				inhouden dat burgers hun identiteit moeten verifiëren of dat meldingen worden geverifieerd aan de hand van andere bronnen. (Een mogelijke werkwijze die voorgesteld kan worden aan het MOL-team). Melders dienen achternaam, postcode en telefoonnummer door te geven. Aan de hand van deze gegevens kan het MOLteam een verificatie doen in de 5.1.2i (andere bron). Ook vind er altijd een eerste gesprek plaats alvorens een melding wordt omgezet tot een aanpak.	
6. Meldingen worden gebruikt om bepaalde groepen te discrimineren of te stigmatiseren, wat kan leiden tot onrechtvaardige behandeling.	Melders melden vanuit een discriminerende gedachtegang.	Midden	Hoog	Beleid doorvoeren dat discriminatie verbiedt en procedures voor het onderzoeken en behandelen van meldingen waarbij sprake is van discriminatie. In 5.1.2i werken wij met een persoonsgerichte aanpak. MOL selecteert hierin op gedrag en niet op eigenschappen waarop gediscrimineerd kan worden.	Gemeente Leeuwarden
7. Het verwerken van meldingen kan mogelijk leiden tot inbreuken op de privacy van individuen, vooral als persoonlijke gegevens onjuist worden gebruikt of gedeeld	De meldingen die ontvangen worden, worden direct als waarheid beschouwd en daarop ook als zodanig gehandeld.	Laag	Hoog	Wij delen sfeerbeelden met bijv. ketenpartners. Meldingen zijn niet op feitelijkheden gebaseerd, maar deze sfeerbeelden kunnen wel door ketenpartners gecheckt worden op feitelijkheden.	Gemeente Leeuwarden

8. Het verwerken van meldingen kan mogelijk leiden tot inbreuken op het gevoel van privacy, als het persoonlijke meldingen betreft)	Benoeming van gedragingen van een beklaagde in de AVG brief	Midden	Midden	Zo feitelijk mogelijk benoemen van de gemelde overlast.	Gemeente Leeuwarden
Advies FG: Akkoord indien aanvullingen worden gedaan en maatregelen ingezet.					
Adviseur data-ethiek: Goede aanvullingen, punten 5-8 moeten nog besproken worden en aangevuld. Dit is iets voor de afdeling zelf om te doen, niet voor de IM-adviseur.					

3.4: Zijn er rest-risico's en zo ja, welke? Leg ook uit waarom.

N.v.t.
Advies FG: Akkoord
Adviseur data-ethiek: Akkoord

Eindoordeel Functionaris voor Gegevensbescherming: **Datum:**

Beoordeling (door management/bestuur)	**Is de beoordeling openbaar, vertrouwelijk, zeer vertrouwelijk of geheim**

Waar wordt de beoordeling opgeslagen

Startdatum verwerkingen (indien van toepassing)	**Wanneer bijwerken register (indien van toepassing)**	**Datum herziening DEPIA (indien van toepassing)**

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2, 4, 5, 6

Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 14058

Gemeente Leeuwarden

GM E M O

Aan:	Gemeentesecretaris gemeente Leeuwarden
Van:	Functionaris Gegevensbescherming
Datum:	5 februari 2026
Onderwerp:	Advies voor inrichting dashboard voor Afas
Registratienummer:	2026-005736

Doel van het advies

Een zo compleet mogelijk beeld te geven van de risico's en mogelijkheden bij de inrichting van een dashboard voor managers, waarbij persoonsgegevens onderdeel daarvan zijn. Door dit zo compleet mogelijk beeld de gemeentesecretaris een besluit te kunnen laten nemen over de inrichting van het dashboard.

Vraag aan gemeentesecretaris

-Geeft het advies een compleet beeld van de risico's en mogelijkheden voor de inrichting van het dashboard vanuit Afas?
-Kunt u op basis van dit advies een besluit nemen over de inrichting van het dashboard?

Context

Al enige tijd wordt er gewerkt aan de inrichting van dashboards met gegevens vanuit Afas via de inzet van Power BI. Deze dashboards bieden de managers een hulpmiddel voor inzicht in onderwerpen als formatie en bezetting, verlof en verzuim. Omdat deze gegevens uit Afas komen, is er sprake van actuele en betrouwbare stuurinformatie.

Daarbij is de wens, om zoveel als mogelijk informatie weer te geven en beschikbaar te stellen voor alle managers; niet alleen voor inzicht, maar ook om van elkaar te kunnen leren. Bijkomend voordeel daarvan is, dat het inrichten van het dashboard daarmee eenvoudiger wordt.

Bij de start van het project is verzuimd om privacy mee te laten denken bij de inrichting van de dashboards. Daardoor kwam het project bij mij pas in beeld, toen de inrichting zo goed als klaar was. Daarbij heb ik aangegeven dat op bepaalde onderdelen informatie inzichtelijk maken tot op persoonsniveau voor álle managers niet past bij de vereisten vanuit de AVG. Mij is verteld dat de inrichting zó is, dat een onderdeel alleen voor iedereen inzichtelijk kan zijn, of voor niemand. Dus alle managers kunnen ofwel alles zien tot op medewerker niveau ofwel alleen op teamniveau.

Mij is nu gevraagd om vanuit de toezichthoudende rol advies te geven, waarna er een besluit kan volgen rondom de definitieve inrichting, omdat de informatie vanuit Afas persoonsgegevens betreft van alle medewerkers op het gebied van functieschaal en salaris, verlof en verzuim.

Provincie Groningen

Tijdens de gesprekken is mij verteld dat Provincie Groningen dezelfde inrichting heeft en dat daar wel alle managers alle informatie konden inzien. Navraag bij de privacy officer van de Provincie Groningen leerde mij dat zij het dasboard als volgt hebben ingericht:

-Formatie en bezetting tot op functienaam (HR21) inzichtelijk voor alle managers, P&O en financieel adviseurs;
-Verlof en verzuim voor alle managers, P&O financieel adviseurs inzichtelijk op teamniveau;
-Verlof en verzuim voor P&O inzichtelijk tot op persoonsniveau.

Daarmee is de inrichting zodanig, dat er voldaan wordt aan de vereisten vanuit de AVG en is er voldoende inzicht om met elkaar in gesprek te gaan. Zowel voor managers onderling als voor managers met eigen teamleden en P&O als ondersteuning daarbij.

Vereisten vanuit de AVG (art 5; de grondbeginselen)

Dit artikel bevat de beginselen van verwerking van persoonsgegevens:

1. Rechtmatigheid, behoorlijkheid en transparantie; persoonsgegevens moeten op een rechtmatige, eerlijke en transparante manier worden verwerkt.
2. **Doelbinding**; gegevens mogen alleen worden verzameld voor specifieke, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Ze mogen niet verder worden verwerkt op een manier die onverenigbaar is met die doeleinden.
3. **Minimale gegevensverwerking** (dataminimalisatie); alleen de persoonsgegevens die **noodzakelijk** zijn voor het doel van de verwerking mogen worden verzameld.
4. Juistheid; persoonsgegevens moeten correct zijn en, indien nodig, worden bijgewerkt. Onjuiste gegevens moeten zonder vertraging worden gewist of gecorrigeerd.
5. Opslagbeperking; gegevens mogen niet langer worden bewaard dan nodig is voor het doel of zoals wettelijk is bepaald in bijvoorbeeld de Archiefwet.
6. **Integriteit en vertrouwelijkheid**; persoonsgegevens moeten op een manier worden verwerkt die een passende beveiliging garandeert, inclusief bescherming tegen **onbevoegde** of onrechtmatige verwerking, verlies, vernietiging of schade.
7. Verantwoordingsplicht; de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze beginselen en moet dit kunnen aantonen.

Advies voor de inrichting

Het dashboard wordt op 3 verschillende onderdelen ingericht, elk met hun eigen informatie en gevoeligheid van de persoonsgegevens. Rekening houdend met de grondbeginselen vanuit de AVG, is mijn advies per onderdeel hieronder weergegeven en in de tabel opgenomen wat dan voor alle managers getoond wordt in Afas.

1.1 Informatie over formatie en bezetting

Salaris valt onder financiële gegevens en wordt vanuit de AVG gezien als een gevoelig persoonsgegeven. Daarbij hoort dat je als organisatie extra maatregelen (zoals beveiliging) treft voor de verwerking daarvan. Daar staat tegenover dat gegevens over een functie en de daarbij horende functieschaal binnen een gemeente vindbaar zijn. Mijn advies om hier wel zorgvuldig mee om te gaan, en de weergave te beperken tot de functienaam vanuit de HR21-systematiek. Dat geeft voldoende informatie en doet zoveel als mogelijk recht aan de privacy van de medewerkers.

Onderstaande gegevens zijn dan inzichtelijk in het dashboard voor alle managers:

Teamniveau:	**Persoonsniveau:**
Formatie in FTE en bedragen	Functienaam volgens HR21
Bezetting in FTE en bedragen	Functieschaal
Functies volgens HR21	Loonschaal

1.2 Informatie over verlof

Omdat er bij verlof sprake kan zijn van verschillende soorten verlof en daarmee dus ook sprake kan zijn van gevoelige gegevens (zoals zorgverlof), adviseer ik deze gegevens alleen beschikbaar

te stellen op teamniveau. Het dashboard laat dan voor alle managers alleen gegevens zien op teamniveau, zonder dat dit direct herleidbaar is naar een medewerker.

Onderstaande gegevens zijn dan inzichtelijk in het dashboard voor alle managers:

Teamniveau:	**Persoonsniveau:**
Hoeveelheid verlof	

1.3 Informatie over verzuim
Verzuim zegt iets over gezondheid en is daarmee een bijzonder persoonsgegeven. Bijzondere persoonsgegevens mogen alleen worden verwerkt, als daarvoor een uitzondering geldt, zoals in art.9 AVG staat. Opname in een dashboard voor alle leidinggevenden hoort daar niet bij. Mijn advies is dan ook, om informatie over verzuim alleen op teamniveau weer te geven in het dashboard.

Onderstaande gegevens zijn dan inzichtelijk in het dashboard voor alle managers:

Teamniveau:	**Persoonsniveau:**
Percentage verzuim	
Aantal verzuimmeldingen	
Verzuim- en betermeldingsfrequentie	
Aantal personen verzuim	

De beperking van de huidige inrichting vraagt dan ook, dat de eigen teamleider een dashboard kan verkrijgen voor verlof en verzuim via M&O, die wel inzage heeft in alle onderdelen.

Overige zaken
Verder adviseer ik om periodiek (3-6 maandelijks) autorisaties te controleren, zodat iemand die niet langer leidinggevende is, geen toegang meer heeft tot informatie waartoe deze niet langer bevoegd is.

Tenslotte is het van belang om bewaartermijnen in te regelen, als dat van toepassing mocht zijn. Er moet voorkomen kunnen worden, dat er nog gegevens in het dashboard staan van personen die niet langer in dienst zijn (of dat er rapportages opgeslagen kunnen worden).

Advies Functionaris voor Gegevensbescherming

Aan
Openbare Orde en Veiligheid

Datum
10 maart 2025

Van
Functionaris voor Gegevensbescherming

E-mail
FG@rotterdam.nl, FG@leeuwarden.nl, FG@utrecht.nl

Onderwerp
Advies t.a.v. DPIA - OOV - Digitale Meldplicht, Versie 1.0 Definitief

Kopie

Bijlagen
Geen

Conclusie

Ten aanzien van de Digitale Meldplicht en de daarbij gewenste toe te passen technische middelen is uitvoerige documentatie aangelegd door de verschillende betrokken partijen. Zo heeft het Ministerie van J&V een concept DPIA uitgevoerd op het deel van de verwerking dat zij en haar diensten uitvoeren. Heeft de gemeente Utrecht een ethiek-assessment (Uthiek) uitgevoerd en heeft de gemeente Leeuwarden een concept DEPIA (DPIA+Ethiek) opgesteld.

Uit deze documentatie komen echter ook tegenstrijdige uitgangspunten naar voren ten aanzien van rollen van de betrokkenen partijen en grondslagen voor gegevensverwerking. Daarnaast signaleren we tekortkomingen en onbekendheden die een risico vormen voor de naleving van de beginselen uit artikel 5 AVG. Deze tegenstrijdigheden, tekortkomingen en onbekendheden kunnen in de praktijk ook leiden tot uitvoeringsproblemen die een significante impact kunnen hebben op de bescherming van persoonsgegevens en de rechten en vrijheden van de betrokkenen.

Hieronder zetten we onze bevindingen en aanbevelingen nader uiteen.

We adviseren om de aanbevelingen op te volgen, met alle betrokken partijen samen een aangepaste gezamenlijke DPIA op te stellen, en de daaruit voortkomende maatregelen te implementeren alvorens de gegevensverwerking te starten. Wij ontvangen daarnaast graag een reactie op de aanbevelingen waaruit blijkt hoe de organisaties aan de aanbevelingen opvolging geven en een afschrift van de aangepast DPIA.

Bevindingen en Aanbevelingen

Grondslag

- Uit de beschikbare documentatie (zoals de DEPIA van de gemeente Leeuwarden, de DPIA van het Ministerie van J&V en de Uthiek-assessment van de gemeente Utrecht) blijkt dat de verschillende betrokken partijen andere grondslagen als uitgangspunt hanteren voor de gegevensverwerking: in het bijzonder de uitvoering van een publiekrechtelijke taak versus toestemming. De gehanteerde grondslag kan veel invloed hebben op andere aspecten van de gegevensverwerking, zoals transparantieverplichtingen, passende technische en organisatorische maatregelen of de noodzaak om ook reële en juridisch houdbare alternatieve oplossingen aan te bieden.

  Aanbeveling: Adresseer met de betrokken partijen de tegenstrijdige grondslagen, de gevolgen en de risico's daarvan.

Beginselen

- Uit de documentatie blijkt dat de exacte geolocatie wordt verzonden van de mini-ID naar het landelijke rekencentrum. Onduidelijk blijft waarom dit noodzakelijk is en waarom er niet gekozen is voor een minder inbreukmakende werkwijze, zoals een on device check van de geolocatie tegen de locatie van het gebiedsverbod.

  Aanbeveling: Licht toe waarom de gekozen inrichting van de verwerking de meest passende is in het kader uitgangspunten zoals privacy by design, dataminimalisatie, proportionaliteit en subsidiariteit.

Transparantie

- Uit de documentatie blijkt niet dat er een wettelijke uitzondering is op de transparantieverplichtingen uit artikel 12 tot en met 34 AVG. Desondanks voldoet het gehanteerde 'Informatieblad Mini-ID' niet deze transparantieverplichtingen en blijkt uit de documentatie dat de betrokken partijen buiten dit informatieblad geen inspanningen wensen te verrichten om aan de transparantieverplichtingen te voldoen.

  Aanbeveling: Pas de informatievertrekking zo aan dat aan de transparantieverplichtingen wordt voldaan.

Belangenafweging

- De richtsnoeren schrijven voor dat de verwerkingsverantwoordelijke zo mogelijk een vertegenwoordiging van de betrokkenen moet overwegen te betrekken bij de DPIA. Uit de documentatie blijkt dat de belangen / houding / standpunt van betrokkenen en hun netwerk t.o.v. digitale meldplicht bij de betrokken partijen onbekend zijn. Ze worden voorondersteld.

  Aanbeveling: Onderzoek op welke manier (een vertegenwoordiging namens) de betrokkenen bij het DPIA-proces betrokken kunnen worden zodat hun belangen en afwegingen beter meegewogen kunnen worden in de belangenafweging bij het bepalen van een passende verwerking van persoonsgegevens. Kijk daarbij behalve naar de primaire doelgroep van de pilot ook naar andere doelgroepen waarop de maatregel op termijn ook toegepast zou (kunnen) gaan worden.

Beveiliging (beschikbaarheid, integriteit en vertrouwelijkheid)

- Een risicoanalyse ten aanzien van de informatiebeveiliging van de technische oplossing ontbreekt. Daarbij kan onder andere gedacht worden aan de opslag van de 'vingerafdruk' op de mini-ID en het via RF, GPS en WIFI bepalen en verzenden van de geolocatie van de betrokkene naar het landelijke rekencentrum.

  Aanbeveling: Voer een risicoanalyse ten aanzien van de informatiebeveiliging van de technische oplossing uit. Denk daarbij met name aan de mini-ID en de gegevensuitwisseling met het centrale rekencentrum.

- De verantwoordelijkheden van de verwerkingsverantwoordelijke, de verwerker en de betrokkene bij technisch falen wordt niet verder uitgewerkt in de stukken. De gevolgen van het technische falen van het systeem worden vrij eenzijdig bij de betrokkenen neergelegd, terwijl deze nauwelijks invloed heeft op de situatie. . Dit creëert een juridische kwetsbaarheid voor de betrokkene.

  Aanbeveling: Werk heldere mitigerende maatregelen uit. Beschrijf voor elke maatregel welke partij verantwoordelijk is voor de implementatie, de uitvoering en het beheer van de maatregel. Onderzoek of deze partij praktisch en juridisch gezien ook in staat is of wordt gesteld om deze verantwoordelijkheid in de praktijk in te vullen.

- **(Juridische) rollen van betrokken partijen**
  Uit de beschikbare documentatie blijkt dat de verschillende betrokken partijen elkaar andere (juridische) rollen toekennen ten aanzien van de gegevensverwerking.

  Voor het feitelijk handhaven van een reguliere fysieke meldplicht heeft de burgemeester het gezag over de politie. Verwerking van persoonsgegevens vindt dan mogelijk plaats onder het regime van de Wet politiegegevens (Wpg). Onduidelijk blijft of de burgemeester voor de feitelijke handhaving van de digitale meldplicht ook gebruik hoort te maken van de politie en of de verwerking van persoonsgegevens dat onder het regime van de Wpg zou vallen. Volgens de Wpg is de werkgever dan de verwerkingsverantwoordelijke. In dit geval zou dat dan de korpschef zijn. In dat geval zou het mogelijk de politie zijn die met het Ministerie van J&V afspraken moet maken over de inzet van Mini-ID.

  Verder wordt bijvoorbeeld de partij 5.1.2i enerzijds als verwerker van de gemeenten aangeduid en anderzijds als subverwerker van het Ministerie van J&V. Een ander voorbeeld is de politie die enerzijds als zelfstandig verwerkingsverantwoordelijke en anderzijds als verwerker wordt aangeduid.

  Daarmee verschuiven verantwoordelijkheden tussen partijen, waarbij uit de DPIA niet duidelijk wordt of ze die verantwoordelijkheden ook kunnen invullen. Daarvan kan bijvoorbeeld sprake zijn als contractuele relaties die niet overeenkomen met de juridische rollen die aan de partijen worden toegedicht of met de feitelijke uitvoeringsrelatie tussen de partijen.

  Aanbeveling: Adresseer met de betrokken partijen de tegenstrijdige rollen, de gevolgen en risico's daarvan. Bekijk ook of de AVG of de Wpg van toepassing is bij de feitelijke handhaving van de digitale meldplicht en adresseer in dat licht de relatie gemeente – politie – Ministerie van J&V.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	4

Gegevens-verwerking	Wanneer de gemeente geen duidelijk beeld heeft van de operationele processen waarin persoonsgegevens worden verwerkt kan dit leiden tot ongecontroleerde en mogelijk onrechtmatige verwerkingen. Door het ontbreken van een duidelijk overzicht en inzicht in de operationele processen kan de gemeente niet of niet voldoende aantonen dat de verwerkingen van de persoonsgegevens in overeenstemming met de AVG worden uitgevoerd (art.24 lid 1 AVG). * Dit kan leiden tot risico's voor betrokkenen, n.l. risico voor de rechten en vrijheden van personen indien persoonsgegevens onbedoeld worden gedeeld, gewijzigd of verloren raken. * Dit kan leiden tot risico's voor de gemeente op slechte datakwaliteit, hoge kosten door het nemen van verkeerde beslissingen.	Controleer of alle operationele processen waarbij persoonsgegevens worden verwerkt, in beeld zijn.	**Methode van beoordeling** Documentatie Interview X Waarneming ter plaatse

Beschrijving controle onderdeel	**Methode van beoordeling**	**functie**	**Datum**	**Bevindingen en reacties**
Controle deel van het proces binnen Inkomen en Zorg, betrekking hebbende op vragen om extra informatie betreffende de informatieplicht	Interview	kwaliteitsmedewerker	15-07-2025	**Bevindingen:** -In door gemeente verzonden brieven (inkomen en zorg en Team financiële ondersteuning) wordt gevraagd BSN in onderwerpregel te zetten. -In door gemeente verzonden brieven staat niet standaard de optie van beveiligd mailen. -In door gemeente verzonden brieven staat niet vermeld dat onbeveiligd mailen een risico betekent voor de betrokkene -Door gemeente verstuurde brieven wordt via post verstuurd, terwijl betrokkene berichtenbox heeft aangevinkt. -In door gemeente verzonden brieven staat geen uitleg over beveiligd mailen (wel/niet wachtwoord, waar wachtwoord naar toe sturen) -De door gemeente verstuurde brieven zijn niet in eenvoudige taal geformuleerd. **Reacties:** -Medewerkers worden erop gewezen om BSN-nummer niet in brieven te gebruiken. Dat betekent ook dat zij niet mogen vragen aan betrokkenen om het BSN volledig in de onderwerpregel te zetten. -Nieuwe collega's krijgen iets van onboarding, welke wordt ge-update. De laatste versie is niet bekend bij de kwaliteitsmedewerker.

				-De training AVG in Vogelvlucht kan worden ingezet voor kennisvergroting. -In de standaard brieven staat naast de optie van beveiligd mailen altijd het emailadres van het betreffende team. Als gemeente moeten we meerdere opties van communicatie geven. -Als een brief via 5.1.2i @leeuwarden.nl wordt verstuurd, komt deze eerst bij DIV terecht, welke deze dan doorstuurt naar de werkvoorraad van het team. Tussen aankomst bij DIV en de werkvoorraad is het de consulenten niet duidelijk dat een document daadwerkelijk is verstuurd. Dat is wel na te gaan, zodra een document is ontvangen in het team. Dan is een datum van verzending en ontvangst terug te vinden. -Meestal is er geen vertraging tussen DIV en de werkvoorraad. Mocht een document met wachtwoord zijn beveiligd, welke nog niet bekend is, kan er vertraging optreden omdat DIV dan via de betrokkene het wachtwoord moet opvragen. -Om een brief via de berichtenbox te versturen, is een extra handeling nodig, welke maximaal 10 seconden extra tijd vraagt. -Er is veel gestandaardiseerd in de processen. Mocht het proces niet goed verlopen zijn er mogelijkheden voor de medewerkers om dit aan te kaarten. Dit kan in teamoverleg of via kwaliteitsmedewerker.

Advies:

- Wijs medewerkers erop dat vragen om het volledige BSN-nummer in de onderwerpregel te plaatsen, niet wenselijk is, gezien de risico's bij onbeveiligd verzenden van allerlei documenten die gevoelige of bijzondere persoonsgegevens bevatten. Dit lijkt een algemeen voorkomend verschijnsel, omdat in brieven van 2 verschillende teams dit verzoek is aangetroffen.
- Richt een standaard inwerkprogramma, danwel onboarding in, waarin aandacht is voor hoe gemeente Leeuwarden omgaat met het verwerken van persoonsgegevens.
- Maak beveiligd versturen van documenten die persoonsgegevens bevatten de standaard in brieven.
- Leg het principe van beveiligd versturen van documenten uit en regel een emailadres waarnaar het wachtwoord verstuurd kan worden.
- Zorg ervoor dat brieven naar de berichtenbox worden verstuurd, als de betrokkene dat als voorkeurskanaal heeft aangegeven.
- Pas brieven aan naar B1-niveau, zodat betrokkenen de inhoud beter begrijpen.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	2

DEPIA Centrale Toegang en Regie Maatschappelijke Opvang (v.4.5)

Wie zijn betrokken bij DEPIA vanuit expertise
(bijv. ISO, juridische expertise, inkoop, procesontwerper etc)

Functie	**Naam**
Projectleider	5.1.2e / 5.1.2e
Proceseigenaar	5.1.2e
Privacy Officer	5.1.2e
Inkoop	5.1.2e
ISO	5.1.2e / 5.1.2e
FG	5.1.2e
Adviseur data-ethiek	5.1.2e

Planning
Vul in wat van toepassing is voor het betreffende project.

	Taak	**Datum gereed**
Fase 1	Uitvoeren Pre-DEPIA	
	Beoordelen Pre-DEPIA door FG	
	Voorafgaande raadpleging van AP (indien van toepassing)	
Fase 2	Uitvoeren DEPIA; invullen door projectleider/beleidsmedewerker	
	Uitvoeren DEPIA; raadplegen PO	
	Uitvoeren DEPIA; raadplegen ISO	
	Uitvoeren DEPIA; raadplegen Adviseur data-ethiek	
Fase 3	Beoordeling door FG en Adviseur Data-ethiek	
	Indien van toepassing; uitvoeren moreel beraad of inzetten data-ethische commissie.	
	Reflectie op de data-ethische waarden vanuit moreel beraad of data-ethische commissie toevoegen aan DEPIA	
	Indien van toepassing; aanpassen DEPIA	
	Beoordeling door FG en Adviseur Data-ethiek	
Fase 4	Eindbeoordeling bestuur/MT/Proceseigenaar	
	Opslaan documenten (Pre-DEPIA. DEPIA)	
	Bepalen mate van vertrouwelijkheid documenten	
	Toesturen documenten naar FG	
	Herziening DEPIA inplannen (3 jaar na datum definitieve versie DEPIA)	

1. Algemeen
Beschrijf het doel, de inrichting en de stakeholders bij het voorgestelde project/proces/experiment

1.1: Wat wil je bereiken met het proces/project? (wat is het doel)
Geef aan welk(e) doel(en) de organisatie met de (nieuwe of gewijzigde) werkprocessen wil bereiken en/of binnen welke context deze gezien moet(en) worden.

Centrale Toegang en Regie Maatschappelijke Opvang (CT&R)

De CT&R maakt deel uit van de Brede Aanpak Dakloosheid (BAD) in Friesland. De CT&R start als pilotproject. De pilotfase duurt tot en met 31 december 2025 met de mogelijkheid om de pilot met een jaar te verlengen. De CT&R zal tijdens de pilotfase ook een kantoor hebben in de Algemene Opvang van Wender aan de Nieuweweg 3 te Leeuwarden. Wender, Leger des Heils en, Limor doen mee aan de pilot.

De insteek is dat na de pilotfase de CT&R structureel geborgd wordt. Onderdeel van de pilot is om tot een besluit te komen over de borging van de CT&R na afronding van de pilotfase. De CT&R valt gedurende de pilotfase onder de verantwoordelijkheid van het Sociaal Domein Fryslân.

De CT&R voor de maatschappelijke opvang in Friesland is gericht op het centraliseren van de toegang tot de voorzieningen voor maatschappelijke opvang in Friesland. De CT&R omvat de aanmelding, inclusie, plaatsing, intake, casemanagement en uitstroomcoördinatie. Gemeente Leeuwarden is centrumgemeente.

Het doel van de CT&R is:
Centraliseren en uniformeren van de manier waarop mensen zich kunnen aanmelden voor- en toegang verkrijgen tot maatschappelijke opvang in Friesland en het voeren van regie op toeleiding naar een passend vervolg door middel van case management en uitstroomcoördinatie.

Door het:
- uitvoeren van het onderzoek conform de Wmo 2015 gericht op het nemen van een besluit omtrent het verzoek tot maatschappelijke opvang.
- op cliënt niveau in kaart brengen van de zorg- en ondersteuningsbehoeften van dak- en thuislozen teneinde daarvoor een ondersteuningstraject in te zetten onder regie van medewerkers van de CT&R en in samenwerking met daarbij betrokken ketenpartners, waaronder zorgaanbieders, gemeenten en woningcorporaties
- versterken van de positie van dak- en thuislozen door hen goed te informeren, te adviseren, waar nodig opvang te bieden, toe te leiden naar passende zorg- en ondersteuning en door randvoorwaarden te creëren op basis waarvan effectief gestart kan worden met maatschappelijk herstel, waaronder zelfstandig wonen.
- tegengaan van versnippering van de gegevensverwerking en ontwikkelen van een actueel overzicht van het aantal dak- en thuislozen in Friesland
- aanmelden en registreren van bank hoppende (dreigend dakloze) jongvolwassenen waar het Jongeren Interventie Team bij betrokken is
- inzichtelijk krijgen van de behoefte aan-, het aanbod van- en de leemten in de verschillende vormen van zorg- & ondersteuning al dan niet in combinatie met zelfstandig wonen of verblijf in een instelling in Friesland
- opheffen van knelpunten, belemmeringen, vertragingen en stagnaties die zich voordoen tijdens het opvangtraject, die daardoor uitstroom uit de maatschappelijke opvang verhinderen of anderszins niet tot gewenste oplossingen leiden.

5.1.2i 5.1.2i nder andere door Amaryllis. Ten behoeve van de CT&R is voor de toegang tot de maatschappelijke opvang een nieuw zaaktype ontwikkeld, welke d.d. 22 september 2023 in preproductie is genomen.

Alle (dreigend) dakloze mensen kunnen zich aanmelden bij de CT&R. Alleen als een aanmelding leidt tot inclusie als (dreigend) dak- of thuisloze wordt in 5.1.2i een volledige zaak gestart. Overige gevallen worden gelijk afgesloten of doorverwezen naar het wijk- of gebiedsteam van de verantwoordelijke gemeente.

De pilot CT&R heeft een grote samenhang met de pilot Jongeren Interventieteam (JIT) uit de BAD. Het JIT richt zich op het outreachend werken met kwetsbare jongvolwassenen. Het betreft jongvolwassenen die van bank naar bank hoppen en dreigen op straat te belanden. Het JIT is op afroep beschikbaar voor gemeenten op het moment dat zij er niet meer uitkomen. Jongeren kunnen zich ook rechtstreeks wenden tot het JIT. Het JIT stemt in dat geval af met de gemeente (wijk- of gebiedsteam)

over het vervolg. Als er sprake is van dakloosheid en daarmee behoefte aan maatschappelijke opvang wordt er toegeleid naar de CT&R.

Advies FG: Uitgebreide omschrijving, geeft uitgebreid en compleet beeld van wat het doel is.

1.2: Hoe werkt het precies?
Beschrijf het systeem, de applicaties, de in- en output, of er acties worden gedaan zonder tussenkomst/beoordeling van de mens (maak een plaatje van het proces).

In de huidige situatie ligt de toegang tot de maatschappelijke opvang bij de verantwoordelijke zorgaanbieders (i.c. Wender, Leger des Heils en Limor). Personen melden zich rechtstreeks bij een zorgaanbieder voor opvang en/of een briefadres en regelmatig bij verschillende zorgaanbieders tegelijkertijd of volgtijdelijk. De zorgaanbieder besluit zelfstandig of er wel/geen opvang wordt geboden of dat er een briefadres wordt verstrekt. De afweging daartoe verschilt per aanbieder. Daarbij wordt er geen beschikking verleend zoals dat bij andere Wmo voorzieningen wel het geval is. De betrokken zorgaanbieders hanteren hun eigen methodieken voor wat betreft casusregie en trajectbegeleiding. Individuele ondersteuningsplannen en/of zorgplannen worden opgesteld door de zorgaanbieders zelf en zijn niet bekend bij gemeentelijke toegangen.

De CT&R doorbreekt de huidige situatie door het proces van aanmelding, intake, toegang en trajectregie te centraliseren en uniformeren voor de maatschappelijke opvang. Daarvoor wordt een nieuwe organisatie opgezet die onder de verantwoordelijkheid van SDF/gemeente Leeuwarden komt te vallen. Deze nieuwe organisatie is de Centrale Toegang en Regie (CT&R). Het bestaande Transferpunt gaat op in de CT&R.

De CT&R bestaat uit een team van medewerkers die deels in dienst zijn van SDF/gemeente Leeuwarden en medewerkers in dienst van Wender, Leger des Heils en Limor. De medewerkers van de zorgaanbieders worden uitgeleend/gedetacheerd aan/bij SDF/gemeente Leeuwarden. Hiervoor worden separate overeenkomsten gesloten. Alle medewerkers krijgen een werkaccount van de gemeente Leeuwarden waarmee toegang wordt verleend tot het gebruik van de verschillende a_plicaties die binnen gemeente Leeuwarden beschikbaar zijn (bijvoorbeeld 5.1.2i en de 5.1.2i).

Ten aanzien van maatschappelijke opvang wordt onderscheidt gemaakt tussen:
1. Eerste opvang
2. Verlengde opvang

Eerste opvang
De eerste opvang volgt op de eerste intake door de aanmeldfunctionaris en duurt in principe maximaal 2 weken. Gedurende de eerste opvang wordt onderzocht of een persoon in aanmerking komt voor Verlengde opvang in Friesland of niet. Het inclusie besluit voorziet in Eerste opvang en een casemanager voert de uitgebreide intake uit en neemt een vervolg besluit over Verlengde Opvang.

Landelijke toegankelijkheid
Wettelijk is geregeld dat alle ingezetenen van Nederland zich voor maatschappelijke opvang mogen melden bij alle gemeenten in Nederland. Dit fenomeen is de landelijke toegankelijkheid van de maatschappelijke opvang. Indien mogelijk moet een persoon dus worden opgevangen ook al komt die persoon niet uit de (in dit geval) de Friese regio. Daarnaast kan het zijn dat een persoon zich meld voor maatschappelijke opvang en is er ook aantoonbaar sprake van een crisissituatie die vraagt om acute opvang. Op dat soort momenten prevaleert het bieden van eerste opvang boven het volledig onderzoeken van het recht op een volledig opvangtraject.

Als blijkt dat de herkomst van een persoon buiten de Friese regio ligt en een persoon wel aanspraak kan maken op maatschappelijke opvang dan is maatschappelijke opvang in de regio van herkomst voorliggend. Het proces van warme overdracht wordt dan in gang gezet als de cliënt niet zelf in staat is zich te melden bij een opvanginstelling in de regio van herkomst. De plaatsingcoördinator neemt contact op met een contactpersoon in de regio van herkomst. Dit kan een medewerker zijn van de desbetreffende centrumgemeente, een centrale toegang of een opvangaanbieder. De casus wordt dan voorgelegd en besproken. De plaatsingcoördinator geeft daarbij aan dat zij afspraken wil maken om de warme overdracht te organiseren. Deze afspraken hebben betrekking op datum, tijdstip, vervoer naar-, ontvangst en opvang in een daarvoor beschikbare opvanginstelling. Ook kunnen er afspraken gemaakt worden over de eventuele vergoeding van kosten tussen regio's. In zijn algemeenheid zullen voor de Eerste opvang geen kosten in rekening gebracht worden bij de regio van herkomst. Eventuele vervoerskosten (trein, taxi of zorgvervoer) kunnen uit het doorbraakbudget worden gefinancierd.

Als het niet lukt om op minnelijke wijze afspraken te maken kan de plaatsingcoördinator opschalen naar de verantwoordelijk beleidsmedewerker bij SDF. De beleidsmedewerker kan dan in overleg treden met de collega beleidsmedewerker van de centrumgemeente van herkomst (https://vng.nl/artikelen/contactpersonen-landelijke-toegankelijkheid-bw-en-mo). Lukt het niet om tot overeenstemming te komen kan de casus worden voorgelegd aan de landelijke geschillencommissie (https://www.degeschillencommissiezorg.nl/over-ons/zorgcommissies/sociaal-domein-woonplaatsbeginsel-en-toegang/). Deze commissie zal een bindende uitspraak doen.

Verlengde opvang
Dat de maatschappelijke opvang landelijk toegankelijk is wil niet zeggen dat een persoon zonder meer recht heeft op maatschappelijke opvang. En ook al heeft een persoon wel behoefte aan maatschappelijke opvang, dat wil niet zeggen dat deze maatschappelijke opvang zondermeer in Friesland moet plaatsvinden. Het recht op maatschappelijke opvang in Friesland wordt door de casemanager onderzocht gedurende de periode van Eerste opvang. Als uit het onderzoek blijkt dat een persoon recht heeft op maatschappelijke opvang in Friesland wordt door de casemanager een positief besluit over Verlengde opvang genomen. Als blijkt dat een persoon wel aanspraak kan maken op maatschappelijke opvang, maar daarvoor terecht kan in de regio van herkomst dan wordt door de casemanager een negatief besluit genomen over Verlengde opvang. Vervolgens moet deze persoon warm overgedragen worden naar een opvanginstelling in de regio van herkomst. Om de warme overdracht te faciliteren draagt de casemanager de casus over aan de plaatsingcoördinator. Als uit het onderzoek blijkt dat een persoon geen aanspraak kan maken op maatschappelijke opvang dan neemt de casemanager ook een negatief besluit over Verlengde Opvang en wordt de toegang tot de maatschappelijke opvang (zorgvuldig) beëindigd. Het traject kan dan worden afgesloten.

Verlengde opvang is voor bepaalde tijd. Het streven is om toe te groeien naar een gemiddelde opvangduur van maximaal 3 maanden. Tijdens de periode van Verlengde opvang heeft de casemanager de regie over het traject. Een persoon verblijft in deze periode in één van de Friese instellingen voor maatschappelijke opvang of staat ingeschreven op één van de daarvoor aangewezen briefadressen.

Fasen in traject maatschappelijke opvang
Een persoon die zich aanmeld bij de CT&R doorloopt een aantal fasen:
1. aanmeldfase
2. intakefase
3. trajectfase
4. uitstroomfase

Aanmeldfase
De aanmeldfase is de start van een traject. Een persoon meldt zich fysiek of telefonisch bij de CT&R en wordt te woord gestaan door de aanmeldfunctionaris. Tijdens deze fase wordt besproken of een persoon toegang krijgt tot de maatschappelijke opvang of dat er andere vormen van ondersteuning voorliggend zijn.

Bij de aanmelding wordt onderscheidt gemaakt tussen:
1. Dreigend dakloos, geen acute opvang nodig
2. Thuisloos, geen acute opvang nodig
3. Dakloos, (acute) opvang nodig
4. Niet (dreigend) dakloos, eventueel verwijzing nodig

De aanmelding is het begin van de intake. Het eerste deel van de intake wordt uitgevoerd door de aanmeldfunctionaris. De aanmeldfunctionaris start een zaak in 5.1.2i. De aanmeldfase wordt afgesloten met een besluit over wel of geen inclusie voor Eerste opvang. Bij inclusie wordt afhankelijk van de situatie de casus overgedragen aan de plaatsingcoördinator of gelijk aan een casemanager.

Als een persoon zich niet kan identificeren, niet ingeschreven staat in de 5.1.2i of rechtmatig in Nederland verblijft kan er geen zaak worden gestart in 5.1.2i. Een persoon kan dan in principe niet geïncludeerd worden. Afhankelijk van de situatie zal de persoon gevraagd worden om zich later opnieuw aan te melden. Als de persoon aangeeft niet (meer) te beschikken over een identiteitsbewijs zal de persoon op reguliere wijze moeten proberen een identiteitsbewijs te verkrijgen. De CT&R is niet verantwoordelijk voor het bieden van ondersteuning bij het verkrijgen van een identiteitsbewijs.

De aanmeldfase duurt in beginsel niet lang en kan binnen een uur afgerond worden. Het is wel afhankelijk van de situatie. Ook in de huidige praktijk kunnen er soms weken overheen gaan voordat een aanmelding is afgerond. Zolang een aanmelding niet is afgerond wordt er geen inclusie besluit genomen en blijft de casus “hangen” in de aanmeldfase.

Intakefase
De intake begint al bij de aanmelding. Als een persoon wordt geïncludeerd (toegang krijgt tot de maatschappelijke opvang) wordt de casus overgedragen aan de casemanager. Elke cliënt krijgt een casemanager aan zich eko eld. De casemanager voert vervolgens een uitgebreide intake uit door alle zaakstappen in 5.1.2i te doorlopen en de benodigde gegevens te registreren. De intakefase wordt afgesloten met een besluit over Verlengde opvang. Afhankelijk van de situatie stemt de casemanager af met de plaatsingcoördinator over het starten van een warme overdracht naar de regio van herkomst of de plaatsing in een (andere) opvanginstelling binnen Friesland. Dit laatste is bijvoorbeeld aan de orde als een persoon voor de Eerste opvang in de Nachtopvang heeft geslapen en voor de verlengde opvang een plek krijgt in de Algemene Opvang.

De intakefase mag gemiddeld niet langer duren dan twee weken. Het is in het belang van de cliënt om zo snel mogelijk duidelijkheid te krijgen over het vervolgtraject. Tijdens de intakefase wordt de woonhistorie van de cliënt gecheckt in de 5.1.2i om vast te stellen waar iemand vandaan komt, waar iemand voor het laatst zelfstandig heeft gewoond en hoe lang dat geleden is. Met name als er sprake is van herkomst buiten de regio Friesland is het noodzakelijk dat zo snel mogelijk gestart wordt met de warme overdracht om te voorkomen dat een cliënt zich wortelt in Friesland. Ook in verband met het aanvragen van uitkeringen en dergelijke kan niet lang gewacht worden met het nemen van een besluit over Verlengde opvang. De intakefase wordt afgesloten met het opstellen van een ondersteuningsplan.

Ondersteuningsplan
Het ondersteuningsplan is een bekend fenomeen in het Sociaal Domein. Het is gebruikelijk dat toegangsorganen als onderdeel van het onderzoek naar de behoefte aan ondersteuning op grond van de Wmo 2015 een ondersteuningsplan opstellen. In het ondersteuningsplan worden doelen en resultaten omschreven en dit uitgesplitst naar de verschillende levensgebieden. Het ondersteuningsplan bevat algemene persoonsgegevens en gegevens die betrekking hebben op de voorgeschiedenis van de cliënt. Het kan dan gaan om informatie over huisvesting, financiën, het psychosociaal functioneren, dagelijks functioneren etc.. Waar het ondersteuningsplan vooral op ingaat is wat het beoogde resultaat is van de in te zetten ondersteuning (i.c. maatschappelijke opvang). Wat is er nodig om van de huidige situatie (dakloosheid) naar een toekomstige situatie (verblijf in een eigen thuis) te gaan? Gebruikelijk is dat het ondersteuningsplan tot stand komt in dialoog met de cliënt en dat zowel de cliënt als de casemanager het plan ondertekenen.

Het ondersteuningsplan wordt gedeeld met de zorgaanbieder waar de cliënt wordt opgevangen. De zorgaanbieder wijst een eigen trajectbegeleider aan die verantwoordelijk is voor de dagelijkse begeleiding. De trajectbegeleider en de casemanager trekken nauw samen op gedurende het opvangtraject. De trajectbegeleider van de zorgaanbieder stelt in overleg met de cliënt een zorgplan op waarin de doelen uit het ondersteuningsplan (praktisch) worden uitgewerkt. Het zorgplan wordt niet gedeeld met de CT&R en wordt niet opgeslagen in 5.1.2i. Wel checkt de casemanager of er door de zorgaanbieder een zorgplan is opgesteld.

Trajectfase
Is éénmaal een positief besluit genomen over de inclusie in de maatschappelijke opvang kan het traject om weer uit te stromen echt van start gaan. De casemanager stelt op basis van de intake een ondersteuningsplan (het wat) op waarin doelen en resultaten worden geformuleerd. Stabilisatie en toeleiding naar uitstroom zijn kerndoelen. Zo weet de cliënt wat er van hem of haar wordt verwacht en waar hij of zij op kan rekenen. De cliënt is op dat moment ondergebracht bij een zorgaanbieder en beschikt ook over een interne trajectbegeleider. De casemanager en de trajectbegeleider stemmen gedurende het traject af over de voortgang van het traject. De trajectbegeleider stelt samen met de cliënt een zorgplan (het hoe) op.

Het streven is dat een traject gemiddeld niet langer duurt dan drie maanden. Dat is Eerste opvang inclusief Verlengde opvang. In de praktijk zal het niet altijd mogelijk zijn om binnen 3 maanden uitstroom te realiseren. Succesvolle uitstroom hangt samen met het de mogelijkheden van de cliënt zelf en is afhankelijk van externe factoren. Omstandigheden die van invloed zijn op uitstroom zijn onvoorziene en onbekende feiten (verzwegen/onbekende schulden, niet gediagnostiseerde verstandelijke beperking, psychiatrische stoornis, verslaving etc.) bij de cliënt. Externe factoren kunnen te maken hebben met wachtlijsten bij wijk- en gebiedsteams, plaatsgebrek bij intramurale zorginstellingen, het ontbreken van woningen etc.

Uitstroomfase
Elk traject wordt afgesloten omdat een cliënt kan uitstromen. Hoewel de ondersteuning gedurende het hele opvangtraject gericht is op uitstroom zal in de eerste fase van het opvangtraject de focus vooral liggen op stabilisatie en observatie. Met het laatste wordt bedoeld wat heeft een cliënt aan

problematiek. Problematiek kan zich voordoen op verschillende levensgebieden. Aan het begin van een traject is meestal niet goed in te schatten wat de aard en omvang de problematiek is en is een oordeel daarover mede afhankelijk van de observatie door de trajectbegeleider en de casemanager.

Zodra een cliënt is gestabiliseerd en er een zo volledig mogelijke observatie is geweest wordt ingezet op het toeleiden naar uitstroom. De ondersteuning van de cliënt richt zich dan vooral op het vinden van een (vervolg)plek. Op basis van de intake en de observatie wordt door de casemanager een uitstroomprofiel bepaald. In essentie zijn er twee uitstroomvarianten:

1. de cliënt gaat zelfstandig wonen
2. de cliënt gaat niet zelfstandig wonen

Als de cliënt zelfstandig kan wonen dan is de inzet van de casemanager gericht op uitstroom naar zelfstandig wonen. Meestal zal dit een sociale huurwoning van een woningcorporatie betreffen. De ervaring leert dat een cliënt meestal niet lang genoeg staat ingeschreven bij een woningcorporatie om regulier een woning toegewezen te krijgen. In dergelijke gevallen kan een cliënt bemiddeld worden. Om het proces van bemiddeling in gang te zetten stemt de casemanager af met de uitstroomcoördinator. De uitstroom met bemiddeling wordt door de casemanager overgedragen aan de uitstroomcoördinator. De uitstroomcoördinator wordt daarbij door de administratie ondersteunt. Het beheer van de 5.1.2i zal door de administratie worden uitgevoerd.

Als de cliënt niet zelfstandig gaat wonen dan is de inzet van de casemanager gericht op toeleiding naar een vorm van intramuraal verblijf bij een zorgaanbieder. Intramuraal verblijf heeft meestal één van de onderstaande grondslagen:

- Beschermd wonen op grond van de Wmo
- Beschermd wonen op grond van de Wlz
- Klinisch verblijf op grond van de Zvw
- Forensisch verblijf op grond van een rechterlijke uitspraak en gefinancierd door het ministerie van Justitie.

Overige uitstroomvarianten zijn:

- Overlijden
- Detentie
- Vertrek op eigen kracht (al dan niet in wederzijds overleg)
- Vertrek met onbekende bestemming

Ten behoeve van de uitstroom niet zelfstandig wonen stemt de casemanager af met de trajectbegeleider op de aanpak. Primair is het de taak van de trajectbegeleider om zaken in gang te zetten, zoals bijvoorbeeld de aanmelding bij een wijk- of gebiedsteam van een gemeente voor het onderzoek naar beschermd wonen, of de aanmelding bij het CIZ voor een Wlz indicatie.

Zodra er een woning is toegewezen of als er een beschikking of indicatie is afgegeven en de cliënt is uitgestroomd kan het traject worden beëindigd.

Rollen in de CT&R

In de praktijk kunnen medewerkers van de CT&R meerdere rollen uitvoeren. De rollen zoals die zijn gedefinieerd hangen sterk samen met de fase van het opvangtraject. De rollen van Aanmeldfunctionaris en Plaatsingcoördinator zullen in de praktijk gecombineerd uitgevoerd worden. Per rol zijn er meerdere medewerkers aangesteld om daarmee minder kwetsbaar te zijn, taken te verdelen, volledige bezetting gedurende de werkweek te waarborgen en over vervanging bij ziekte en verlof te beschikken.

Binnen de CT&R zijn de volgende rollen vertegenwoordigd:

1. Aanmeldfunctionaris
2. Plaatsingcoördinator
3. Casemanager
4. Uitstroomcoördinator
5. Administratie
6. Team coördinatie
7. Cliënt

Aanmeldfunctionaris

De aanmeldfunctionaris “neemt de telefoon op”. Een persoon meldt zich bij de aanmeldfunctionaris, dit kan zowel telefonisch als aan de balie. Het eerste contact van een cliënt is met de aanmeldfunctionaris. De aanmeldfunctionaris start indien nodig een nieuwe zaak. De aanmeldfunctionaris vraagt om een identificatie van de cliënt. De aanmeldfunctionaris kan de persoon eventueel ook ondersteuning aanbieden bij het contact leggen met relevante instanties. De

Aanmeldfunctionaris kan in schrijnende gevallen besluiten dat een persoon wel voor Eerste opvang in aanmerking komt zonder dat er een inclusiebesluit hoeft te worden genomen. De aanmeldfunctionaris neemt een inclusiebesluit en indien nodig een aanvullend besluit over Eerste opvang. Als blijkt acute opvang nodig is (anders slaapt de cliënt vannacht op straat) wordt de cliënt overgedragen naar de plaatsingcoördinator.

Plaatsingcoördinator
De plaatsingcoördinator heeft als taak om de (fysieke) plaatsing in een opvanginstelling te organiseren in een opvangvoorziening bij één van de Friese opvanginstellingen (van Wender of Limor) of in te schrijven op een briefadres (bij Leger des Heils of VNN). Daartoe stemt de plaatsingcoördinator af met de locatiemanager van de betreffende opvanginstelling. De beslissing van de plaatsingcoördinator is doorslaggevend. Zodra plaatsing een feit is houdt de betrokkenheid van de plaatsingcoördinator op en wordt de cliënt (administratief) overgedragen aan een casemanager. Indien een cliënt buiten de Friese regio opgevangen moet worden is het de taak van de plaatsingcoördinator om de cliënt warm over te dragen naar een opvanginstelling buiten de Friese regio.

Casemanager
Zodra een cliënt is geïncludeerd wordt er een casemanager gekoppeld aan de cliënt. De casemanager is verantwoordelijk voor het uitvoeren van een uitgebreide intake (het onderzoek zoals bedoeld in de Wmo). Op basis van de intake neemt de casemanager een besluit over Verlengde opvang. Als uit de intake blijkt dat de cliënt geen aanspraak kan maken op opvang in Friesland wordt het proces van warme overdracht in gang gezet. De casemanager draagt de cliënt dan weer over naar de plaatsingcoördinator. Blijkt uit de intake dat de cliënt in aanmerking komt voor opvang in Friesland wordt bepaald in welke opvanginstelling opvang het beste plaats kan vinden. De bevindingen uit de intake worden door de casemanager vastgelegd in een ondersteuningsplan. In het ondersteuningsplan worden doelen, resultaten en verplichtingen vastgelegd en afgesproken. De cliënt ondertekent het ondersteuningsplan voor gezien. Onderzocht wordt of op termijn er ook een beschikkin afgegeven moet worden aan de cliënt. Het ondersteuningsplan wordt opgeslagen in [redacted].

Een casemanager heeft een caseload van ca. 30-40 cliënten tegelijkertijd. De casemanager blijft gedurende het gehele traject betrokken bij de cliënt en voert de regie uit. De casemanager trekt nauw op met de trajectbegeleiders van de cliënten in de caseload van de casemanager. De casemanager faciliteert bij het oplossen van knelpunten die tijdens het traject kunnen ontstaan die de uitstroom vertragen of belemmeren. De zaak wordt door de casemanager in [redacted] afgesloten zodra opvang is beëindigd en de cliënt definitief is uitgestroomd. Na uitstroom is de casemanager beperkt beschikbaar voor nazorg.

Uitstroomcoördinator
De uitstroomcoördinator wordt door de casemanager betrokken zodra blijkt dat een cliënt kan uitstromen naar een eigen woning. De uitstroomcoördinator coördineert de afstemming met- en tussen zorgaanbieders, woningcorporaties en wijk- en gebiedsteams. In het bijzonder op het gebied van bemiddeling ziet de uitstroomcoördinator er op toe dat de afspraken uit het convenant Weer Thuis worden nageleefd. De uitstroomcoördinator is tevens verantwoordelijk voor de triagering voorafgaand aan de instroom in Duurzaam Verblijf te Engwierum en de Doorstroomwoningen te Leeuwarden. Daarnaast zal in de toekomst de uitstroomcoördinator ook verantwoordelijk worden voor de triagering/ toegang tot het Skills project te Leeuwarden.

Administratief medewerker
De administratief medewerker is verantwoordelijk voor de all round administratieve werkzaamheden in de CT&R. De administratief medewerker vult de cliënt dossiers aan in [redacted] en verzorgt de caseloadoverzichten voor de casemanagers en de uitstroomcoördinatoren. De administratief medewerker ondersteunt de Aanmeldfunctionaris tijdens de aanmeldin van een (nieuwe) cliënt. Daarnaast vult de administratief medewerker de diverse [redacted] in, beheert deze en houdt deze bij. De administratief medewerker staat ook ter beschikking van het JIT welke organisatorisch onder de CT&R komt te vallen.

Team coördinatie
De coördinator stuurt het team van de CT&R inhoudelijk aan en is verantwoordelijk voor de afstemming met de opdrachtgever (SDF) en de betrokken ketenpartijen. De coördinator vervult daarnaast ook werkzaamheden die bij de rol van casemanager horen. In de opstartfase van de pilot zal er wekelijks afstemming zijn tussen de coördinator, de teamleider SDF en de projectleiding BAD. Ook sluit de coördinator aan bij de periodieke afstemming tussen de teamleiders van de bij de pilot betrokken organisaties, waaronder SDF. De afstemming met de projectleiding en de teamleiders gaat over de voortgang van de pilot, de onderlinge samenwerken, knelpunten etc..

Cliënt
De cliënt meld zich vrijwillig aan bij de CT&R, is in staat om zelf een hulpvraag te stellen en voelt zich gemotiveerd om zich te laten ondersteunen. De cliënt meld zichzelf aan of wordt daarbij ondersteunt door een derde (iemand uit het netwerk, zorgaanbieder, wijk- of gebiedsteam medewerker, verwijzer, etc.). De cliënt is zelf verantwoordelijk voor het aanleveren van de gevraagde gegevens gedurende de intake en tijdens het traject. De cliënt tekent het ondersteuningsplan voor gezien en committeert zich aan de daarin gemaakte afspraken.

5.1.2i

Binnen de CT&R wordt gebruik gemaakt van 5.1.2i. 5.1.2i is het zaaksysteem waar in een zaaktype in zaakstappen (persoons)gegevens worden vast_ele_d. Voor de CT&R is een specifiek zaaktype ontwikkeld, namelijk “Toegang MO”. Binnen 5.1.2i wordt gewerkt met een autorisatiematrix. Per rol zijn de autorisaties/rechten voor het bekijken en bewerken van de zaakstappen vastgelegd. Alle zaakstappen worden doorlopen met tussenkomst van een mens , i.c. medewerker van de CT&R.

Binnen 5.1.2i is een koppeling met de 5.1.2i en dat is ook nodi_ omdat zonder deze koppeling er geen zaak kan worden gestart. Daarnaast worden in 5.1.2i gegevens aangevuld op basis van gekoppelde systemen, zoveel mogelijk op “dat” niveau. Bijvoorbeeld “dat” cliënt een beschikking heeft voor Beschermd Wonen, WLZ zorg of een andere vorm van maatschappelijke ondersteunin_ etc.. Er worden in het kader van de pilot CT&R geen nieuwe systemen gekoppeld aan 5.1.2i.

De cliënt weet welke gegevens worden verwerkt in 5.1.2i omdat deze gegevens afkomstig zijn van de cliënt zelf tijdens de intake. Bij sommige vragen in een zaakstap wordt de cliënt expliciet om toestemming gevraagd voor het contact opnemen met derden voor het opvragen van informatie. De vragen in het zaaktype waarbij toestemming moet worden verleend staan expliciet vermeld in de betreffende zaakstap. Dat de cliënt toestemming verleent om contact op te nemen met derden moet ook met “Ja” worden “aangevinkt” in de zaakstap. De toestemmingen worden samengevat in het ondersteuningsplan die de cliënt voor gezien tekent. Door middel van een documentsjabloon wordt het ondersteuningsplan gegenereerd. Zo weet de cliënt zelf waar toestemmin_ voor is verleend. Het voor gezien ondertekende ondersteuningsplan wordt aan het dossier in 5.1.2i toegevoegd.

Als de cliënt geen toestemming verleent voor het contact opnemen met derden beoordeelt de casemanager of dit doorslaggevend is bij het nemen van een besluit over Verlengde opvang. Als de casemanager geen voldragen besluit kan nemen over de aanspraak op Verlengde opvang kan het besluit genomen worden om geen Verlengde opvang te bieden. De cliënt kan dan de toegang tot de maatschappelijke opvang worden ontzegd. In schrijnende gevallen kan de casemanager besluiten om de fase van Eerste opvang te verlengen.

De cliënt wordt voorafgaand aan de intake en na afloo_ van de intake mondeling geïnformeerd over wat er met de gegevens wordt gedaan die in 5.1.2i worden verwerkt. Voor het Transferpunt is een folder ontwikkeld waarin cliënten geïnformeerd worden over wat er met de verwerkte gegevens wordt gedaan. Deze folder wordt aangepast naar de situatie van de CT&R en zal uitgedeeld worden aan de cliënten.

5.1.2i
5.1.2i is gekoppeld aan de 5.1.2i. Deze koppeling is nodig om een zaak te kunnen starten op een "bestaand" persoon. Bij het starten van een zaak wordt alleen het huidige adres van inschrijving "aan_etikt" maar wordt verder niet naar de woonhistorie van een persoon gekeken. Daarnaast wordt de 5.1.2i geraadpleegd door de Aanmeldfunctionaris, de Casemanager of de Administratief medewerker om de woonhistorie te reconstrueren en om de gemeente van herkomst te bepalen. Dit is nodig omdat in principe een dakloos persoon terugkeert naar de gemeente van herkomst. Het is namelijk niet zo dat het huidige adres van inschrijving of het voorlaatste adres van inschrijving ook daadwerkelijk het adres was waar een persoon voor het laatst zelfstandig woonde. Het kan bijvoorbeeld ook een instelling, briefadres of PI zijn geweest.

5.1.2i
Het werken in 5.1.2i is gericht op de veilige samenwerking tussen de op de betreffende cliënt betrokken medewerkers van de ketenpartners. Gemeente Leeuwarden sluit aan bij de DPIA (t.a.v. 5.1.2i li_aties 5.1.2i, 5.1.2i en 5.1.2i) van het Strategisch Leveringsmanagement (SLM) 5.1.2i van het Rijk. Ook werkt_emeente Leeuwarden aan een algemene DEPIA over het gebruiken van tools en applicaties van 5.1.2i 365 en een extra gecodeerd schild (dit is echter nog voorlopig nog niet aan de orde).

Richtlijnen persoonsgegevens en 5.1.2i:

Het SLM heeft een memo geschreven waarin ze adviseren om geen bijzondere persoonsgegevens uit te wisselen via [redacted], [redacted] of [redacted]. De CT&R volgt deze lijn.

Werkwijze:
Externe gebruikers worden door de CT&R medewerker als eigenaar van de [redacted]-omgeving via SSC Leeuwarden uitgenodigd voor de [redacted]-omgeving en aan een besloten kanaal gekoppeld. De koppeling komt tot stand o basis van werk e-mailadres en werkmobiele nummer en wordt geverifieerd door de [redacted]. Deze wordt gevraagd bij de koppeling en bij het openen van documenten. Elke deelnemer van het Team krijgt een vastgemaakt bericht te zien waarin nog eens wordt benoemd in de [redacted]-omgeving geen bijzondere persoonsgegevens mogen worden gedeeld.

[redacted] wordt gebruikt als communicatiemiddel en bevat alleen informatie van betrokkenen die in traject zijn. Documenten worden verwijderd uit de [redacted] kanalen zodra die niet meer nodi zijn voor de communicatie. Elke aanbieder, woningcoöperatie, afdeling of project heeft een eigen [redacted] kanaal.

Voordelen en overweging:
- De gedeelde informatie kan beter gekaderd worden. Er is nu één open invulveld (Stand van zaken) waarin medewerkers van de CT&R, zorgaanbieders en woningcorporatie informatie over het proces kunnen delen.
- Er staat bij dit invulveld nu expliciet dat hier geen bijzondere persoonsgegevens gedeeld moeten worden. Anders worden deze direct verwijdert.
- Er worden geen lijsten, formulieren of documenten heen en weer gemaild waardoor er meerdere versies in de omloo
- Het werken in [redacted] is minder foutgevoelig en het risico op datalekken is kleiner omdat er het [redacted] kanaal een beveiligde omgeving is.

Data analyse, monitoring sturin en verantwoording
De data zoals vastgelegd in [redacted] wordt gebruikt voor data analyse waarbij de data op geaggregeerd niveau inzichtelijk wordt gemaakt in [redacted]. In [redacted] worden dashboards gemaakt die door de medewerkers van de CT&R worden gebruikt om de caseload te managen. De dashboards die door de CT&R gebruikt worden bevatten wel naar personen herleidbare informatie. Door middel van autorisaties is geborgd dat alleen medewerkers van de CT&R hiervoor rechten hebben die gekoppeld zijn aan hun rol. Het werken met [redacted] vergemakkelijkt het caseloadmanagement op een manier die met [redacted] zelf niet goed mogelijk is. [redacted] wordt binnen de gemeente Leeuwarden voor heel veel onderwerpen gebruikt en is ook volledig intern in beheer waarmee de beveiliging optimaal geborgd is.

De dashboards zijn ook toegankelijk voor beleidsmedewerkers in dienst van gemeente Leeuwarden, waarbij rechten zodanig ingesteld worden dat er geen namen en BSN nummers zichtbaar zijn voor beleidsmedewerkers. De toegang tot de dashboards is voor rapportagedoeleinden en beleidsanalyse wenselijk en noodzakelijk. Management informatie bevat nooit informatie op persoonsniveau.

Het is met [redacted] mogelijk om rapportages op te stellen. Deze rapportages kunnen bijvoorbeeld trends en ontwikkelingen inzichtelijk maken of de situatie per gemeente. Een rapportage is een export vanuit [redacted] en is niet doorklikbaar naar de onderli gende database. Het gaat hierbij niet om rapportages op persoonsniveau. Bovendien is [redacted] niet van buitenaf (buiten het netwerk van de gemeente Leeuwarden) online toegankelijk. Ook heeft niet iedereen intern bij gemeente Leeuwarden toegang tot [redacted]. En niet iedereen die toegang heeft tot [redacted] heeft dezelfde rechten. Medewerkers hebben een beperkte rechten en autorisaties. Toestemming voor autorisatie binnen [redacted] verloopt via de manager van de medewerker.

Data analyse is gericht op verantwoording naar de colleges, raden en ambtelijke organisaties van de Friese gemeenten en betrokken ketenpartijen zoals zorgaanbieders en woningcorporaties. Daarnaast is data analyse bedoeld voor beleidsontwikkeling en evaluatie, inkoop, contractmanagement en productontwikkeling.

Bij de ontwikkeling en inrichting van het zaaktype MO in [redacted] is geanticipeerd op de aanlevering van data aan de gemeentelijke monitor Sociaal Domein (https://www.waarstaatjegemeente.nl/mosaic/dashboard/gemeentelijke-monitor-sociaal-domein) en het landelijke dashboard Actieplan Dakloosheid van het ministerie van VWS. Daarvoor is het op termijn mogelijk vereist om data door te geven aan het CBS. Zodra dit aan de orde is dan kan dit vrij eenvoudig opgeleverd worden via [redacted].

Advies FG: Akkoord. (over)compleet overzicht van het totale werkproces.

1.3: Hoe worden de persoonsgegevens gebruikt?
Beschrijf alle gegevensverwerkingen (Een verwerking is alles wat je met persoonsgegevens kunt doen: verzamelen, vastleggen, opslaan, bijwerken of wijzigen, opvragen, raadplegen, versturen, combineren, afschermen , vernietigen).

In 5.1.2i worden alleen die persoonsgegevens verzameld, vastgelegd, opgeslagen, bewerkt, bijgewerkt, gewijzigd, opgevraagd en geraadpleegd die nodig zijn om de identiteit van de cliënt vast te stellen, het netwerk van de cliënt in kaart te brengen, het uitstroomprofiel te bepalen, de ondersteuningsbehoefte te onderzoeken, het ondersteuningsplan op te stellen teneinde de regie op het traject te kunnen voeren gericht op maatschappelijk herstel.

De CT&R is als uitvoeringsorgaan onderdeel van de gemeenten. Formeel valt de CT&R onder centrumgemeente Leeuwarden. Centrumgemeente Leeuwarden heeft op grond van de Centrumregeling Sociaal Domein Fryslân de opdracht gekregen namens alle 18 Friese gemeenten om de wettelijke taken op het gebied van de maatschappelijke opvang en beschermd wonen uit te voeren. Deze taken zijn belegd bij het Sociaal Domein Fryslân (SDF). De CT&R valt gedurende de pilot periode onder de verantwoordelijkheid van het SDF. SDF is onderdeel van gemeente Leeuwarden. Tegelijkertijd is de CT&R van en voor alle Friese gemeenten.

Het doel van de gegevensdeling is het voorkomen van het opnieuw uitvragen van dezelfde gegevens door gemeentelijke afdelingen zoals wijk- en gebiedsteams, sociale zaken, burgerzaken, schuldhulpverlening, onderwijs, belastingen. Met andere woorden elke gemeentelijke afdeling die een taak heeft in het treffen van voorzieningen voor een cliënt. De cliënt wordt hierover vooraf geïnformeerd. Voor zover het wettelijk mag en er een grondslag voor is hoeft hiervoor geen toestemming gevraagd te worden. Wel zal de cliënt om toestemming worden gevraagd als die grondslag ontbreekt. Het vragen om toestemming gaat specifiek om het “contact opnemen door de medewerker van de CT&R met een specifieke hulpverlener of instantie die voor een specifiek onderdeel (bv. een schulden re eling) noodzakelijk is. Een loket waar je bij langs moet. Uitgangspunt is dat gegevensdeling als 5.1.2i aan de cliënt mogelijk/ wenselijk is om dat hiermee minder belasting is voor de cliënt in het herhaaldelijk opnieuw moeten vertellen van het verhaal. Indien de cliënt weigert toestemming te verlenen dan worden er geen gegevens gedeeld. De cliënt zal dan zelf de voor het specifieke loket de gevraagde gegevens delen.

Vanuit de CT&R wordt het ondersteuningsplan van een cliënt gedeeld met de zorgaanbieder waar de cliënt gaat verblijven. Hiervoor geeft de cliënt geen toestemming, maar tekent “voor gezien” het ondersteuningsplan. Zodra duidelijk is welke gebiedsteam(s) betrokken zijn bij een cliënt wordt het ondersteuningsplan gedeeld met het betreffende gebiedsteam ten behoeve van het onderzoek door het gebiedsteam naar benodigde vervolgondersteuning.

De werkwijze is dat een cliënt door een trajectbegeleider van de zorgaanbieder waar de cliënt verblijft wordt begeleid bij het langs de instanties gaan. De cliënt houdt hierbij zoveel mogelijk zelf de regie, de trajectbegeleider is echter wel verantwoordelijk voor de sturing hierop. Als er knelpunten ontstaan die de voortgang vertragen dan kan de trajectbegeleider de casemanager van de CT&R inschakelen om het knelpunt te bespreken en te verkennen wat er nodig is om een doorbraak te organiseren. Andersom kan de casemanager ook ongevraagd op basis van de voortgang, zoals besproken tijdens het caseloadoverleg, sturen op een actievere begeleiding door de trajectbegeleider en de gerichtheid van de begeleiding. Dit is de regierol van de casemanager. Daarbij kan de casemanager het aanbod doen om contact op te nemen met de betreffende instanties om de casus te bespreken en benodigde gegevens te delen. Cliëntgegevens kunnen functioneel gedeeld worden met derde partijen voor zover dit in het belang is van een vlotte en ongehinderde uitvoering van het traject. Persoonsgegevens die gedeeld worden zijn in beginsel naam en geboortedatum en eventueel BSN.

Partijen waarmee informatie contact opgenomen kan worden en waarmee informatie gedeeld kan worden zijn:
- Gemeenten, afdelingen burgerzaken, sociale zaken, onderwijs, participatie, veiligheid, schulden, armoede en vroegsignalering; voor het inschrijven op een briefadres, het aanvragen van een uitkering, het in gang zetten van regelingen op het gebied van schuldhulpverlening, armoedebestrijding, vroegsignalering schulden, dreigende uithuiszetting, huiselijk geweld
- Wijk- en gebiedsteams; voor het onderzoeken van de (ambulante) ondersteuningsbehoefte en het nemen van een besluit daarover.
- Zorgaanbieders die betrokken zijn bij de cliënt; voor het plaatsen in een opvanginstelling, het delen van het ondersteuningsplan, het voeren van het caseloadoverleg en ten behoeve van de uitstroomcoördinatie.
- Woningcorporaties; ten behoeve van de uitstroomcoördinatie bij bemiddeling
- Zorg- en Veiligheidshuis Friesland; ten behoeve van het maatwerkoverleg

- GGD Friesland; in het kader van de zorg in verband met de publieke gezondheid
- Bewindvoerders, mentoren en/of curatoren; in het kader van het gezag die betreffende instanties hebben op de persoon
- Schuldhulp instanties; ten behoeve van het onderzoek naar en de inzet van schuldhulp regelingen
- Zorgverzekeraar; ten behoeve van het onderzoek naar en inzet van verzekerde zorg en/of het (opnieuw) in verzekering nemen van cliënt.
- Eerstelijnszorg (huisarts, tandarts, apotheker etc.); voor het inschrijven als patiënt/ cliënt danwel het in behandeling nemen van de cliënt voor benodigde persoonlijke zorg.
- CIZ; voor het aanmelden van een cliënt voor het indiceren van (eventueel) benodigde langdurige zorg op grond van de Wlz.
- Het Zorgkantoor (het Matchpoint); voor afstemming over het onderzoek naar en de inzet van zorg en ondersteuning voor een cliënt
- ACT Team in geval van dakloze mensen met zeer complexe problematiek in combinatie met zorgmijdend gedrag
- De specialistische schil; bestaande uit (verpleegkundig) specialisten van de GGZ, Alliade en VNN, rondom de voorziening Duurzaam Verblijf (nu alleen nog maar in Engwierum) ten behoeve van de triagering voor instroom in Duurzaam Verblijf.
- Het Jongeren Interventie Team (JIT); in geval van (dreigende) dakloosheid van jongvolwassenen tot 27 jaar. Het JIT bestaat uit medewerkers van Jeugdhulp Friesland, Wender, het Zorg- en Veiligheidshuis en SDF.

Onderdeel van de pilot is om te onderzoeken met welke instanties het nodig is om mee af te stemmen om de voortgang van het uitstroomtraject er in te houden dan wel te versnellen.

De gegevens die in 5.1.2i worden verwerkt zijn afgeschermd voor mensen die niet geautoriseerd zijn om in 5.1.2i te werken. Hiervoor wordt aangesloten bij de bepalingen, afspraken, richtlijnen die voor alle 5.1.2i gebruikers van toepassing zijn. Mensen die niet geautoriseerd zijn om in MC te werken kunnen überhaupt niet inloggen en hebben dus geen toegang tot de gegevens. 5.1.2i is alleen via gewhiteliste ip-ranges te benaderen. Daarnaast is per zaak in te richten welke autorisaties er zijn en ook per zaakstap kan de toegang worden beperkt.

Medewerkers CT&R hebben geen eigen toe_an_ tot andere systemen dan waarvoor zij geautoriseerd zijn. 5.1.2i . Op de klantpagina in 5.1.2i is DAT informatie inzichtelijk. In de autorisatieprofielen, die zijn gekoppeld aan zaaktypes, is in te stellen of medewerkers CT&R bij een cliënt kunnen zien, opstarten, bewerken en/of raadplegen. Deze autorisaties worden aan medewerkers CT&R wel/niet toegekend. Als er geen autorisatieprofiel is toegekend voor een bepaald zaaktype, zal de betreffende medewerker niets kunnen zien van dat zaaktype.

Conform de wettelijke bewaartermijnen zullen de gegevens in 5.1.2i na verloop van de wettelijke bewaartermijnen worden vernieti_d_ met uitzonderin_ van de_e_evens die voor data 5.1.2i gegevens verwijderd kunnen worden. De data die nodig_ is voor gegevensanalyse algemeen, dus niet op persoonsniveau_zal_eanonimiseerd worden opgeslagen in het DWH-dataWareHouse. Alle gegevens in 5.1.2i van alle zaaktypen worden in DWH opgeslagen via een dagelijkse verwerking na anonimisatie. Dit om de gegevensanalyse (geanonimiseerd) van alle jeugd, Wmo etc. zaken te doen op een niveau van wijk, straat, zaaktype. In de tijd worden deze gegevens dus gebruikt voor management rapporten en zor_anal_ses_Dit gebeurt in het DWH en dat zal dus geen last hebben van verwijderde gegevens uit de 5.1.2i -applicatie/database.

De persoonsgegevens worden dus:
- Opgevraagd door raadplegen bij de bron (de cliënt en betrokken zorgaanbieders of instanties).
- Opgeslagen en verwerkt in 5.1.2i , 5.1.2i en 5.1.2i).
- Bijgewerkt als een cliënt opnieuw wordt aangemeld of als er een mutatie optreed in de situatie van de cliënt
- Gecombineerd bij complexe aanvragen of in contact met ambtenaren/consulenten. Bij complexe vraagstukken zoals schulden, werkeloosheid en Jeugdzorg zal altijd de normale wettelijke grondslag worden gebruikt.
- Gegevens worden ingevoerd en gelezen door de medewerkers van de CT&R die daarvoor geautoriseerd zijn.
- Gegevens die nodig zijn voor de aanvraag van andere voorzieningen aan cliënt, of waar sprake is van wettelijke taken dan wel voorzieningen die het maatschappelijk herstel van de cliënt bevorderen danwel daarin randvoorwaardelijk zijn worden gedeeld met daartoe gerechtigde functionarissen.

Eventuele uitgaande brieven naar cliënten worden gearchiveerd in 5.1.2i. Daarbij kan gedacht worden aan beschikkingen.
Advies FG: Duidelijk en compleet overzicht van de verschillende verwerkingen.

1.4: Welke stakeholders zijn betrokken? (klant/client/inwoner, leveranciers, eindgebruikers en andere belanghebbenden)
Maak een stakeholderanalyse omtrent rol, positie en verwachtingen/wensen:
(verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger; vraag bij twijfel de privacy officer)

Stakeholder	Rol	Positie	Verwachtingen/wensen
Inwoner	Betrokkene	Voorstander/-tegenstander	Krijgt toegang tot voorziening voor opvang en een traject gericht op maatschappelijk herstel. De CT&R draagt bij aan de mogelijkheid dat de inwoner maar 1 keer zijn/ haar verhaal hoeft te doen. De Inwoner kan weerstand voelen om gegevens te delen vanuit een ervaring of gevoel van wantrouwen richting instanties in het algemeen en de overheid in het bijzonder. De extra kwetsbare positie van de Inwoner als gevolg van dakloosheid maakt de afhankelijkheid groter. Dit kan een ervaring of gevoel van gebrek aan eigen regie oproepen.
Medewerker CT&R	Gebruiker	Voorstander	Overzichtelijk systeem om integraal een dossier samen te stellen gericht op doelmatige en efficiënte uitvoering van een traject waardoor opvang zo lang als nodig en zo kort mogelijk kan worden geboden. Noodzakelijk ten behoeve van een goede samenwerking tussen CT&R, cliënt, gemeenten, zorgaanbieders en andere ketenpartijen.
Team coördinator	Proceseigenaar	Voorstander	Krijgt voor zijn medewerkers een integraal cliënt registratie systeem.
ICT	Functioneel beheer en record beheer	Neutraal	Verwacht een eenvoudig te beheren systeem.
Data analist	5.1.2i 5.1.2i naar dashboards t.b.v. analyse en sturing	Neutraal	Verwacht dat data in 5.1.2i eenvoudig te gebruiken is voor het bouwen van dashboards
Beleidsmedewerker	Afstemmen met coördinatie CT&R ten behoeve van beleidsevaluatie en verantwoording.	Voorstander	Beschikt over data waarmee beleid, inkoop, rapportage en verantwoording uitgevoerd kan worden
College van B&W	Verwerkingsverant-woordelijke, eindverantwoordelijk voor verwerking	Voorstander	Eenvoudiger en/of sneller voldoen aan wettelijke taak om in opvang te voorzien en ondersteuning te bieden. Overzicht van de aantallen in dak- en thuislozen (zie doel van verwerking)
Zorgaanbieder (Wender, Limor, Leger des Heils).	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Wenst een uniform Toegangsproces en reductie van de administratieve last. Wordt ontlast op het punt van de toegang, het uitvoeren van dubbele intakes.

Wijk- of gebiedsteam (van alle Friese gemeenten)	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Wenst inzicht in dakloosheid in de gemeente en om op persoonsniveau af te kunnen stemmen over in te zetten ondersteuning.
Woningcorporatie (alle in Friesland werkzame woningcorporaties)	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Verwacht in het kader van een aanvraag bemiddeling bij woningtoewijzing inzicht in de identiteit van woningzoekende, huidig adres, herkomstgemeente, huishoudensgrootte en betrokken zorgaanbieder
Gemeenten (diverse afdelingen)	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Wil inwoners ondersteunen met voorzieningen op het gebied van schuldhulpverlening, inkomen en ondersteuning bij zelfredzaamheid en participatie.
Zorg- en veiligheids-huis Friesland	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Wil personen waar sprake is van complexe veiligheidsproblematiek i.c.m. dakloosheid effectief maatwerk bieden.
GGD Friesland	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Wil personen waar sprake is van (onverzekerde) gezondheidsproblematiek en/of onbegrepen gedrag effectief maatwerk bieden
Bewindvoerders, mentoren en/of curatoren	Betrokkene in de plaats van inwoner	Voorstander	Wil namens personen die onder bewind of curatele staan of gementord worden effectief in staat gesteld worden om voor deze personen effectieve passende vervolgstappen te nemen.
Schuldhulpinstanties	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Willen hun diensten aan inwoners kunnen bieden en daarvoor zo laagdrempelig mogelijk toegankelijk zijn.
Zorgverzekeraar	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Hebben de taak om personen in verzekering te nemen teneinde rechtmatig aanspraak te kunnen maken op verzekerde zorg.
Eerstelijnszorg (huisarts, tandarts, apotheker, etc.)	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Willen laagdrempelig toegankelijk zijn voor personen die zorg nodig hebben maar daar niet/minder aanspraak op (kunnen) maken vanwege dakloosheid.
CIZ	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Heeft de taak om te beoordelen of personen aanspraak kunnen maken op langdurige zorg en daar een indicatie voor af te geven.
Het Zorgkantoor	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Is verantwoordelijk voor het beschikbaar hebben van voldoende aanbod van passende langdurige zorg door dit in te kopen.
ACT Team	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Heeft als taak om met zorgwekkend zorgmijdende dakloze personen contact te leggen en een vertrouwensband te creëren op basis waarvan effectief toegeleid kan worden naar een passende vorm van zorg- en ondersteuning in combinatie met verblijf.
Specialistische schil	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Heeft als taak om in specifieke casuïstiek te adviseren en diagnosticeren omtrent de toeleiding naar Duurzaam Verblijf

			en is ter consultatie van de medewerkers Duurzaam Verblijf beschikbaar.
Jongeren Interventie Team	Ketenpartner (Verstrekker/ontvanger)	Voorstander	Heeft als taak om met bankhoppende jongvolwassenen op verzoek van CT&R en/of het wijk- of gebiedsteam contact te leggen en vertrouwen te winnen teneinde dakloosheid te voorkomen danwel toe te leiden naar maatschappelijke opvang.
Leverancier	Verwerker, eind-verantwoordelijk voor software ontwikkeling	Voorstander	Wil zo generiek mogelijk Open Source software ontwikkelen
Advies FG: Akkoord, geen verdere opmerkingen			
Adviseur data-ethiek: Lijkt een redelijk complete lijst, opmerkingen van vorige keer zijn aangepast.			

2. Baten

Bij baten kun je denken aan vrijheid, welzijn, welvaart, duurzaamheid, inclusiviteit en diversiteit, gelijkheid, efficiëntie en kostenreductie. (Deze brede benadering is belangrijk, omdat ethische en juridische aspecten invloed kunnen hebben op de relatie tussen onze organisatie en de omgeving)

2.1: Wat zijn de baten voor gemeente Leeuwarden/ SDF/ Friese gemeenten als organisatie?

5.1.2i stelt de Centrale Toegang & Regie in staat om voor inwoners van Friesland op eenduidige, uniforme en gestructureerde wijze toegang te verlenen tot ondersteuning in de vorm van maatschappelijke opvang op grond van de Wmo 2015. Daarmee worden inwoners beter geholpen wat zich vertaalt in een ondersteuningstraject van hoge kwaliteit in een zo kort mogelijke tijd. Het voorkomen en het verkorten van de duur van dakloosheid draagt bij aan gezondere individuen, meer welzijn, beperking van maatschappelijke teloorgang en een krachtiger samenleving waarin voorzien wordt in de basisvoorwaarden die ten grondslag liggen aan de bestaanszekerheid van inwoners in Friesland.

De maatschappelijke schade en kosten als gevolg van dakloosheid kunnen zodoende worden gereduceerd. Het doelmatig en efficiënt organiseren van de maatschappelijke opvang draagt mogelijk bij aan het reduceren van het aantal opvangvoorzieningen. Daardoor gaat het beter lukken om de wettelijke taak uit te voeren binnen het daarvoor beschikbare budgettaire kader (i.c. de Decentralisatie Uitkering Maatschappelijke Opvang).

Het reduceren van het aantal opvangvoorzieningen is wel een doel, maar niet vanuit een bezuinigingsdoelstelling. Het doel is dat door een actiever "er-op-af" casusregie mensen sneller door- of uitstromen naar een passende plek (zelfstandig of in een instelling). In combinatie met een focus op preventie zou ook de instroom kunnen afnemen. M.a.w. minder instroom, snellere uitstroom, korter verblijf in de MO dan zou het aantal plekken kunnen afnemen. Afbouw van plekken is een wens en een opgave, maar kan alleen plaatsvinden als er daadwerkelijk minder vraag is naar opvang.

Door vanuit de CT&R met 5.1.2i te gaan werken wordt het mogelijk om meer zicht te krijgen op de vraag naar maatschappelijke opvang, de oorzaken van dakloosheid, de knelpunten die zich voordoen bij het beëindigen van dakloosheid en de mate waarin het voorgaande zich voordoet. Inzicht stelt gemeenten in staat (nieuw) beleid te ontwikkelen, de inkoop van passende ondersteuning te organiseren en input te leveren ten behoeve van bijvoorbeeld woningbouwprogrammering. Daarnaast vraagt de landelijke overheid om meer regie van gemeenten zowel in het sociale- als het fysieke domein. Dit brengt een kwantitatieve verantwoordingopgave met zich mee waar momenteel niet/ nauwelijks aan voldaan kan worden, tenzij tegen (zeer) hoge kosten. De registratie in 5.1.2i draagt bij aan een stelselmatige administratie die in zichzelf een continu karakter heeft en daarmee robuust is en bestand tegen de dynamiek in de omgeving van de Centrale Toegang.

5.1.2i tenslotte is een applicatie welke goed is doorontwikkeld en voldoet aan diverse standaarden. 5.1.2i is ook de basisapplicatie van Amaryllis waarmee het dus geen nieuwe applicatie betreft. Het beheer en onderhoud van de applicatie is geborgd en vindt onafhankelijk van de CT&R plaats, hiervoor is een SLA beschikbaar. De continuïteit van zowel de CT&R als 5.1.2i is

daarmee voldoende gewaarborgd. De keuze voor 5.1.2i is daarmee ook qua kosten een doelmatige en efficiënte keuze.

Advies FG: Akkoord

Adviseur data-ethiek:
Akkoord

2.2: Wat zijn de baten voor het individu?

Het werken vanuit de CT&R met 5.1.2i draagt er aan bij dat een cliënt weet waar hij/ zij moet zijn voor de toegang tot maatschappelijke opvang. De werkwijze draagt er verder aan bij dat een cliënt niet elke keer zijn/ haar verhaal opnieuw hoeft te doen, of in ieder geval veel minder vaak. De vernieuwde werkwijze draagt naar verwachting ook bij aan de versterking van de rechtspositie van de cliënt omdat er omtrent het besluit tot opvang door de CT&R meer wordt vastgelegd dan momenteel het geval is. Daarnaast maakt de CT&R een einde aan de versnippering van de toegang die tot op heden aan de orde is aangezien de toegang nu belegd is bij de verschillende opvang aanbieders. Zodra een persoon zich heeft aangemeld en als dakloos wordt geregistreerd wordt er een casemanager gekoppeld aan deze persoon. Dat wordt ook gecommuniceerd met deze persoon.

Rondom de start van de CT&R wordt een uitgebreid communicatietraject gestart om bekendheid te geven aan de CT&R. Er is een Factor C sessie geweest en er wordt een communicatieplan opgesteld. De eerste periode loopt de communicatie met cliënten via de huidige zorgaanbieders. De informatie op de websites van de zorgaanbieders en van de BAD wordt aangepast naar de nieuwe situatie. Alle ketenpartners worden geïnformeerd aan de hand van nieuwsbrieven, gesprekken en bijeenkomsten. Aan de hand van folders die op plekken liggen waar daklozen kunnen komen worden daklozen geïnformeerd over de CT&R. Medewerkers van de zorgaanbieders worden geïnstrueerd over de te volgen handelswijze. De lijnen zijn kort omdat de medewerkers van de CT&R afkomstig zijn van de zorgaanbieders zelf. De fysieke aanmelding vindt overigens plaats op de locaties waar mensen zich nu ook al aanmelden. De verwachting is dat de impact qua waar en hoe een persoon zich kan melden gering is.

Omdat maatschappelijke opvang in principe van korte duur is (streven is maximaal 3 maanden gemiddeld) zal de periode dat iemand in de maatschappelijke opvang verblijft niet alle problemen die een cliënt ondervindt op kunnen lossen. Daarom is het de taak van de CT&R om een stevige basis te leggen voor succesvolle ondersteuning in de periode na uitstroom uit de maatschappelijke opvang. Om dat te kunnen doen moeten de casemanagers en de uitstroomcoördinatoren partijen en instanties vergen en verbinden op het doen wat nodig is. Het doel is om de impact daarvan op cliënten zo laag mogelijk te houden. Dat cliënten vaak hun verhaal opnieuw moeten vertellen werkt ontmoedigend en is belastend. De CT&R draagt bij aan het voorkomen van een dergelijke belasting.

Het werken in 5.1.2i is transparant in die zin dat gegevens goed beveiligd zijn, er sprake is van een systeem met accounts en autorisaties die verhinderen dat ongenode gasten mee kunnen kijken. De persoonsgegevens worden centraal gehouden waardoor er geen twijfel meer hoeft te zijn over de locatie van verschillende gegevens. Hierdoor is het ook goed mogelijk om de cliënt inzicht te bieden in de door de CT&R verzamelde gegevens.

De focus vanuit de CT&R is gericht op het zo snel mogelijk beëindigen van daklooshеid. 5.1.2i is zo ingericht dat stapsgewijs alle relevante informatie wordt uitgevraagd en verzameld. Zodat een casemanager in staat is om een integraal ondersteuningsplan op te stellen. De positionering van de CT&R ontsluit ook op een laagdrempeliger manier de weg naar andere (overheids)loketten op een wijze die vaak niet mogelijk is voor zorgaanbieders.

Advies FG: Duidelijk omschreven en akkoord

Adviseur data-ethiek:
Akkoord

2.3: Wat zijn de baten voor de Leeuwarder/Friese samenleving als geheel?

Dakloosheid is een ernstige aantasting van de menselijke waardigheid en ondermijnt het vermogen van mensen om zo volwaardig mogelijk deel te nemen aan de samenleving. Dakloosheid in het algemeen is een verspilling van talent, capaciteiten en kapitaal. Dakloosheid is maatschappelijk gezien ook ontwrichtend omdat, teneinde dakloosheid te beëindigen, bijzondere voorzieningen getroffen moeten worden die ingaan tegen de reguliere gang van zaken. Een voorbeeld in dit verband is dat voor dakloze mensen woningen via bemiddeling kunnen worden toegewezen. Dakloze mensen krijgen daarmee voorrang op de toewijzing van een woning ten opzichte van andere woningzoekenden. In een gespannen woningmarkt schuurt dit omdat alle woningzoekenden een gelijke kans willen hebben op een woning. Door ongelijkheid te organiseren ontstaat er concurrentie tussen kwetsbare groepen. Dit is in zichzelf onwenselijk. Het bestrijden van dakloosheid zowel door middel van preventie als door het verkorten van de periode dat opvang nodig is draagt daarmee bij aan het vermijden van ongelijkheid.

Door meer en in een vroeger stadium inzicht te krijgen in de populatie van dakloze mensen die dakloos dreigen te worden moet het beter gaan lukken om dakloosheid te voorkomen of zo kort mogelijk te laten duren. De pilotfase van de CT&R is er op gericht om onder andere vroegsignalering uit te kunnen oefenen. Wat daarmee wordt bedoeld is, dat als een persoon zich meld bij de CT&R maar nog niet feitelijk dakloos is er sneller en effectiever doorverwezen kan worden naar lokale wijk- en gebiedsteams. Sneller en effectiever verwijzen draagt mogelijk bij aan het voorkomen van feitelijke dakloosheid. Het voorgaande is vooral op persoonsniveau nuttig en noodzakelijke. Op de langere termijn moet inzicht in oorzaken en aanpak beleidsinformatie opleveren voor Friese gemeenten die ingezet kan worden om nieuwe en effectievere beleidsinstrumenten te ontwikkelen of om input op te leveren voor inkoop van gemeenten van passend ondersteuningsaanbod.

Binnen de koker van de CT&R ligt de focus op het curatieve stuk aangezien de dakloosheid zich heeft voorgedaan. Preventie heeft dan een ander karakter. Vanuit het casemanagement door de CT&R is de inzet er actief op gericht om te voorkomen dat iemand na uitstroom opnieuw dakloos raakt. Het voorkomen van recidive zogezegd. De CT&R draagt bij aan een zachte landing van mensen die weer zelfstandig gaan wonen of naar een zorginstelling gaan. Bovendien wordt het Fair Share principe (alle Friese gemeenten hebben een aandeel in het oplossen van het vraagstuk) concreter en stuurbaar. Met de data die de CT&R verzamelt kan inzichtelijk gemaakt worden hoe gemeenten presteren op het gebied van instroom en uitstroom van mensen in de opvang.

Advies FG: Akkoord.

Adviseur data-ethiek:
Akkoord

3. Verantwoording; Is het doel en hoe het doel wordt bereikt juridisch en ethisch verantwoord?
Beschrijf de invloed die het gebruik van gegevens of techniek heeft/kan hebben op menselijke en maatschappelijke waarden en belangen.
Wanneer de verwerking invloed heeft op de data-ethische waarden, betekent dit vaak dat de belangen van stakeholders geschaad worden. Dit kan richting geven aan de beoordeling of een toepassing data-ethisch verantwoord is. Hieronder staan de ethische waarden, die voor gemeente Leeuwarden van belang zijn.

- ***Rechtvaardigheid:***
  We dragen bij aan rechtvaardigheid, gelijke kansen en inclusiviteit. Onze digitale oplossingen zijn laagdrempelig en waardevol voor iedereen. We zijn alert op het voorkomen van ongewenste vooringenomenheid bij de selectie van data. Ook letten we erop dat er geen discriminatie, stereotypering of vooroordelen in algoritmes zit (bias).

- ***Machtsevenwicht:***
  We streven ernaar dat bewoners, ondernemers en bezoekers vertrouwen hebben in de gemeente en onze digitaliseringstrajecten. We toetsen of digitale oplossingen echt meerwaarde hebben voor de gemeente.

- ***Menselijke waardigheid:***
  We behandelen bewoners, ondernemers en bezoekers als mensen, niet als 'nummer'. Onze digitaliseringstrajecten sluiten aan bij de leefwereld en behoeften van de mensen in onze gemeente. De mens is altijd leidend , niet de techniek/data.

- ***Privacy:***

We beschermen de privacy van bewoners en ondernemers. Data van inwoners worden geanonimiseerd gebruikt en zijn niet herleidbaar tot een persoon. We gebruiken 'Privacy by design' en doen onderzoek naar de impact van digitaliseringstrajecten op de privacy.

- ***Veiligheid:***
  We waarborgen de openbare orde en veiligheid, zodat iedereen zich veilig voelt in onze gemeente. We beveiligen onze data. Via cybersecurity bereiden we ons voor op digitale aanvallen.

- ***Autonomie:***
  We respecteren menselijke autonomie (vrijheid). We vermijden onbewuste beïnvloeding, manipulatie en stimulering van dwangmatig gedrag of overheidstoezicht ('Big Brother'). We zijn terughoudend met het gebruik van data waarmee we gebruikers kunnen volgen, hun reputatie schaden of hun toekomst negatief kunnen beïnvloeden.

- ***Controle over technologie:***
  We controleren of onze digitaliseringstrajecten nog goed werken. We letten op datastromen en -opslag. Door open en transparant om te gaan met data en informatie, kan iedereen deelnemen op basis van dezelfde kennis en inzichten.

- ***Kwaliteit van leven/duurzaamheid:***
  We vinden gezond en duurzaam leven belangrijk in Leeuwarden. We zoeken naar duurzame oplossingen waarbij de gezondheid van bewoners, ondernemers en bezoekers voorop staat. Dat geldt ook voor onze digitaliseringstrajecten.

3.1: Welke van de eerder genoemde waarden worden beïnvloed of geraakt door het project/proces?
Beoordeel in de onderstaande vragen of er één of meerdere waarden zijn die mogelijk geraakt worden door het project/proces. (Als de waarde negatief wordt geraakt, neem deze dan op in de risico's bij vraag 11.3 en 11.4)

- ***Rechtvaardigheid:***
  Het werken vanuit de CT&R in het algemeen en met 5.1.2i draagt bij aan het principe van rechtvaardigheid omdat in beginsel de toegang voor een ieder open staat en er geen onderscheidt wordt gemaakt waarvoor geen wettelijke basis aanwezig is. Het recht op maatschappelijke opvang zoals dat in de Wmo 2015 is geformuleerd staat centraal bij de beoordeling van de toegang tot de maatschappelijke opvang. De beoordeling is vrij van stigma en stelt de cliënt centraal. In het uitstroomtraject wordt uitgegaan van het fair share principe waarbij alle Friese gemeenten hun aandeel hebben in het faciliteren van de uitstroom (instroom = uitstroom). Terugkeer naar de gemeente van herkomst en het vertrouwde netwerk van de cliënt wordt daarmee bevorderd.

  De centrale registratie bevordert de gelijke kansen van alle cliënten die opgevangen worden vanwege de in essentie uniforme werkwijze voor alle cliënten. Op hoofdlijnen doorloopt iedereen hetzelfde traject en wordt tegelijkertijd rekening gehouden met unieke persoonskenmerken, behoeften en mogelijkheden.

  Het feit dat de CT&R fysiek toegankelijk is en er gewerkt wordt met medewerkers die gekoppeld zijn aan een cliënt maakt dat de toegang laagdrempelig en klantvriendelijk zal zijn, ook voor mensen die geen/ weinig gebruik kunnen of willen maken van de digitale varianten van contact met instanties.

- ***Machtsevenwicht/machtsverhoudingen:***
  Het werken met 5.1.2i versterkt het machtsevenwicht aangezien het duidelijk is voor een cliënt wat daarin wordt vastgelegd en met welk doel dat gebeurd. Hoewel er geen interface beschikbaar is voor een cliënt waarmee hij/ zij zelf de status kan inzien en volgen, kan er wel een uitdraai gemaakt worden van de data die in 5.1.2i staat. Verder heeft de cliënt zelf de regie op wat de cliënt wel/niet wil delen. Aan de andere kant is de CT&R transparant over de mogelijkheden tot succesvolle ondersteuning op het moment dat een cliënt weigert relevante informatie te delen.

  De regie ligt bij de cliënt. Als een persoon geen informatie wil delen dan hoeft dat niet. De consequentie is dat de cliënt dan niet effectief in traject genomen kan worden. De cliënt draagt dan zelf een grotere verantwoordelijkheid om bij de diverse instanties de benodigde gegevens aan te leveren en mogelijk zijn of haar verhaal opnieuw te vertellen. De wens om niet geholpen te willen worden is een goed recht. De vraag is wel hoe realistisch het is dat een persoon zich wel

aanmeld voor ondersteuning en vervolgens geen informatie deelt. Het is daarnaast de afweging van de casemanager zelf hoe ernstig het is als bepaalde informatie niet beschikbaar is. Dat verschilt per onderwerp en dat verschilt ook per persoon.

Als een persoon zodanig zorgmijdend is dat ondersteuning richting uitstroom niet mogelijk is dan is dat een gegeven waar rekening mee gehouden kan worden vanuit zorgoogpunt. Uitstroom is dan geen doel op zich. Het doel van de zorg en ondersteuning ligt in dergelijke situaties op het contact leggen en vertrouwen winnen van de cliënt. Dit gebeurt nu ook al, bijvoorbeeld door het ACT team.

Een persoon kan overigens wel opgevangen worden in de Nachtopvang. De mogelijkheid om daar te overnachten blijft bestaan ook zonder dat er sprake is van een volledige inclusie en intake.

Als een persoon niet mee wil/kan werken aan het delen van gegevens dan wil dat niet zeggen dat deze persoon dan aan zijn/haar lot wordt overgelaten. Maar de mogelijkheden om alles voor deze persoon te doen zijn dan wel beperkter en het traject zal naar alle waarschijnlijkheid ook langer duren.

- ***Menselijke waardigheid:***
  De cliënt staat centraal. De ondersteuningsbehoefte van een cliënt manifesteert zich concreet op het moment dat iemand zich aanmeld voor opvang. Vanuit de CT&R en met behulp van 5.1.2i 5.1.2i ontvouwt zich een route naar maatschappelijk herstel. Dit is altijd maatwerk gebaseerd op de behoefte en mogelijkheden van de cliënt en de samenwerking met- en expertise van professionals. Uitgaande van de premisse dat dakloosheid in wezen mensonwaardig is leidt het doorlopen van een traject via de CT&R naar meer menswaardigheid.

  Hoewel zoveel mogelijk rekening gehouden wordt met de behoeften en mogelijkheden van de cliënt heeft de CT&R wel als doel dat trajecten zo snel mogelijk worden doorlopen. Daarom wordt er bij betrokken zorgaanbieders vanuit de CT&R wel druk op de ketel gehouden en kan het zijn dat het tempo waarmee vanuit de CT&R gewerkt wordt niet noodzakelijkerwijs altijd als het juiste tempo worden gewaardeerd vanuit het oogpunt van de cliënt. Dit kan overigens twee kanten opwerken, voor de één ga je te snel en voor de ander niet snel genoeg.

  Het traject/proces CT&R is een middel en geen doel op zich. Het proces is een ideaaltypische representatie van de werkelijkheid. De werkelijkheid verloopt anders dan modelmatig is bedacht. De kunst is om binnen de kaders van het proces mee te bewegen met de situatie. Het werkproces CT&R biedt daar alle ruimte voor.

  Overigens bepalen wij (als gemeente) zelf wat de redelijk is. Bijvoorbeeld het uitgangspunt dat een traject gemiddeld 3 maanden mag duren. Dit is geen natuurwet maar een (overigens landelijke) beleidsambitie. Voor de CT&R is het iets om naar te streven. Je monitort en evalueert hoe realistisch een dergelijke termijn is. Ook dit soort termijnen zijn een hulpmiddel en geen doel op zicht. Toch is het niet helemaal uit de lucht gegrepen. Landelijk (en ook in Europees verband) is 3 maanden wel een norm.

  De kunst is om het goede midden te vinden tussen wat op persoonsniveau realistisch en acceptabel is en wat op Fries niveau de beleidsambitie is.

- ***Privacy:***
  Het werken met 5.1.2i is vanwege de opzet van de applicatie de best mogelijke waarborg voor de borging van de privacy van de cliënt. De cliënt kan een uitdraai opvragen van de informatie en kan een verzoek indienen voor het recht op vergeten.

  De uitwisseling van informatie met derden gebeurt beveiligd en de koppeling met andere systemen zoals het 5.1.2i en 5.1.2i vindt intern plaats en voldoet aan de daartoe benodigde standaarden. Koppelingen zijn gestandaardiseerd aan ele d via 5.1.2i via standaard beveiligde tunnels en zijn roven technology naar 5.1.2i en de standaard 5.1.2i -koppelvlakken (intern via 5.1.2i). Binnen 5.1.2i wordt gewerkt met persoonsgebonden accounts en autorisaties zodat alleen mensen die in 5.1.2i moeten werken toegang hebben tot de data en dan ook nog alleen de voor hen relevante data. Binnen 5.1.2i krijgt gebruikers ook een standaard bericht met daarin richtlijnen wat men niet mag delen, bijvoorbeeld geloofsovertuiging/ politieke voorkeur of seksuele voorkeur

  De koppeling met 5.1.2i waarmee de benodigde dashboards worden gemaakt is in de basis anoniem. Ten behoeve van het uitvoeren van caseload management is de data niet geanonimiseerd beschikbaar. Dit laatste is alleen aan de orde voor de medewerkers van de

CT&R. De toegankelijkheid van data vindt plaats op basis van autorisaties en dient de voortgang van- en sturing op het casemanagement en de bewaking van de datakwaliteit. De dashboards zijn niet publiek toegankelijk met uitzondering van geanonimiseerde rapportages die met 5.1.2i worden gegenereerd. De platte rapportage is enkel een kwantitatieve weergave van de onderliggende data. De data zelf kan niet worden benaderd via de rapportage (doorgaans een PDF, Word document of Excel bestand).

- ***Veiligheid:***
  De data wordt veilig opgeslagen conform de standaarden waaraan 5.1.2i moet voldoen. Data wordt opgeslagen in de 5.1.2i bij de leverancier van 5.1.2i . 5.1.2i . De opslag gebeurt in een 5.1.2i database die standaard is ingericht per gemeente en dus afgeschermd is van de rest van gebruikers. Het toegangsproces van de CT&R is gericht op het versterken van de veiligheid van mensen in een kwetsbare positie. Door de veiligheid van dakloze mensen te bevorderen wordt een bijdrage geleverd aan een veiliger samenleving voor iedereen.

  Het veiligheidsgevoel van een persoon hangt naast de veilige omgang met gegevensdeling en verwerking vooral samen met de ervaren benadering en bejegening. Het laagdrempelige karakter van de CT&R en het feit dat alle cliënten beschikken over een eigen casemanager die bereikbaar en toegankelijk is een versterking van de veiligheid ten opzichte van de huidige situatie. De gemeentelijke overheid zet namelijk een flinke stap naar voren in het nemen van de verantwoordelijkheid voor kwetsbare inwoners.

- ***Autonomie:***
  Het uitgangspunt is dat daklоosheid autonomie verhindert en dat de centrale toegang en de regie op het traject autonomie moet bevorderen. Door in te zetten op casemanagement wordt cliënten perspectief geboden op maatschappelijk herstel als haalbaar doel. Daar waar zelfstandig wonen niet in de lijn der verwachting is wordt vanuit casemanagement ingezet op toeleiding naar intramuraal verblijf.

  Een persoon mag ongehinderd dakloos zijn zolang de wet niet wordt overtreden (of de APV) en er geen overlast plaatsvindt. Als mensen zorgwekkend zorgmijdend gedrag laten zien wordt er bemoeizorg ingezet. In Friesland zijn er diverse outreachend werkers actief, zijn er FACT teams van GGZ en VNN en in Leeuwarden is het ACT actief bezig met deze groep. Ingewikkelde casuïstiek met een veiligheidscomponent wordt door het Zorg- en Veiligheidshuis opgepakt. Het voorgaande is bestaande praktijk en gaat buiten de CT&R om.

  Als iemand zich niet meld bij de CT&R dan zal er geen druk uitgeoefend worden door de CT&R om dat wel te doen. Pas op het moment dat iemand zich meld gaat de CT&R aan de slag. Dat is uiteraard niet vrijblijvend. Echter is het een autonome beslissing van de persoon zelf geweest om zich te melden. Krachtig is dat de persoon onderkent dat het hem zelf niet meer lukt om op eigen kracht uit de situatie te komen. Deze stap is een betekenisvolle stap naar herstel. Dit kunnen we vanuit de CT&R alleen maar toejuichen en ondersteunen door vervolgens onze uiterste best te doen om op alle mogelijke manieren de cliënt een steun in de rug te bieden op het pad van maatschappelijk herstel.

  De CT&R voert regie uit op het traject. Cliënten worden daarbij gevolgd in het traject wat met hen in het ondersteuningsplan is afgesproken. Als een cliënt is uitgestroomd of als een traject (zaak) wordt afgesloten dan komt daarmee ook een einde aan de betrokkenheid vanuit de CT&R.

  Deelname aan het traject is vrijwillig. De individuele begeleiding heeft een outreachend karakter. In specifieke situaties zal er sprake zijn van bemoeizorg vanuit de GGZ en/of verslavin szor (het ACT team). Dit is op dit moment ook de situatie. Het werken vanuit de CT&R en 5.1.2i verandert aan die werkwijze niet zo veel. Wel zal er meer zicht ontstaan op de benodigde inzet van bemoeizorg en de kwaliteit daarvan.

  De data die in 5.1.2i wordt geregistreerd wordt niet ingezet om cliënten te volgen voor andere doeleinden dan uitstroom uit de MO.

- ***Controle over technologie:***
  Het beheer en onderhoud van 5.1.2i is belegd bij 5.1.2i en vindt onafhankelijk van de CT&R plaats. Is met de 5.1.2i die aan gemeenten de 5.1.2i 5.1.2i verkoopt geborgd. Er worden Pentesten uitgevoerd met TPM verklaring. Pentesten worden niet gedeeld door leverancier omdat er gevoelige informatie in staat/kan staan. De veiligheid is daarmee voldoende geborgd.

De datastroom is versleuteld via [redacted] vanuit [redacted] naar [redacted] is een interne datastroom en voldoet aan de daarvoor van toepassing geldende standaarden.

De samenwerking binnen [redacted] en het delen van gegevens binnen [redacted] valt onder de reikwijdte van de samenwerking zoals momenteel is vastgelegd in de DEPIA voor het Transferpunt en wordt voortgezet vanuit de CT&R. Het werken vanuit de CT&R met [redacted] is in dit opzicht een verbetering ten opzichte van de huidige situatie omdat het beveili_d mailen van handmatig ingevulde formulieren zal vervallen met de start van het werken in [redacted].

- ***Kwaliteit van leven/duurzaamheid:***
  Het werken vanuit de CT&R met [redacted] beoogt het verbeteren van de dienstverlening aan kwetsbare inwoners van Friesland. Door vanuit 1 plek op een integrale manier het onderzoek uit te voeren naar wat de best passende ondersteuning is, het in kaart brengen van de route naar het beoogde resultaat en de regie daarop, wordt vorm gegeven aan de principes van kwaliteit van leven en duurzaamheid.

De mogelijke risico's op de publieke waarden zijn in het overzicht van de risico's bij vraag 11.3 opgenomen.

Advies FG: Helder en akkoord.

Adviseur data-ethiek:
Akkoord

3.2: Welke wet-, regelgeving en beleid is betrokken bij de gegevensverwerkingen?
Denk aan wetten, besluiten, gedragscodes, convenanten of beroepscodes. Ook normenkaders zoals voor de IT General Controls: de internationale norm ISO/IEC 27002 en de BIO. (vraag eventueel de privacy officer/privacy jurist).

Wet maatschappelijke ondersteuning 2015

De Wmo 2015 stelt in algemene zin en vooral op grond van artikel 1.2.1 dat:

Een ingezetene van Nederland overeenkomstig de bepalingen van deze wet in aanmerking komt voor een maatwerkvoorziening, bestaande uit:

a. door het college van de gemeente waarvan hij ingezetene is, te verstrekken ondersteuning van zijn zelfredzaamheid en participatie, voor zover hij in verband met een beperking, chronische psychische of psychosociale problemen niet op eigen kracht, met gebruikelijke hulp, met mantelzorg of met hulp van andere personen uit zijn sociale netwerk voldoende zelfredzaam is of in staat is tot participatie,

b. beschermd wonen, te verstrekken door het college van de gemeente tot welke hij zich wendt, voor zover hij in verband met psychische of psychosociale problemen niet in staat is zich op eigen kracht, met gebruikelijke hulp, met mantelzorg of met hulp van andere personen uit zijn sociale netwerk te handhaven in de samenleving, dan wel

c. opvang, te verstrekken door het college van de gemeente tot welke hij zich wendt, indien hij de thuissituatie heeft verlaten, al dan niet in verband met risico's voor zijn veiligheid als gevolg van huiselijk geweld, en niet in staat is zich op eigen kracht, met gebruikelijke hulp, met mantelzorg of met hulp van andere personen uit zijn sociale netwerk te handhaven in de samenleving.

Convenant Weer Thuis
In 2022 is het Convenant Weer Thuis gesloten tussen alle Friese gemeenten, zorgaanbieders maatschappelijke opvang en beschermd wonen en alle Friese woningcorporaties. Het doel van het convenant is het bevorderen van de uitstroom uit voorzieningen voor maatschappelijke opvang en beschermd wonen. Daarnaast het organiseren van een zachte landing in de wijk en het sturen op- en monitoren van de uitstroom naar de herkomstgemeente van cliënten. Uitstroom wordt mede bevorderd door middel van woningtoewijzing door woningcorporaties na bemiddeling. Bemiddeling komt neer op het met urgentie toewijzen van een woning in plaats van op reguliere wijze (op basis van voldoende inschrijfduur). Om het proces van bemiddelen te faciliteren is het Transferpunt opgericht. Het Transferpunt bestaat uit een aantal medewerkers in dienst van gemeente Leeuwarden/SDF. Voor de registratie van daklozen maakt het Transferpunt gebruik van een monitor

welke gevuld wordt met data die door zorgaanbieders wordt aangeleverd bij het Transferpunt (via beveiligde 5.1.2i kanalen en/of via beveiligde mail). Bij de aanvang van het Transferpunt is ook een DEPIA uitgevoerd. Het Transferpunt gaat functioneel o_ in de CT&R. De monitor die het Transferpunt nu gebruikt wordt vervangen door registratie in 5.1.2i. Het is niet nodig het convenant aan te passen: de overgang naar CT&R zorgt voor het verbeteren van het uitvoeren van de convenantafspraken.
Advies FG: Akkoord.

4. Persoonsgegevens & Betrokkenen
4.1: Van welke type personen worden persoonsgegevens verwerkt? En welke persoonsgegevens worden van elk type persoon verwerkt?
Denk aan medewerkers, consumenten, kinderen, cliënten, bezoekers, gebruikers of inwoners van een gemeente. Denk bij persoonsgegevens bijvoorbeeld aan naam, adres, telefoonnummer, BSN, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, kenteken, bankrekeningnummer en -saldo, functie, opleiding, inkomens-en vermogensgegevens, lidmaatschap vakbond, persoonlijke voorkeuren, loonschaal, gespreksverslagen, gegevens over de gezondheid of strafrechtelijke gegevens (Denk bij risicoklasse I aan NAW, bij II aan bijzondere persoonsgegevens zoals ras, etniciteit en gezondheid en bij III aan strafrechtelijke gegevens).

Ter toelichting op onderstaande tabel. Om de toegang (inclusie) tot de maatschappelijke opvang (MO) te onderzoeken is in 5.1.2i een zaaktype ontwikkeld. Daarom wordt hieronder ingegaan op de verschillende zaaktypen. De vragen die (met name tijdens de intake) worden gesteld zijn veelal gesloten vragen met beperkte antwoordcategorieën; ja/nee, keuzelijsten aangevuld met open tekstvelden voor toelichting en het oordeel van de medewerker als basis voor het opstellen van het ondersteuningsplan en het uitvoeren van de regie. Het gaat naast concrete persoonsgegevens vaak om informatie “dat” er sprake is van het één of ander. Bijvoorbeeld: “gebruik je medicijnen? Ja of Nee. Welke medicijnen worden gebruikt wordt niet uitgevraagd.

Persoon	**Soort persoonsgegeven**	**Risicoklasse**
Medewerker	Naam, emailadres, telefoonnummer	I
Inwoner - algemeen	BSN, Naam, Adres, Woonplaats, geboortedatum, Email, telefoonnummer, gezinssamenstelling	I
Inwoner - zaakstap 1 Start zaak MO	ID bewijs, leefsituatie, burgerlijke staat, nationaliteit, verblijfsstatus, vluchtelingennummer, redenen aanmelding en/of (dreigende) dakloosheid.	I, II en III
Inwoner - zaakstap 2 – Aanmelding MO	Geboorteplaats, herkomstgemeente, laatst bekende adres van inschrijving, her-aanmelding MO, locatie huidig verblijf en bij wie, kinderen, netwerk, soort inkomen, vermogen, wettelijke vertegenwoordiging, postadres, contactpersoon gebiedsteam.	I
Inwoner - zaakstap 3 – Plaatsing MO	Inschrijving postadres, adres van plaatsing in opvang, bepaling overdracht herkomstgemeente	I
Inwoner - zaakstap 4 - Intake	Algemene achtergrondinformatie over kinderen (aantal, gezag, meerderjarigheid), kinderbeschermingsmaatregel, naam, geboortedatum, BSN kinderen, locatie verblijf kinderen, omgangsregeling, betrokkenheid jeugdhulp, naam jeugdhulpinstantie, contactgegevens betrokken jeugdhulpverlener, maatregel, (gezins)voogd. Laatste woonsituatie cliënt, reden verlaten woonsituatie, verblijf in netwerk. Betrokkenheid gebiedsteam/ herkomstgemeente, contactgegevens medewerkers gebiedsteam/ gemeente, naam & contactgegevens andere betrokken instanties. Inkomenssituatie. Werksituatie. Schuldsituatie: type, hoogte, regeling/ traject. Huurverleden: sociaal, particulier, huurschulden, uitzetting. Zorgverzekering, inschrijving huisarts, tandarts, apotheek, actuele gezondheidssituatie, behandelsituatie, medicatie. Mate van zelfredzaamheid. Geestelijke gezondheid, klachten, diagnostiek, medicatie. Verslaving, gebruik middelen, type middelen, verleden van verslaving, frequentie, ervaren problemen, soort problemen, verkrijging middelen. Justitieel verleden, contact reclassering, openstaande zaken. Huiselijke relaties, aard en kwaliteit contact familie. Plaatsing verlengd verblijf in opvang. Inschatting zelfredzaamheid.	I, II en III

Inwoner - zaakstap 5 – Bepalen type uitstroomtraject	Uitstroomprofiel. Ondersteuningsplan met doelen op levensgebieden. Bevat onder meer informatie die tijdens de intake is uitgevraagd. En acties en status voortgang.	I, II en III
Inwoner - zaakstap 6 – Uitstroomprofiel zelfstandig wonen	Omstandigheden die van invloed zijn op terugkeer naar herkomstgemeente. Woonwensen. Uitstroomgemeente, woonsituatie na verhuizing.	I
Inwoner - zaakstap 7 – Uitstroom verblijf instelling	Indicatie/ beschikking zorg of ondersteuning, locatie van uitstroom, naam instelling.	I
Inwoner - zaakstap 8 - Trajectafsluiting	Definitief uitstroomprofiel, uitstroomgemeente.	I
Advies FG: Akkoord.		

4.2: Wie hebben er toegang tot de gegevens?

5.1.2i is alleen toegankelijk voor de medewerkers van de CT&R en alleen zij kunnen de gegevens lezen en bewerken. Hoe de autorisaties per medewerker uiteindelijk definitief ingesteld moeten worden is een vraag waar de pilot CT&R een antwoord op moet geven. Het is voorstelbaar dat de Aanmeldfunctionaris en de Plaatsingcoördinator geen inzicht nodig heeft in alle zaakstappen. De cliënt kan toegang krijgen tot eigen gegevens op aanvraag, er komt echter geen klantpagina o.i.d.. De casemanager, administratief medewerker en uitstroomcoördinator hebben autorisaties voor lezen van het hele dossier in 5.1.2i. De casemanager en de administratief medewerker kunnen alle zaakstappen bewerken. De uitstroomcoördinator is geautoriseerd voor het bewerken van de zaakstappen die betrekking hebben op de uitstroom (zaakstap 5-7).

Derde _artijen hebben _een directe toe_an_ tot de _e_evens in 5.1.2i 5.1.2i. Informatie kan 5.1.2i

Meestal is daar een wettelijke grondslag voor. In een aantal specifieke gevallen wordt de toestemming gevraagd van de cliënt om de betreffende gegevens te delen.

Zorgaanbieders ontvangen het ondersteuningsplan en de casemanager stemt af met de trajectbegeleider van de cliënt. Wijk- en gebiedsteam medewerkers in verband met het uit te voeren onderzoek naar thuisondersteuning na uitstroom en ten behoeve van de overdracht bij uitstroom. Woningcorporaties voor zover noodzakelijk om een bemiddeling naar woningtoewijzing in gang te zetten.

De data in 5.1.2i wordt intern aangeleverd bij de afdeling bedrijfsvoering en advies sociaal domein van de gemeente Leeuwarden ten behoeve van data analyse en de verwerking van de data in 5.1.2i. Door middel van autorisaties wordt de toegang tot het dashboard geregeld. De dashboards zijn niet openbaar.

In 5.1.2i wordt er samengewerkt tussen de medewerkers van de CT&R, zorgaanbieders (Wender, Limor, Leger des Heils en VNN) en woningcorporaties. In besloten en beveiligde 5.1.2i kanalen wordt informatie gedeeld ten behoeve van een vlotte en soepele samenwerking in het uitstroomtraject van een cliënt. De 5.1.2i kanalen worden beheerd en onderhouden door de casemanagers, uitstroomcoördinatoren en administratie van de CT&R. Binnen 5.1.2i krijgt iedereen ook een standaard bericht met daarin richtlijnen wat men niet mag delen, bijvoorbeeld geloofsovertuiging/ politieke voorkeur of seksuele voorkeur. Hierover zullen procesafspraken over gemaakt worden over het beschrijven documenteren in het zaaksysteem 5.1.2i, zodat ook later en door anderen terug te zien is waarom dingen zo zijn gedaan. Het is aan te raden om een vernietigingstermijn hiervoor vast te stellen, bijv. 1 jaar na beëindiging traject en goed te laten keuren door de gemeentearchivaris via de IRO.

Medewerkers van het Shared 5.1.2i Centrum/Informatiemanagement/Functioneel Beheer Beheerders Leeuwarden hebben toegang ten behoeve van foutopsporing/hulpverlening techniek.

Advies FG: Akkoord

5. Waar worden de gegevens opgeslagen?
Bijvoorbeeld in de Cloud of op onze eigen servers. Benoem ook eventueel in welke landen de gegevensverwerkingen en opslag plaatsvinden. Waar slaan (sub)verwerkers de gegevens op?

- De gegevens die worden verwerkt in [5.1.2i] en [5.1.2i] worden opgeslagen in de cloudopslag op servers van [5.1.2i]. Deze hostingpartij van [5.1.2i] heeft servers staan in datacentra in NL.
- Correspondentie met de cliënt in de vorm van brieven worden in [5.1.2i] gearchiveerd op de eigen servers van gemeente Leeuwarden
- In [5.1.2i]. Data wordt opgeslagen in de [5.1.2i] van [5.1.2i]
- Uitgaande correspondentie (bijvoorbeeld beschikkingen) wordt gearchiveerd in [5.1.2i], vergelijkbaar- en in lijn met de wijze waarop dit gebeurd voor alle uitgaande correspondentie op de eigen servers van gemeente Leeuwarden.

De vol ende gekoppelde systemen zijn aanwezig:
- [5.1.2i]: GBA voor correcte klantregistratie en -mutaties.
- [5.1.2i]: documentgenerator.
- PDC: Producten- en Dienstencatalogus van de [5.1.2i] [5.1.2i], voor het bestelproces en financiële afhandeling m.b.t. Wmo en Jeugdwet zorgproducten. (Wordt in de toekomst mogelijk ingezet voor producten verblijf bij de Centrale toegang)
- SOM: sociale monitor, met standaard datarapporten m.b.t. [5.1.2i] [5.1.2i])
- Mana ement Informatie (MI) Datadump: dagelijkse aanlevering van (in basis) alle in [5.1.2i] geregistreerde data. Deze wordt in het datawarehouse gezet en gebruikt voor diverse ra orten en dashboards voor de gebruikersorganisaties.
- [5.1.2i]: [5.1.2i] wordt z.s.m. gekoppeld aan het zaaksysteem [5.1.2i], hier wordt het centrale informatiebeheer geregeld.

Alle geautoriseerde gebruikers van [5.1.2i] hebben toegang tot zogenaamde klantpagina's. Een gebruiker moet wel op zoek naar een klantpagina. Bijvoorbeeld door gericht op basis van een BSN nummer en/of geboortedatum en achternaam op zoek te gaan naar de klantpagina van een persoon. Een klantpagina bevat "DAT" informatie, zo weet een gebruiker dat er op de betreffende klant mogelijk al voorzieningen actief zijn (bv. klant heeft een beschikking voor Beschermd Wonen). Dit laatste is relevante informatie omdat een actieve beschikking voor Beschermd Wonen voorgaat op Maatschappelijke Opvang. Het is dan de bedoeling dat, voordat er besloten wordt om iemand daadwerkelijk op te vangen, eerst onderzocht wordt waarom deze klant niet in Beschermd Wonen verblijft, maar blijkbaar op straat is beland. Terugkeer naar Beschermd Wonen is dan een voorliggende actie. Lukt dat laatste om allerlei redenen niet dan kan opvang alsnog een passende voorziening zijn. Het inzien van DAT informatie stelt gebruikers in staat om gericht de samenwerking op te zoeken.

Wat betreft de DAT informatie in [5.1.2i] is deze inzichtelijk voor zover een medewerker CT&R geautoriseerd is tot de klant a ina in [5.1.2i]. Dat betekent dus dat, voor alle ersonen voor wie er een klantpagina in [5.1.2i] aangemaakt is, dit voor alle gebruikers van [5.1.2i], die toegang hebben tot de klantpagina, inzichtelijk is. Een klantpagina kun je niet aan je werkvoorraad koppelen, dat kan alleen op zaakniveau. De kans dat een gebruiker onterecht op de klantpagina terechtkomt is daardoor heel klein. De klantpagina is in gebruikersprofielen af te schermen, maar wie in zijn proces de klantpagina gebruikt, kan zijn eigen klant a ina's niet voor andere gebruikers afschermen. Kortom, wie geautoriseerd is om binnen [5.1.2i] een klantpagina te gebruiken, kan alle klantpagina's inzien. Vanuit het Klant Informatie Model is in de daarbij behorende DEPIA is geregeld dat "DAT" informatie kan worden ingezien, dit is ook binnen [5.1.2i] uitgerold.

In de autorisatiematrix van het zaaktype Opvang is vastgelegd wat de autorisatieprofielen per rol zijn. In deze autorisatieprofielen (die zijn gekoppeld aan zaaktypes) is in te stellen of gebruikers zaaktypes bij een persoon kunnen zien, opstarten, bewerken en/of raadplegen. Deze autorisaties worden aan individuele gebruikers al dan niet toegekend. Als er geen autorisatieprofiel is toegekend voor een bepaald zaaktype, zal de betreffende gebruiker niets kunnen zien van dat zaaktype.

NR	Naam zaakstap	Toegangsrechten	Toewijzing

	Zaakstap 1: Start - Aanmaken nieuwe zaak	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Aanmeldfunctionaris (alle rechten)
	Zaakstap 1a: Start en Aanmelding	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Aanmeldfunctionaris
	Zaakstap 1b: Aanmelding – Conclusie en Besluit Inclusie	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Aanmeldfunctionaris
	Zaakstap 1c: Aanmelding – Afronding geen inclusie maatschappelijke opvang	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Aanmeldfunctionaris
	Zaakstap 2a: Plaatsing – Eerste opvang	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Aanmeldfunctionaris & Plaatsingscoördinator (bewerken)
	Zaakstap 2b: Plaatsing – Inschrijving briefadres	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Plaatsingscoördinator
	Zaakstap 2c: Plaatsing – Warme overdracht regio van herkomst	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Plaatsingscoördinator
	Zaakstap 3a: Intake	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager
	Zaakstap 3b: Intake – Conclusie en Besluit Verlengde Opvang	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager
	Zaakstap 3c: Intake – Zelfredzaamheidsmatrix	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager
	Zaakstap 4a: Uitstroomtraject – Bepalen uitstroomprofiel	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager
	Zaakstap 4b: Uitstroomtraject – Ondersteuningsplan	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager
	Zaakstap 4c: Uitstroomtraject – Acties	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager

	Zaakstap 5a: Uitstroomprofiel zelfstandig wonen – Aanvullende vragen	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat (bewerken)
	Zaakstap 5b: Uitstroomprofiel zelfstandig wonen – Bepalen uitstroomgemeente	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat
	Zaakstap 5c: Uitstroomprofiel zelfstandig wonen – Bepalen woonwensen	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat
	Zaakstap 5d: Uitstroomprofiel zelfstandig wonen – Onderzoek benodigde thuisondersteuning	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat
	Zaakstap 5e: Uitstroomprofiel zelfstandig wonen – Regulier of Bemiddeling?	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat
	Zaakstap 5f: Uitstroomprofiel zelfstandig wonen – Aanvraag bemiddeling	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat
	Zaakstap 5g: Uitstroomprofiel zelfstandig wonen – Verhuizing naar woning	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat
	Zaakstap 5H: Uitstroomprofiel zelfstandig wonen – Woningcorporatie niet akkoord	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat
	Zaakstap 6: Uitstroom naar een instelling	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat
	Zaakstap 7 Trajectafsluiting	Bewerkrecht voor administratief medewerkers (altijd alle zaken, niet via functionaliteit zaakondersteuner)	Casemanager & Uitstroomcoördinat

Advies FG: Akkoord. Goed, dat de autorisatiematrix is toegevoegd.

6. Hoe lang worden de persoonsgegevens bewaard en vervolgens vernietigd?
D_b_ - en vernietigingstermijnen staan in de Gemeentelijke selectielijst en kun je opvragen bij 5.1.2e .

De bewaartermijn bij vestrekking is vastgesteld op (minimaal) 15 jaar, bij weigering of buiten behandeling stellen is dit 5 jaar en bij het afbreken van het proces is dit 6 weken gebaseerd op de wet Wmo 2015 en gemeentelijke selectielijst 2020. De informatie zal na deze termijnen worden vernietigd volgens de gemeentelijke vernietigingsprocedure. De informatie in 5.1.2i wordt ook vernietigd volgens een vast_estelde procedure binnen dit systeem dit wordt beheerd door functioneel beheer 5.1.2i .

In 5.1.2i worden alle gegevens verwijderd door de verantwoordelijk medewerker van de CT&R na het beëindigen van een traject, nadat hier afspraken over zijn gemaakt en dit is vastgele_d en goedgekeurd door de gemeentearchivaris via de IRO, dus bij het afsluiten van de zaak. 5.1.2i is voor zover het gebruikt wordt binnen de CT&R geen archief om_egevens in te bewaren. Sowieso mogen bijzondere persoonsgegevens niet worden_edeeld via 5.1.2i . Alle te bewaren gegevens en documenten staan standaard in 5.1.2i . 5.1.2i bevat de bron data en 5.1.2i niet.

Advies FG: Helder en akkoord.

7.1 Is er sprake van (semi-) geautomatiseerde besluitvorming en/of profilering? Zo ja, beschrijf deze?
Geautomatiseerde besluiten worden zonder medewerker genomen. Profileren is het opbouwen van profielen waarmee je mensen in categorieën kunt indelen.

Er is geen sprake van (semi) geautomatiseerde besluitvorming en/of profilering.

Advies FG: Helder en akkoord.

7.2 Wordt er gebruik gemaakt van nieuwe technologieën zoals kunstmatige intelligentie (AI), Robotisering (RPA), biometrie etc.? Zo ja, beschrijf deze

Nee, op AI en Biometrie. Robotisering (RPA) wordt mogelijk alleen_ebruikt (in de nabije toekomst) om vragenlijsten, formulieren en gegevens over te zetten naar 5.1.2i of een ander door de gemeente gebruikte zaaksysteem. Voor ingebruikname van robot-processen wordt de DEPIA aangepast en opnieuw besproken.

Voor de migratie van de monitor van het Transferpunt wordt door_emeente Leeuwarden een robot ontwikkeld om de data uit de monitor over te zetten in 5.1.2i .

Advies FG: Helder en akkoord.

8. Op welke rechtsgronden zijn de verschillende gegevensverwerkingen gebaseerd?
Als er sprake is van een publieke taak of wettelijke verplichting moet deze (zo veel mogelijk) te herleiden zijn naar specifieke bepalingen in de betreffende wetgeving. (vraag de privacycontactpersoon van jouw domein om deze vraag te beantwoorden)

Het proces Centrale Toegang en Regie Maatschappelijke Opvang valt onder de Wmo 2015 (artikel 1.2.1 sub c) en is daarmee een wettelijk verplichte taak van de gemeente. De grondslag is artikel 6 lid 1 sub c AVG.

Advies FG: Helder en akkoord.

9. Is de verwerking in lijn met het doel of is er sprake van een verenigbare verdere verwerking?
Gebruik je de persoonsgegevens die je voor dit proces of project hebt verzameld ook nog voor iets anders? Is deze verdere verwerking dan verenigbaar is met het doel waarvoor ze zijn verzameld? Denk bijvoorbeeld aan gegevens voor de bijstand die vervolgens worden gebruikt voor kwijtschelding van belastingen. (vraag de privacy contactpersoon van jouw domein)

Voor de gegevensverwerking in [5.1.2i] is sprake van een wettelijke grondslag, in het bijzonder op grond van de Wmo 2015. De gegevensverwerking staat ten dienste van de ondersteuning aan de cliënt die zich heeft gemeld voor maatschappelijke opvang en ondersteuning bij toeleiding naar passende zorg/ondersteuning en/of uitstroom naar zelfstandig wonen/ zachte landing. Medewerkers van de CT&R werken daarvoor samen met bij de cliënt betrokken instanties zoals wijk- en gebiedsteams, gemeenten, zorgaanbieders en woningcorporaties. Het doel van de CT&R vloeit voort uit de Wmo 2015 waarbij de inzet gericht is op het bieden van ondersteuning bij zelfredzaamheid en deelname aan de samenleving. Het traject via de CT&R bevordert het maatschappelijk herstel van de cliënt.

Onderdeel van de pilot CT&R is om te onderzoeken of en zo ja op welke wijze gegevensdeling ten behoeve van andere gemeentelijke voorzieningen (bijvoorbeeld inkomen, schuldhulpverlening of andere vormen van Wmo ondersteuning) verenigbaar is het doel waarvoor de CT&R gegevens verwerkt. Tijdens de pilotfase wordt onderzocht of en in welke mate afstemming vanuit de CT&R met instanties plaatsvindt, hoe deze afstemming verloopt en wat daarbij de behoefte is van instanties aan eventueel te delen gegevens. Zoals eerder gesteld verleent de cliënt toestemming aan de CT&R voor het contact opnemen met instanties als dat nodig is om voortgang te houden of te brengen in het uitstroomtraject. Contact met instanties is nodig omdat instanties verantwoordelijk zijn/ mandaat hebben voor het treffen van voorzieningen. De ervaring leert dat instanties niet altijd goed samenwerken en er langs elkaar heen gewerkt wordt. Dit vraagt dan om coördinatie die voor een cliënt zelf haast niet is op te brengen en ook niet altijd door een trajectbegeleider tot stand kan worden gebracht. De regie functie van de CT&R en het feit dat het een gemeentelijke organisatie is levert naar verwachting meer doorzettingskracht op in de afstemming met instanties. Omdat we dit nog niet eerder zo hebben gedaan is het op voorhand niet goed mogelijk om hierin een uitputtende opsomming in te maken. Deels zal het proefondervindelijk tot stand komen.

Voor het einde van de pilot periode zal geëvalueerd worden wat de ervaringen en behoeften zijn en de DEPIA zal daarop worden geactualiseerd.

Zoals eerder in deze DEPIA vermeld worden de in [5.1.2i] verwerkte gegevens gebruikt voor het maken van dashboards in [5.1.2i].

Advies FG: Helder en akkoord, mooi dat de uitkomsten van de evaluatie opgenomen worden in deze DEPIA, waarna het traject van advies weer gevolgd gaat worden.

10. Betrouwbaarheid, veiligheid & transparantie;
Beschrijf de randvoorwaarden zoals betrouwbaarheid, veiligheid, transparantie door de volgende vragen te beantwoorden. Beschrijf welke maatregel welk risico aanpakt. (vraag de security officer)

10.1 Welke technische/organisatorische/juridische (zoals beveiliging, wachtwoorden, een verwerkersovereenkomst) maatregelen zijn genomen om de betrouwbaarheid van de toepassing te borgen?

WCAG 2.1 voor websites
Leverancier is ISO 27001 en Nen7510 gecertificeerd
Pen-tests worden jaarlijks uitgevoerd. De onderdelen waarop de Pen-test wordt uitgevoerd staan genoemd in de verklaring van toe assin De verklarin staat in de [5.1.2i]-zaak van CLM-Contract Leveranciers Management van [5.1.2i] contract [5.1.2i].

Momenteel wordt door de medewerkers van het Transferpunt gewerkt in een op Excel gebaseerde uitstroommonitor. Hiervoor is indertijd een Epia uitgevoerd. Deze DEPIA is in vervolg hierop. Indertijd is al aangegeven dat het werken met een Excel applicatie niet ideaal was en dat er mede daarom gekeken werd om op termijn in [5.1.2i] te gaan werken. Voorliggende DEPIA is daar het gevolg van.

[5.1.2i] is zoals in voorgaande delen van deze DEPIA is toegelicht een betrouwbaar en gekend systeem waarin gegevens zorgvuldig en conform daarvoor geldende specificaties en standaarden wordt verwerkt. Medewerkers van de CT&R beschikken over een eigen account en middels autorisaties is het mogelijk om (delen van) [5.1.2i] voor anderen af te schermen. Toegang tot [5.1.2i] verloopt via een gebruikersnaam en wachtwoord.

Ten behoeve van de pilot fase CT&R waarmee in 2024 gestart wordt zullen medewerkers van betrokken zor aanbieders (Limor, Wender en het Leger des Heils) geworven worden die ook met [5.1.2i] gaan werken. Tussen gemeente Leeuwarden/ SDF en Wender, Limor en het Leger des Heils worden samenwerkingsovereenkomsten afgesloten over de uitleen van medewerkers aan de

CT&R. De medewerkers komen als het ware in dienst van gemeente Leeuwarden/ SDF. De vorm is nog onderwerp van gesprek. De samenwerkingsovereenkomst wordt opgesteld door de juridisch adviseur van gemeente Leeuwarden. Alle medewerkers van de CT&R werken vanuit hun eigen account van de gemeente Leeuwarden (laptop, telefoon, mail). Hiervoor worden overeenkomsten opgesteld die de vertrouwelijke omgang met de gegevens zullen borgen (geheimhoudingsplicht etc.).

De gegevensverwerking in 5.1.2i zal geanonimiseerd worden gepresenteerd in rapportages en verantwoordingen. Voor medewerkers van de CT&R is de data ook niet-geanonimiseerd inzichtelijk ten behoeve van caseload management en het opsporen van fouten en leemten in de data (in algemene zin het op orde brengen en houden van de datakwaliteit).

Het delen van gegevens in de 5.1.2i kanalen vindt beveilig plaats. Deelnemen aan een kanaal is alleen mogelijk op basis van een persoonlijk account. De deelnemende medewerkers van betrokken instanties zijn gehouden aan de vertrouwelijke omgang met de gedeelde gegevens en zijn daarin gebonden aan de AVG en de interne regelgeving van hun moederorganisaties. Nieuwe deelnemers kunnen alleen door een medewerker van de CT&R worden toegevoegd. Er is geen rechtstreekse koppeling tussen 5.1.2i en 5.1.2i Gegevens worden handmatig geplaatst. Na afronding van een traject wordt de informatie uit het 5.1.2i Kanaal verwijdert door de CT&R.

In principe mogen er geen cliënt gerelateerde documenten worden opgeslagen buiten 5.1.2i om op schijven, anders dan persoonlijke notities van medewerkers die geen naar cliënten herleidbare informatie bevatten. Het opvragen en opslaan van “wat-informatie” zoals diagnoses etc. wordt tot een minimum beperkt.

Indien er e evens er mail worden gedeeld dan gebeurt dat met externen uitsluitend op beveiligde wijze met 5.1.2i of een ander vergelijkbaar systeem.

Advies FG: Akkoord. Wederom zeer uitgebreid geformuleerd.

10.2: Welke technische/organisatorische/juridische maatregelen zijn genomen om de veiligheid te borgen?

Juiste aanbestedingen qua vorm en inhoud, juridische contracten en technische eisen (autorisaties, logging, 2FA etc. etc.).

De autorisatie matrix voor 5.1.2i beschrijft wie, in welke rol waarvoor geautoriseerd is. De accounts in 5.1.2i zijn persoonsgebonden. De aanvraag voor een account in 5.1.2i verloopt via de manager van SDF. Voor de overige technische en juridische maatregelen wordt verwezen naar wat in 10.1 en in 11.3 staat beschreven.

5.1.2i is geen nieuw systeem wat door de CT&R voor het eerst gebruikt gaat worden. Ten behoeve van de CT&R is een nieuw zaaktype toegevoegd. Dit zaaktype is net als alle andere zaaktypen in 5.1.2i onderhevig aan de technische en juridische maatregelen die genomen zijn voor 5.1.2i als systeem.

Advies FG: Helder en akkoord.

10.3: Welke maatre elen zijn genomen om de transparantie van de toepassing te borgen?

Het zaaktype in 5.1.2i is zodanig vormgegeven dat er weinig onduidelijkheid bestaat over wat er specifiek wordt gevraagd. Er worden veel gesloten vra en esteld met een gelimiteerd aantal antwoordmogelijkheden. De open tekstvelden staan in 5.1.2i zelf en worden als zodanig ook opgeslagen in 5.1.2i en zijn daarmee altijd vindbaar. Er worden geen cliënt gerelateerde documenten buiten 5.1.2i om opgeslagen. Een uitzondering vormt mogelijk het zaaksysteem van gemeente Leeuwarden van waaruit correspondentie met inwoners wordt gearchiveerd.

De casemanager informeert de cliënt tijdens de intakefase actief wat de achtergrond is van de vragen die gesteld worden. Het ondersteuningsplan geeft weer wat over de benodigde ondersteuning op de levensgebieden is besproken en afgesproken. De cliënt ondertekent het ondersteuningsplan voor gezien. De cliënt kan ten allen tijde in overleg met de CT&R over de voortgang van het traject. We gaan een folder ontwikkelen om de cliënten te informeren over het hoe en wat van de CT&R. Deze folder zal op de website worden gepubliceerd en beschikbaar zijn op de plekken waar cliënten zich melden.

Advies FG: Helder en akkoord.

Adviseur data-ethiek:
Akkoord

11. Afweging;
Afweging van alle onderdelen in het kader van ethiek, privacy en informatieveiligheid.

11.1: Kan hetzelfde doel op een andere manier worden bereikt (subsidiariteit)? Leg uit waarom wel/niet.

Momenteel worden gegevens uitgevraagd door zorgaanbieders (Wender, Limor, Leger des Heils en VNN) en deze worden door middel van formulieren in Word gedeeld met het Transferpunt. Het verwerken in 5.1.2i is een automatisering en professionalisering van dat proces. En doordat de gegevensverwerking wordt gecentraliseerd treed er geen/ minder versnippering van gegevensopslag meer op. Dit bevordert de privacy en de informatieveiligheid.

Advies FG: Duidelijk, dat door deze manier van werken en het toepassen van 5.1.2i er een proces ontstaat dat privacy en informatiebeveiliging bevorderend is.

11.2: Kan hetzelfde doel met minder gegevens worden bereikt (proportionaliteit)? Leg uit waarom wel/niet.

Vanuit de CT&R wordt met behulp van 5.1.2i breed gekeken naar de verschillende levensgebieden waarop sprake is van kwetsbaarheid en waar ondersteuning nodig is. De medewerkers worden voorafgaand aan de start van de pilot getraind in het gebruik van 5.1.2i 5.1.2i en het uitvoeren van de intake. Daarnaast zijn- en worden er werkinstructies ontwikkeld voor de omgang met specifieke situaties. In de training en opleiding van de medewerkers wordt uitgebreid stilgestaan bij wat de bedoeling is van de zaakstappen en hoe daar mee om te gaan bij de rolinvulling. De medewerkers gaan periodiek om de tafel met elkaar om te bespreken hoe er gewerkt wordt en om ervaringen te delen.

Hoewel alle zaakstappen in 5.1.2i doorlopen moeten worden zal het niet in alle gevallen nodig zijn om volledig te zijn. Van belang is om alle bij langs te lopen en er bij de cliënt naar te vragen. Voorkomen moet worden dat er belangrijke informatie over het hoofd wordt gezien. Het ontbreken van relevante informatie, bijvoorbeeld over schulden, kan later in het uitstroomproces namelijk voor vertraging of stagnatie zorgen.

De casemanager bepaalt wat wordt vastgelegd in 5.1.2i. In voorkomende gevallen kan worden volstaan met de mededeling “n.v.t.”. Bij de rol van casemanager hoort dat de casemanager op basis van het contact met de cliënt een professionele beoordelin doet van wat de cliënt vertelt. De waarneming van de casemanager wordt vastgelegd in 5.1.2i als dit een basis vormt voor de afspraken over doelen in het ondersteuningsplan. In feite vormt wat de casemana er in 5.1.2i 5.1.2i opschrijft een gespreksverslag. Medewerkers beschikken binnen 5.1.2i over een notitieblad waar persoonlijke notities kunnen worden vastgelegd. Deze zijn niet openbaar.

De CT&R is gericht op het verkorten en beëindigen van dakloosheid. Uit ervaring en op basis van kennis en inzicht is bekend dat achter dakloosheid vaak problematiek speelt op veel verschillende levensgebieden. Om gericht en effectief passende zorg en ondersteuning te kunnen bieden en om goed te kunnen toeleiden naar een passende vorm van verblijf of wonen is het noodzakelijk om breed te kijken. Dat gezegd hebbende is het niet noodzakelijk dat in alle gevallen altijd alles gedetailleerd ingevuld moet worden. Als blijkt dat op één of meerdere levensgebieden geen acute/ zorgwekkende of ernstige problematiek speelt dan kan de medewerker van de CT&R besluiten de betreffende vragen eenvoudig af te doen. De vraagstelling is verder zodanig in 5.1.2i geprogrammeerd dat op basis van voorwaardelijkheden vragen overgeslagen kunnen worden afhankelijk van het gegeven antwoord. De hoeveelheid daadwerkelijk geregistreerde gegevens is daarmee afhankelijk van de breedte en diepte van de problematiek bij de cliënt.

Gezien de doorgaans complexe problematiek bij dakloze mensen is het daarom wenselijk om breed te kunnen kijken en onderzoeken om daarmee een goede aanpak te kunnen vormgeven.

Tevens is het zo dat gemeenten taken en verantwoordelijkheden hebben op het gebied van preventie, ondersteuning, opvangcapaciteit, inkoop, wonen, welzijn etc. De informatie die voortvloeit uit een goede registratie levert daarmee relevante data op die ingezet kan/ moet worden ten behoeve van beleidsontwikkeling, aanbestedingen, regelgeving en woningbouwprogrammering.

Advies FG: Akkoord. Ik zou graag zien, dat in de evaluatie wordt bekeken of daadwerkelijk alle informatie ook uitgevraagd en verwerkt moet worden. Ik doel daarmee vooral op de informatie rondom de kinderen, gezondheid en diagnostiek.

11.3: Wat zijn de negatieve gevolgen en de genomen maatregelen voor de betrokkenen
Beschrijf en beoordeel risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Noem ook de risico's voor de waarden vanuit vraag 3.1;

Negatieve gevolgen	**Oorzaak hiervan**	**Impact**	**Maatregel**	**Geïmplementeerd door**
1. Datalek	Delen van persoonsgegevens door medewerker CT&R waar dat niet mag/gewenst is	Hoog	Informeren en trainen van bewustwording bij medewerkers over veilig en zorgvuldig omgaan met persoonsgegevens.	Management SDF/Leeuwarden
2. 5.1.2i	Gegevens inwoners in verkeerde handen	Hoog	5.1.2i en de leverancier heeft alle benodigde beveiligingsaudits doorstaan en geeft hierover TPM-verklaringen en digitale certificaten uit. Er is een VWO afgesloten. De voorziening kan met 1 druk op de knop uit de lucht worden gehaald.	Shared 5.1.2i Centrum/Informatiemanagement/Functioneel Beheer
3. Meer gegevens verwerken dan afgesproken	Medewerker vraagt meer gegevens dan waar in de zaakstappen naar gevraagd wordt.	Hoog	Op trainen en in de werkinstructie vermelden om zeer terughoudend te zijn in het uitvragen van zaken die niet vermeld zijn in het zaaktype MO en afspreken om het opslaan van documenten in MC tot een minimum beperken.	SDF
4. Gegevens voor een ander doel verwerken	Derde partijen vragen om in 5.1.2i verwerkte gegevens op	Hoog	Het delen van gegevens voor een ander doel is niet toegestaan zonder het akkoord van een daarvoor gemandateerde manager inclusief een advies van de Privacy Officer	Management SDF/Leeuwarden
5. Betrokkenen onvoldoende informeren	Medewerker CT&R vergeet of laat na betrokkenen te informeren over de gang van zaken en de verwachtingen over en weer	Medium	In de werkinstructie, werkprocessen en in het zaaktype zijn de momenten waarop betrokkenen wordt geïnformeerd aangegeven. Het ondersteuningsplan wordt getekend door betrokkene.	Management SDF/Leeuwarden
6. Onjuiste of onvolledige gegevens verwerken	Betrokkene kan zelf niet beschikken over juiste en volledige informatie. Er kan verwarring ontstaan over de identiteit van de betrokkene. Medewerker CT&R kan slordig werken.	Hoog	Alle zaakstappen zijn zodanig geformuleerd dat de kans op interpretatie fouten e.d. zo veel mogelijk is geminimaliseerd. Het risico is niet volledig uit te sluiten. Doordat betrokkene ook zelf het ondersteuningsplan ondertekent is het risico dat ongezien onjuiste gegevens zijn verwerkt kleiner. In het traject zelf	Management SDF/Leeuwarden

			zijn er diverse momenten waarop voortgang met cliënt en andere betrokkenen wordt besproken dat onvolledigheid snel aan het licht komt.	
7. Gegevens en/of applicatie tijdelijk niet beschikbaar	Stroomuitval, onderhoud, storing etc.	Laag	E.e.a. hang af van hoe lang het duurt dat de gegevens of applicatie tijdelijk niet beschikbaar zijn. Er van uitgaande dat de gegevens niet voor altijd zijn verloren en niet gewijzigd worden als het gevolg van het tijdelijk niet beschikbaar zijn, zijn er vanuit de CT&R geen aanvullende maatregelen nodig. Bij langdurig niet beschikbaarheid zijn kan er teruggevallen worden op de gegevens die in geko elde systemen staan (5.1.2i en 5.1.2i). De leverancier levert de brondata via een MI-datadump. Deze leest IM in, in het Datawarehouse. Gegevens worden geanonimiseerd (standaard werkmethode) en kunnen gebruikt worden in Mana ement informatie rapporten via 5.1.2i . De leverancier bewerkt dus de gegevens niet maar heeft binnen de applicatie wel standaard rapporten beschikbaar (ook in de SOM-applicatie staan standaard rapporten maar deze worden niet vaak gebruikt) De leverancier levert alleen de ruwe data in de eerdergenoemde MI-dump. Wij (IM) zelf halen deze informatie op en slaan deze op, op eigen servers om ze vervolgens geanonimiseerd in te lezen. Als blijkt dat de verwerking in het DWH-datawarehouse goed is gelukt wordt na een bepaalde tijd de MI-dump verwijderd.	Management SDF/Leeuwarden
8. Koppelingen werken niet goed	Technische storingen binnen de respectievelijke applicaties	Midden	Als de koppeling met de 5.1.2i niet goed werkt zal het niet mogelijk zijn om in 5.1.2i een nieuwe zaak aan te maken. Het is niet mogelijk dat een	SSC

			storing bij een koppeling niet wordt opgemerkt. SSC collega's zullen aan de slag gaan om de storing te verhelpen.	
9. Gegevens te lang of te kort bewaren	Onduidelijkheid over bewaartermijnen en/of het niet functioneren van automatische signalering in de gebruikte applicaties	Midden	Het bepalen van de termijnen in de applicatie en het programmaren van signalering in de applicatie. En daarnaast in werkinstructies opnemen wat, wanneer en door wie verwijderen van gegevens. Bij het afsluiten van een traject worden de gegevens uit 5.1.2i verwijderd.	SSC en Management SDF/Leeuwarden
10. Gegevens delen met anderen die er geen recht op hebben	Het onterecht autoriseren van personen voor toegang tot applicaties. Of het (on)opzettelijk onterecht delen van gegevens door een medewerker CT&R met anderen.	Hoog	Het autoriseren van (nieuwe) gebruikers van de applicaties laten verlopen na akkoord van manager en de feitelijke autorisatie uitvoeren door medewerker SSC. Alle medewerkers CT&R zijn getraind en opgeleid in het gebruikt van de applicaties. En medewerkers ondertekenen verklaringen waarin zij geïnformeerd zijn over rechten en plichten verbonden aan het gebruik van de applicatie. Sancties op het opzettelijk onterecht delen van gegevens zijn bekend gemaakt.	Management SDF/Leeuwarden en SSC
11. Gegevens niet veilig uitwisselen of delen	Het (per ongeluk) versturen van gegevens via een onbeveiligde lijn door een medewerker van de CT&R.	Hoog	In de werkinstructie opnemen dat gegevens niet of anders bij hoge uitzondering per mail worden gedeeld. De medewerkers zijn getraind in het gebruik maken van 5.1.2i (of een toekomstige vergelijkbaar door gemeente Leeuwarden in gebruik genomen alternatief). Het bewust niet beveiligd versturen van gegevens is een fout en wordt door de coördinator of teamleider met de medewerker besproken. Afhankelijk van de aard/ ernst van het voorval kan	Management SDF/Leeuwarden en SSC

			de teamleider een passende maatregel nemen.	
12. Klant voelt de druk om uit te stromen als “het niet serieus genomen” worden of als aantasting van zijn of haar waardigheid.	De CT&R heeft ook als taak om dakloze mensen zo snel mogelijk toe te leiden naar een passende vorm van verblijf. De snelheid waarmee dit “moet” kan ervaren worden als te snel.	Midden	In de werkinstructie naar de medewerkers van de CT&R toelichten en uitwerken dat het handelen naar de letter van de wet en in de geest van de wet hand in hand gaan. De Mens staat Centraal en een succesvol uitstroomtraject staat en valt met de motivatie van de klant om uit te stromen. Meebewegen met het tempo van de klant hoort daarbij maar staat actieve regie niet in de weg.	Management SDF/Leeuwarden en SSC
13. Het gevoel of ervaring bij de klant dat zijn of haar privacy van de klant onvoldoende gewaarborgd is.	Tijdens de intake wordt in relatief korte tijd veel gevraagd aan de klant.	Midden	In de werkinstructie en tijdens de training en opleiding van de medewerkers CT&R wordt uitgebreid stilgestaan bij de kwaliteit van het klantcontact. Onderdeel van het casemanagement is om structureel uit te leggen waarom informatie wordt uitgevraagd, wat er mee gedaan wordt en waar het toe moet leiden.	Management SDF/Leeuwarden en SSC
14. Het gevoel of ervaring bij de klant dat zijn of haar autonomie onder druk staat	De klant kan zich overgeleverd en daarin zich volledig afhankelijk voelen van de CT&R voor het “in traject” komen.	Hoog	In de werkinstructie en tijdens de training en opleiding van de medewerkers CT&R uitgebreid stilstaan bij de vaardigheden die nodig zijn om (nieuwe) klanten tijdens de intake op hun gemak te stellen, laagdrempelig te zijn, niet bedreigend, perspectief te bieden en de klant ook positief aan te spreken op de eigen autonomie. De klant heeft wat te kiezen en de CT&R is er voor om de klant daarbij te helpen. Tegelijkertijd helder en transparant zijn over de rechten en plichten.	Management SDF/Leeuwarden en SSC
Advies FG: Helder en akkoord.				
Adviseur data-ethiek: Akkoord				

11.4: Zijn er rest-risico's en zo ja, welke? Leg ook uit waarom.

Voor zover dit is te overzien niet.
Advies FG: Akkoord.
Adviseur data-ethiek: n.v.t.

11.5: Zijn er (verwerkers)overeenkomsten gemaakt met betrokken externe artijen? Zo ja, voeg deze dan toe als bijlage (en sla deze op in het zaaksysteem en in 5.1.2i onder het contract met de leverancier)

Er is al een verwerkersovereenkomst met de leverancier van 5.1.2i. Met de deelnemende zorgaanbieders wordt een samenwerkingsovereenkomst afgesloten. Alle medewerkers van de CT&R worden middels een onderliggende overeenkomst (detachering) aangesteld en kunnen uitsluitend werken in gemeentelijke systemen op basis van een account binnen de gemeente Leeuwarden. Zorgaanbieders zijn zelfstandig verwerkingsverantwoordelijke voor de persoonsgegevens die zij verwerken, net zoals de gemeente dit is voor de persoonsgegevens die wij verwerken.

Eindoordeel Functionaris voor Gegevensbescherming: Akkoord. Voor de evaluatie is afgesproken dat dan ook wordt bekeken of daadwerkelijk alle informatie ook uitgevraagd en verwerkt moet worden. Daarbij gaat het om de informatie rondom de kinderen, gezondheid en diagnostiek **Datum: 23-09-2024**

Beoordeling (door management/bestuur)	**Is de beoordeling openbaar, vertrouwelijk, zeer vertrouwelijk of geheim**

Waar wordt de beoordeling opgeslagen (voeg zaaknummer 5.1.2i toe)

Startdatum verwerkingen (indien van toepassing)	**Wanneer bijwerken register (indien van toepassing)**	**Datum herziening DEPIA (indien van toepassing)**
	De verwerking staat nog niet in het register. Dit volgt na afloop van het DEPIA traject.	

Bijlagen

Functioneel ontwerp zaaktype Maatschappelijke Opvang

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 26
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 17, 18, 19, 20, 21, 22, 23, 26, 27, 28, 29, 30, 31, 32, 34

DEPIA

Digitale Meldplicht – fase 1 (Mini-ID)

Verwerkingsverantwoordelijke:	Burgemeester
Sector/Afdeling/Team:	Juridische en Veiligheidszaken, teams OOV en JZ
Pre-DEPIA uitgevoerd:	Nee. Vanuit de landelijke Werkgroep Digitale Meldplicht is het Ministerie van JenV betrokken, daar is eerder beoordeeld dat een DPIA vereist is voor fase 1 van de Digitale Meldplicht
Data-ethische reflectie:	Via deze DEPIA
Datum DEPIA:	14 april 2025
Zaaknummer:	2024-156323

Gemeente Leeuwarden

1 Algemeen

Het verwerken van persoonsgegevens kan een hoog privacyrisico opleveren voor de betrokken personen. Is dit het geval? Dan is het verplicht vooraf de risico's te onderzoeken. En maatregelen in kaart te brengen die deze risico's wegnemen of verkleinen. In Leeuwarden onderzoeken we niet alleen de privacyrisico's maar ook de ethische dilemma's van gegevensverwerkingen. Dit noemen we een DEPIA: Data en Data-ethische Protection Impact Assessment.

Zijn er na het uitvoeren van de DEPIA belangrijke restrisico's? En kunnen we deze niet beperken? Dan moeten we de gegevensverwerking eerst voorleggen aan de Autoriteit Persoonsgegevens (AP). Dit is een voorafgaande raadpleging. Verder voeren we iedere drie jaar een herbeoordeling van de DEPIA uit. Dit doen we ook bij ingrijpende wijzigingen van een bestaande gegevensverwerking.

Leeswijzer

Na dit algemene hoofdstuk is de DEPIA als volgt opgebouwd:

- Hoofdstuk 2 Persoonsgegevens
- Hoofdstuk 3 Baten en data-ethiek
- Hoofdstuk 4 Beveiligingsmaatregelen
- Hoofdstuk 5 Risico's en maatregelen
- Hoofdstuk 6 Conclusies en aanbevelingen

Aan het eind volgen wat algemene gegevens, beoordeling proceseigenaar en aandachtspunten.

1.1 Wie zijn betrokken bij de DEPIA?

Geef aan wie betrokken zijn bij het uitvoeren van de DEPIA. Vul aan waar nodig.

Proceseigenaar (teamleider/manager)	5.1.2e
Projectleider	5.1.2e (lokaal) / 5.1.2e (Ministerie JenV)
Privacy Officer (PO)	5.1.2e
Data-ethiek Officer (DO)	5.1.2e
Information Security Officer (ISO)	5.1.2e
Functionaris Gegevensbescherming (FG)	5.1.2e

1.2 Wat ga je doen?

Hoe ziet het project/proces eruit, wat zijn de stappen of fasen, de applicatie(s), hoe ga je de persoonsgegevens gebruiken en zijn er acties zonder tussenkomst of beoordeling van een medewerker? Maak bij voorkeur ook een plaatje of schematische weergave van het proces.

Deze DEPIA heeft betrekking op fase 1 van de **Digitale Meldplicht**, waarbij gebruik wordt gemaakt van een device genaamd '**Mini-ID'**.

Dit experiment is voorbereid door een landelijke werkgroep onder leiding van een projectteam van het Ministerie van JenV. De gemeente Leeuwarden is één van de deelnemende gemeenten, naast Utrecht en Rotterdam; gemeenten met een Betaald Voetbal Organisatie (BVO) derhalve. Gekeken wordt naar de mogelijkheden om de digitale meldplicht toe te passen naar aanleiding van openbare ordeverstoringen rond betaald voetbal ('hooliganism').
Het experiment heeft tot doel, kort gezegd, het realiseren van een digitale faciliteit waarmee de reeds bestaande wettelijke mogelijkheid – op grond van artikel 172a, eerste lid, aanhef en onder c, van de Gemeentewet – om (al dan niet in combinatie met een gebiedsverbod) een meldplicht op te leggen aan een betrokkene, deze ook in digitale variant kan worden opgelegd door de burgemeester en kan worden gehandhaafd. Deze wettelijke mogelijkheid bestaat al sinds 2015, waarbij de formele wetgever – zo blijkt uit de parlementaire geschiedenis – ook heeft beoogd de digitale variant van de meldplicht mogelijk te maken. Tot dusver is alleen de fysieke variant (bv. melden op politiebureau) toegepast omdat er geen geschikte techniek voorhanden was om het digitaal melden te faciliteren.
Dit betreft zaken waarin betrokkenen zijn betrokken bij ernstige en/of herhaaldelijke (groepsgewijze) ordeverstoringen. De burgemeester kan zo'n maatregel dan opleggen in het belang van de openbare orde en veiligheid. De (digitale) meldplicht is bedoeld om deze werking te versterken. De burgemeester legt deze aan een betrokkene op (na zorgvuldige voorbereiding en besluitvorming), daarmee is het een bevel van de burgemeester en geen vrije keuze van een betrokkene.

In dit project wordt nu nadrukkelijk gekeken naar het toepassen van de Mini-ID (zie hieronder voor nadere toelichting) als digitale meldfaciliteit, in combinatie met een gebiedsverbod (op grond van artikel 17, eerste lid, aanhef en onder a, Gemw). Voorafgaand aan fase 1, waarop deze DEPIA ziet, is er begin 2024 ook een fase 0 geweest waarin door pseudomeldplichtigen (lees: een groep vrijwilligers, bestaande uit medewerkers van gemeenten, politie, ministerie JenV) enige tijd is geoefend met de Mini-ID; deze groep heeft gedurende langere periode een Mini-ID gekregen, waarmee elke pseudomeldplichtige – op grond van een fictief gebiedsverbod dat op bepaalde tijden van kracht was – zich diende te melden. Fase 0 is, kort samengevat, positief verlopen, heeft geleid tot enkele technische aanpassingen en uiteindelijk tot de conclusie dat de Mini-ID een geschikte meldfaciliteit is voor toepassing in fase 1.

In fase 1 wordt het gebruik van deze Mini-ID proefondervindelijk onder de loep genomen, door deze in 'echte zaken' toe te passen. Verdere uitrol van dit middel/deze mogelijkheid naar landelijke toepassing, is voorzien in fase 2. Die vindt niet eerder plaats dan na evaluatie van fase 1 (nadere invulling van deze evaluatie moet nog plaatsvinden).

> *NB. Naast de digitale variant, kan een meldplicht ook fysiek worden opgelegd. Landelijk wordt deze fysieke meldplicht al wel toegepast, zij het dat dit vanuit een oogpunt van proportionaliteit juridisch lang niet altijd houdbaar is. Deze fysieke variant beperkt de betrokkene in (veel) grotere mate in zijn/haar vrijheid dan een digitale meldplicht; de betrokkene dient zich dan op gezette tijden te melden op een specifieke locatie (bv. een politiebureau) terwijl dat voor de digitale variant niet noodzakelijk is: dan dient de betrokkene alleen buiten het verboden gebied te blijven. De digitale meldplicht maakt derhalve in veel geringere mate inbreuk op de bewegingsvrijheid van de betrokkene. Tegelijkertijd is het een zeer effectieve wijze om het opgelegde gebiedsverbod te handhaven. Uit een oogpunt van evenredigheid (geschiktheid/effectiviteit, noodzakelijkheid en evenwichtigheid) is dat een cruciale verbetering ten opzichte van de fysieke meldplicht. Dit maakt de deelname van de gemeente Leeuwarden aan dit project waardevol.*

Naast de genoemde gemeenten en het Ministerie van JenV nemen ook deel aan het project en deze fase van de Digitale Meldplicht:

- de Dienst Vervoer en Ondersteuning (DV&O), vanuit diens huidige rol bij het monitoren middels Mini-ID bij TBS-ers;
- Het Openbaar Ministerie;
- De politie.

Met betrekking tot de rol van de politie en DV&O moet verder het volgende worden opgemerkt. Het monitoren van de naleving van de digitale meldplicht valt buiten de feitelijke handhaving van de openbare orde door de politie. Dit toezicht op de naleving van de digitale meldplicht, is hier een schakel die voorafgaat aan de feitelijke handhaving door de politie (en die ontbreekt bij de fysieke meldplicht). Voor deze schakel wordt DV&O door de gemeenten aangewezen als toezichthouder (bestuursrechtelijk). DV&O houdt dan toezicht op de naleving van de digitale meldplicht. De politie ontvangt een melding van de toezichthouder als deze constateert dat de digitale meldplicht niet wordt nageleefd. Daarop kan de politie feitelijk handhaven. De gegevensverwerking door de toezichthouder bij DV&O valt onder het regime van de AVG (onder verwerkingsverantwoordelijkheid van de burgemeester). Als de politie feitelijk handhaaft, wordt het een verwerking binnen het regime van de Wet politiegegevens (WPG) onder verantwoordelijkheid van de korpschef. Dit betreft een 'regulier' proces dat ook geldt in andersoortige informatieverstrekking van politie naar gemeente in het kader van de openbare orde en veiligheid. (*Aanvulling op de rollen van partijen, aanbeveling 7 en 10 in advies FG's 21 maart 2025.)*

Onderaan deze toelichting staat een processchema waaruit blijkt welke rol voornoemde instanties hebben in fase 1. Verder zijn een aantal scenario's, waarvan de verwachting vanuit het project is dat deze de meest-voorkomende situaties afdekken, opgenomen in zgn. opvolgprotocollen. In deze opvolgprotocollen is stapsgewijs opgenomen welke acties er door welke partij moeten worden gezet in bepaalde scenario's. Als voorbeeld: in de opvolgprotocollen is opgenomen wat er gebeurt als een melding via de Mini-ID mislukt of überhaupt niet wordt ontvangen. Dergelijke situaties leiden mogelijk tot vervolgstappen voor verschillende partijen. In eerste instantie komt de informatie over het niet-succesvol melden in de software (5.1.2i), en dan is er in verschillende situaties nog een stap te zetten door het monitoringscentrum van DV&O of automatisch (ingeregeld via 5.1.2i) in de vorm van een extra contactmoment met de betrokkene. Als vervolgens een succesvolle melding uitblijft beschrijven de protocollen wanneer de politie worden geïnformeerd, waar vervolgens de zaak wordt beoordeeld (mogelijke overtreding of niet?). Afhankelijk van die beoordeling wordt de burgemeester geïnformeerd door de politie (middels een bestuurlijke rapportage). De opvolgprotocollen beschrijven dit proces stapsgewijs en in verschillende scenario's.

Voor wat betreft de **werking** van de Mini-ID kan verder nog het volgende worden opgemerkt:
De Mini-ID is een GPS-device met biometrie, online is e.e.a. aan informatie te vinden over de werking van dit apparaat[1]. De Mini-ID wordt aan de digitaal meldplichtige verstrekt voor de gehele duur van het aan hem/haar opgelegde gebiedsverbod en die hij/zij bij zich moet dragen op momenten dat zijn/haar gebiedsverbod geldt (lees: in een tijdsbestek van 2 u voorafgaand tot 2 u na afloop van betaald voetbalwedstrijden in het Kooistadion in Leeuwarden). Gedurende die tijdsbestekken werkt de Mini-ID automatisch en vraagt deze meldingen (door middel van vingerafdruk) uit bij de betrokkene. Aldus kan worden gecontroleerd of de digitaal meldplichtige zich bevindt in verboden gebied[2]. Tijdens voormeld tijdsbestek zal een aantal (in beginsel 3) meldingen worden 'uitgevraagd', waarop de betrokkene zich middels vingerafdruk moet melden via de Mini-ID.

De Mini ID is dus een apparaat dat voorziet in het kunnen controleren van een vingerafdruk om identificatie van de drager van de Mini ID te faciliteren. Daarnaast kan de Mini ID, wanneer dat nodig is, locatie-informatie van het apparaat verzenden. Het apparaat is niet ontwikkeld om een on-device controle van een gebied te kunnen faciliteren. Het apparaat zou daartoe compleet anders opgebouwd moeten worden, met veel meer geheugen en rekenkracht aan boord. Het is vanuit het ontwerp van het apparaat nooit de intentie geweest om het op een dergelijke manier vorm te geven. Feitelijk is deze mogelijkheid er

[1] Zie bv. https://fcc.report/FCC-ID/ZDLST10/7100043.pdf

[2] Als een gebiedsverbod wordt opgelegd, wordt daarbij (per individueel geval) het verboden gebied vastgesteld. In beginsel wordt daarbij aangehouden: het gebied dat rondom het Kooi stadion is gesitueerd en dat wordt omsloten door de volgende straten: Heliconweg, Marnixstraat, Brederostraat, Van der Nootstraat, Harlingertrekweg, Snekertrekweg, Marshallweg, Zwettestraat, James Wattstraat, Fahrenheitweg, Archimedesweg, Einsteinweg, Bisschopsrak, Simon Vestdijkwei, Piter Terpstrawei, Poptawei, Harlingerstraatweg, Europaplein. De straten zelf tellen ook mee voor het stadiongebiedsverbod.

derhalve niet. Het niet faciliteren van een on-device check van een gebiedsverbod heeft ten aanzien van dataminimalisatie en mogelijk misbruik van het apparaat voordelen (zie hieronder). Deze wijze van functioneren van de Mini ID brengt wel mee dat data naar de (backend van) de software 5.1.2i – zie verderop) wordt gestuurd, teneinde – kort gezegd – de controle op juiste naleving van de meldplicht te kunnen doen.

In de wisselwerking tussen het apparaat en software heeft de leverancier gekozen voor het kunnen faciliteren van (meerdere) verboden gebieden in een softwareomgeving waar deze rekenkracht beschikbaar is: 5.1.2i, de monitoringssoftware waar de medewerkers van het Monitoringscentrum hun werk doen.De gekozen oplossing is de meest passende omdat enkel op het moment van melden de locatiegegevens van de meldplichtige worden doorgegeven. De data die wordt doorgegeven betreft de volgende data:

1. De unieke identificatie van de Mini ID (het mini ID nummer)
2. De Verificatie (OK of Niet OK)
3. de vastgestelde locatie op moment van melden.

Ad. 1: Het Mini ID nummer (MID/MIE….) betreft een uniek apparaatnummer. Hiermee is identificeerbaar om welk apparaat het gaat.
Ad. 2: De verificatie betreft de check op vingerafdrukken. Bij ingebruikname van de Mini ID worden er 4 vingerafdrukken vastgelegd op het apparaat (2 per hand). Deze vingerafdrukken worden op het apparaat zelf vastgelegd en verlaten het apparaat niet.
Ad. 3: De locatie-informatie betreft lattitude-longitude details op moment van melden.
Deze informatie is op moment van verzenden onpersoonlijk en pas herleidbaar tot een meldplichtige wanneer er sprake is van een mogelijke overtreding. Dit past binnen de beginselen van privacy by design, omdat de data-uitwisseling naast minimaal ook niet op personen herleidbaar is. De data uit de Mini ID wordt pas op persoon herleidbaar op moment van binnenkomst in het monitoringscentrum omdat dan de data van de mini ID gekoppeld wordt aan de persoon die administratief aan de Mini ID is gekoppeld.

Daarbij zijn er twee scenario's te onderscheiden:
1. De meldplichtige voldoet aan zijn meldplicht (verificatie OK, en de meldplichtige bevindt zich buiten verboden gebied)
2. De meldplichtige voldoet niet aan zijn meldplicht omdat hij zich meldt, maar binnen verboden gebied.
In het tweede scenario tonen we gegevens aan de medewerkers van het monitoringscentrum. Op het moment dat de meldplichtige zich moet melden, biedt hij/zij een van de vooraf vastgelegde vingers aan de vingerafdruksensor. De vingerafdruksensor registreert de aangeboden vingerafdruk, waarna de Mini ID deze vergelijkt met de vooraf vastgelegde vingerafdrukken op het apparaat. Is er een match dan stuurt de Mini ID een "vinkje" (Verificatie OK) terug naar 5.1.2i, tezamen met de op dat moment vastgelegde locatie en dus het Mini ID nummer. Ten aanzien van de locatie, betreft dit een momentopname – van het *volgen* van de locatie is geen sprake.

Er is dus ten aanzien van de verificatie alleen bekend of deze akkoord is (of niet, als de meldplichtige verkeerde vingers aanbiedt of zich geheel niet meldt). Er wordt geen biometrische informatie verstuurd naar 5.1.2i. Het verzenden van de geolocatie op deze wijze is vanuit de werking van het device de meest dataminimalistische optie mogelijk. Dit omdat enkel lattitude-longitude gegevens verstuurd worden, zonder verdere context. Belangrijk om te vermelden is dat de locatiebeoordeling (bevindt de meldplichtige zich wel of niet binnen verboden gebied) geautomatiseerd plaatsvindt wanneer de data in het monitoringscentrum binnenkomt, zonder menselijke interactie. Wanneer zowel de verificatie als de locatie OK zijn (meldplichtige bevindt zich buiten het verboden gebied en de identificatie is succesvol verlopen), dan wordt de data van dat meldmoment automatisch gewist, zonder dat een medewerker deze heeft kunnen inzien. Dit proces gebeurt binnen een stuk IT-infrastructuur dat niet toegankelijk is voor medewerkers van het monitoringscentrum.
Slechts in die gevallen waarbij een meldplichtige zich meldt **én** hij/zij dit doet binnen verboden gebied wordt de data bewaard en wordt deze zichtbaar gemaakt aan de medewerkers in het

monitoringscentrum, zodat zij daarop passende actie kunnen ondernemen volgens de opvolgprotocollen die in die situatie van toepassing zijn. Niet melden: Wanneer een meldplichtige zich niet meldt wordt na verloop van tijd de melding als “gemist” geadministreerd. Er werd actie van de meldplichtige gevraagd, maar die heeft de actie niet ondernomen. Dit kan bijvoorbeeld zo zijn als de meldplichtige zich had moeten melden maar de Mini ID thuis heeft laten liggen terwijl de meldplichtige elders verblijft.

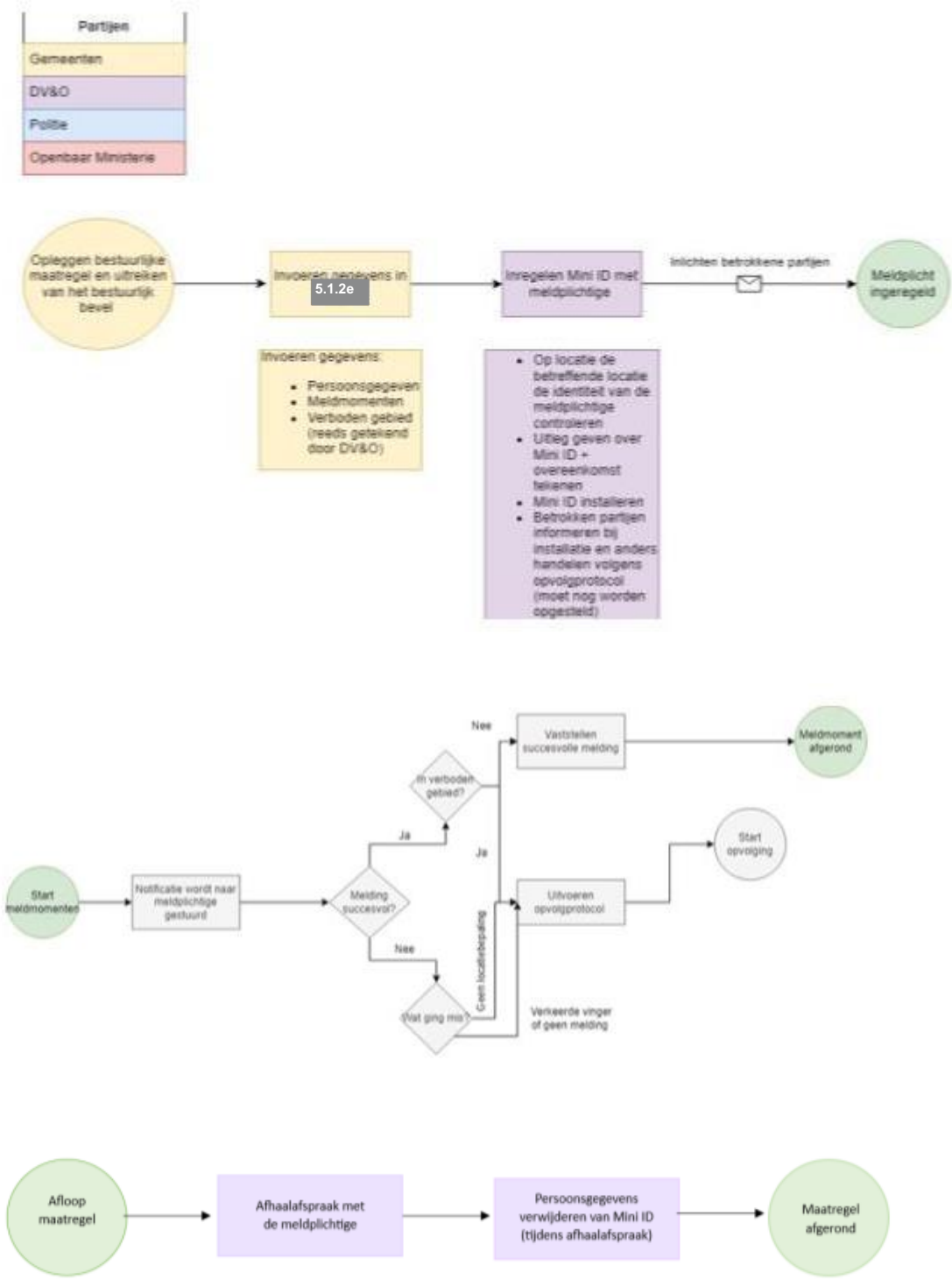
Omdat de meldplichtige zich niet meldt is er geen verificatie-informatie bekend en überhaupt geen locatie-informatie, omdat deze enkel verstuurd wordt op moment van melden.

De locatie-informatie wordt gedurende 10 minuten bewaard en daarna automatisch verwijderd. Het gedurende 10 minuten vasthouden van locatie-informatie is nodig om in geval van een mogelijke overtreding het systeem de tijd te geven de juiste locatie-informatie te selecteren. De locatie-informatie ouder dan 10 min wordt automatisch verwijderd. Er is een memo over de noodzaak om de locatie-informatie 10 min te bewaren. De memo is goedgekeurd door de privacy-officier van JenV, zie bijlage 5. Wanneer er sprake is van een mogelijke overtreding (in casu melden binnen verboden gebied) dan wordt de locatie-informatie behorend bij dat meldmoment opgezocht en veilig gesteld (gekopieerd naar een andere locatie binnen de infrastructuur), zodat deze data in het strafrechtelijk feitenonderzoek gebruikt kan worden. *(Aanvulling n.a.v. aanbeveling 2 en 9 advies FG’s 21 maart 2025)*

De persoons- en locatiegegevens van de betrokkene worden gedurende fase 1 in het systeem ‘5.1.2i’ verwerkt. 5.1.2i is het softwaresysteem dat DV&O gebruikt en waaraan de hardware (de Mini-ID) is gekoppeld. Voor fase 1 krijgen enkele (huidige inschatting: 3) medewerkers van de gemeente toegang, en dan louter tot de front-end (zie hierna).
In 5.1.2i moet onderscheid worden gemaakt tussen de zgn. front-end en back-end. De front-end van de software is de ‘gebruikerskant’ van de software. De front-end is het systeemdeel waar de medewerkers Elektronische Monitoring van DV&O mee werken. Zij kunnen wel de gegevens van de drager en van de Mini ID zien, maar niet de locatie-informatie. Slechts als blijkt dat bij een meldmoment de meldplichtige in overtreding is wordt de overtreding getoond, maar niet de locatie-informatie waarop de overtreding betrekking heeft. In de front-end zijn dus geen locatie bepalingen (RF, GPS of Wi-Fi) terug te vinden. In de front-end worden wel de gegevens van de meldplichtige ingevoerd en deze zijn daar ook in te zien. Deze gegevens zijn de gegevens die bij de registratie van de digitale meldplicht worden aangeleverd, zoals o.a. de naam en adres, en ook tot welke deelnemersgroep de meldplichtige behoort (in dit geval, kort gezegd: dat de betrokkene meldplichtig is op basis van een besluit van de burgemeester). Verder worden in de front-end alle gegenereerde meldingen weergegeven (in de software worden de meldingen *regels* genoemd). De regels staan in templates en de templates zijn aan een deelnemersgroep toegewezen. Aan een deelnemersgroep kunnen meerdere templates worden toegewezen. De regels zijn naar wens in te stellen op type melding en prioriteit. Afhankelijk van de prioriteit zal de melding, als deze gegenereerd wordt, worden getoond in het meldingenoverzicht bij het monitoringscentrum. Het monitoringscentrum (MC) van DV&O zal aan de hand van het opvolgprotocol (zie toelichting boven) de melding afhandelen.

De back-end is de ‘achterkant’ van de software. De back-end is voor de ‘reguliere’ gebruiker niet toegankelijk en alleen te benaderen als hier toegang tot verleend is. Op dit moment zijn de enige medewerkers waar de back-end benaderbaar voor is, werkzaam bij DV&O (Functioneel Beheer EM) en de leverancier die ook rechten heeft om in de back-end te kijken in geval van storingen etc. – deze medewerkers van de leverancier kunnen het systeem alleen benaderen met toestemming van DV&O.
In de back-end zijn de GPS coördinaten van de overtreding van een meldplichtige wel te zien. Wanneer een ingestelde Biometric Location Check regel wordt overtreden, een succesvolle vingerscan en een overtreding van het verboden gebied, zullen in de back-end 3 GPS coördinaten (meldmoment met 1 ervoor en 1 erna) worden opgeslagen. Mocht deze data nodig zijn kan Functioneel Beheer EM deze gegevens aan de toezichthouder aanleveren. Niet-succesvolle meldingen leiden aldus tot een signaal bij het MC van DV&O. Vervolgens treden – afhankelijk van de aard van het signaal – opvolgingsprotocollen (zie uitleg hierboven) in werking. Mocht het daarbij nodig zijn dan kan de politie direct geïnformeerd worden over een mogelijke overtreding.

Afbeelding: processchema's



1.3 Wat wil je bereiken? (wat is het doel)

Wat is het doel dat je wil bereiken met het project/proces? Dit kunnen uiteraard ook meerdere doelen zijn.

Het doel van deze fase van de Digitale Meldplicht is het realiseren van een goed functionerende en veilige digitale meldfaciliteit, voor het toezicht op en de handhaving van gebiedsverboden op grond van artikel 172a van de Gemeentewet. Het achterliggende, hogere doel voor de gemeente Leeuwarden is dat er door

het toepassen van de digitale meldplicht een effectief en proportioneel middel in kan worden gezet in casuïstiek die zich daarvoor leent – i.c. gaat het om personen die betrokken zijn bij ernstige ordeverstoringen rond het betaald voetbal, dan wel herhaaldelijk zijn betrokken bij dergelijke ordeverstoringen – om nieuwe ordeverstoringen door de persoon met een gebiedsverbod te voorkomen. Dit draagt bij aan de veiligheid en de openbare orde rond betaald voetbalwedstrijden van SC Cambuur.

Voor fase 1, waar deze DEPIA betrekking op heeft, is specifiek het doel: het gebruiken van de Mini-ID in 'echte situaties' (door de digitale meldplicht daadwerkelijk in voorkomende gevallen op te leggen aan daarvoor in aanmerking komende personen, en daarbij het gebruik van de Mini-ID voor te schrijven).
Op deze wijze kan het gebruik van de Mini-ID worden beproefd en proefondervindelijk verbeterd.

Op een nog te bepalen moment zal er een evaluatie worden uitgevoerd, waarin de verbeterpunten uit fase 1 worden geïnventariseerd.
Bij deze evaluatie is onder meer van belang hoe de doelgroep de maatregel ervaart. De meldplichtige krijgt de maatregel opgelegd vanuit het bevoegd gezag. De verwerking van de persoonsgegevens gebeurt om toe te kunnen zien op de juiste naleving van de opgelegde meldplicht. De pilot digitale meldplicht fase 1 wordt geëvalueerd door het Wetenschappelijk Onderzoeks- en Documentatiecentrum. Hierbij worden ook de meldplichtigen bevraagd naar hun ervaringen. De wijze waarop de ervaring van de meldplichtigen wordt nagegaan wordt nog afgestemd. De evaluatie vindt gedurende en na afloop van de pilot plaats. Mochten de bevindingen aanleiding geven om wijzigingen in het ketenproces door te voeren, zal dit door de stuurgroep worden opgepakt. Op dit moment zijn andere doelgroepen geen onderdeel van het huidige project. In volgende fases wordt bezien op welke andere doelgroepen een digitale meldplicht van toepassing kan zijn.
Aanvulling n.a.v. aanbeveling 4 advies FG's 21 maart 2025

1.3.1 Ga je de persoonsgegevens ook voor een ander doel gebruiken?
Als je persoonsgegevens ook nog voor een ander doel dan dit project/proces gaat gebruiken, is dat een 'verdere verwerking'. Dit mag als je uitdrukkelijke toestemming hebt van de betrokkenen, de verdere verwerking in een wet staat of als het doel verenigbaar is met het doel waarvoor je de gegevens gaat gebruiken. Voorbeelden zijn gegevens voor de bijstand gebruiken voor kwijtschelding van belastingen of het samenstellen van managementinformatie.

Niet van toepassing. De persoonsgegevens die in het kader van fase 1 worden verwerkt, worden louter voor bovengenoemde doelen verwerkt.

1.3.2 Kan je het doel ook op een andere manier bereiken?
Een belangrijk begrip bij het beoordelen van de noodzaak is 'subsidiariteit'. Dit betekent dat je afweegt of het verwerken van persoonsgegevens nodig is en nagaat of je het doel ook op een andere manier (dus zonder persoonsgegevens) kan bereiken. En dat je deze afweging kan uitleggen.

De hierboven beschreven doelen kunnen niet worden bereikt op een andere 'geschikte' wijze, d.w.z. op een wijze die even effectief is en tegelijkertijd minder ingrijpend voor de betrokkene.

Als mogelijk alternatief zou bv. kunnen worden gedacht aan melden door videobellen of het melden bij politie of handhaver in de buurt. Dit zijn echter modaliteiten die ingrijpender zijn voor de betrokkene, omdat ze meer impact hebben op de persoonlijke levenssfeer (videobellen) en bewegingsvrijheid (in persoon melden). Ten aanzien van videobellen speelt daarnaast ook mee dat het lastiger is (dan bij de Mini-ID) om met zekerheid vast te stellen dat de betrokkene niet in verboden gebied is.
De inzet van de digitale meldplicht (dus: inclusief een goed functionerende meldfaciliteit) is veel minder ingrijpend voor de betrokkene, dan de fysieke variant van de meldplicht a.b.i. artikel 172a van de Gemeentewet. Zie ook de toelichting bij 1.2. De fysieke variant van de meldplicht is wordt in onze gemeente niet ingezet, vanwege praktische en juridische bezwaren. Deze variant is immers afhankelijk van de locatie, openingstijden en bemanning van politiebureaus waar de betrokkene zich (tijdens en rond betaald voetbalwedstrijden) zou moeten melden. Ook drukt het op de capaciteit van de politie, vooral op

de momenten waar politie-inzet ergens anders nodig is. Naast deze praktische bezwaren wordt de meldplicht vaak gezien als een disproportionele belasting voor degene die zich moet melden.
Verder is de persoonsgegevensverwerking in fase 1, die in deze DEPIA wordt omschreven, noodzakelijk voor het beproeven van de Mini-ID als geschikte meldfaciliteit.

1.4 Wat is het juridisch en beleidskader?

De AVG kent zes grondslagen: 1) wettelijke verplichting, 2) algemeen belang/openbaar gezag, 3) overeenkomst, 4) toestemming, 5) gerechtvaardigd belang en 6) vitaal belang.
Wettelijke verplichting en algemeen belang/openbaar gezag komen het meest voor; deze staan altijd in een wet. Overeenkomst sluit je met een persoon af, bijv. een arbeidsovereenkomst. Toestemming kan alleen onder strikte voorwaarden, gerechtvaardigd belang alleen voor bedrijfsvoeringstaken van de gemeente. Vitaal belang gebruik je alleen in levensbedreigende situaties. Verwerk je (ook) gegevens op grond van de Wet politiegegevens (Wpg)? De twee meest voorkomende grondslagen zijn dan algemene opsporing (art. 8) of gericht onderzoek (art. 9). Specifiek(e) beleid of richtlijnen van de gemeente kunnen ook relevant zijn. Die noteer je bij 1.4.2.

1.4.1 Wat is de grondslag vanuit AVG of Wpg?

In dit geval draait het om het algemeen belang/openbaar gezag zoals bedoeld in artikel 6, eerste lid, aanhef en onder e, van de AVG:
"De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan: (…)
e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen."

Deze taak van algemeen belang/i.h.k.v. openbaar gezag betreft de taak van de burgemeester om de openbare orde te handhaven, en dan specifiek de bevoegdheid die de burgemeester (met het oog op die taak) heeft gekregen in artikel 172a lid 1 sub c van de Gemeentewet. Dit betreft een zgn. 'discretionaire bevoegdheid': een burgemeester kan op grond van dit artikel een meldplicht aan personen die de openbare orde ernstig (en/of herhaaldelijk) hebben verstoord bij ernstige vrees voor verdere verstoring van de openbare orde. Hij kan deze maatregel ook tegelijkertijd opleggen met een gebiedsverbod of een groepsverbod. In het geval aan een persoon of groep een gebiedsverbod wordt opgelegd, dan mag die persoon of groep zich een bepaalde tijd niet in dat betreffende gebied bevinden.
Van belang is hierbij, dat de burgemeester niet verplicht is deze bevoegdheid toe te passen (immers: discretionaire bevoegdheid). Dat maakt dat de AVG-grondslag van artikel 6 lid 1 sub c van de AVG (t.w.: noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust) hier niet van toepassing is.
Artikel 6 lid 1 sub g AVG is de enige grondslag voor de gegevensverwerking in fase 1 van de digitale meldplicht. Van een andere grondslag (zoals bv. toestemming, sub a) is géén sprake. Volledigheidshalve: toestemming als grondslag voor gegevensverwerking is in dit geval geen optie, per definitie is sprake van een ongelijke verhouding tussen burgemeester en meldplichtige – onder die omstandigheid kan vrijwel geen sprake zijn van de vereiste vrijelijk gegevens toestemming.
Aangevuld n.a.v. aanbeveling 1 advies FG's 21 maart 2025

De grondslag voor gegevensverwerking (zoals bedoeld in artikel 6 AVG) én de uitvoering van de digitale meldplicht (artikel 172a Gemw) is omschreven in een memo en het implementatieplan van het project (zie bijlagen bij deze DEPIA). Een uniforme werkwijze bij de uitvoering van de digitale meldplicht wordt hiermee gewaarborgd. Ook de opvolgprotocollen fungeren als leidraad voor uniforme toepassing, deze perotocollen zijn ook als bijlage bij deze DEPIA gevoegd. Voornoemd memo is akkoord bevonden door de privacy-adviseur van het ministerie van Justitie en Veiligheid. Ook de stuurgroep is akkoord gegaan met de memo, het implementatieplan en de opvolgprotocollen.
(Aanvulling n.a.v. aanbeveling 8 advies FG's 21 maart 2025)

Qua openbaar gezag kan verder nog opgemerkt worden dat de burgemeester op grond van de Gemeentewet (artikel 172 jo. 174) verantwoordelijk is voor de openbare orde en de bescherming van de gezondheid en veiligheid rond openbare samenkomsten, w.o. de betaald voetbalwedstrijden.

1.4.2 Welke andere wet- en regelgeving en eventueel beleid is relevant?

Naast bovenvermelde wettelijke bepalingen heeft de burgemeester van Leeuwarden beleidsregels opgesteld waarin hij zijn gebruik van de wettelijke bevoegdheid van artikel 172a van de Gemeentewet nader invult: Beleidsregels aanpak overlast (Wet Mbveo)

1.5 Wie zijn de stakeholders?

Maak een stakeholderanalyse over de rol, positie en verwachtingen/wensen. Enkele voorbeelden: De persoon over wie je gegevens gaat verwerken (klant, cliënt, inwoner, bezoeker, etc.) is de betrokkene. Een organisatie die namens de gemeente gegevens verwerkt of een leverancier van een applicatie is een verwerker. Een andere organisatie kan ook een verwerkingsverantwoordelijke zijn; voeg dan in de tabel ook toe of deze organisatie ontvanger of verstrekker is.

Stakeholder	Rol	Positie	Verwachtingen/wensen
Digitaal meldplichtige	Betrokkene	Onbekend	Minimale inbreuk op persoonlijke levenssfeer en een goed functionerende meldfaciliteit
Netwerk van de meldplichtige	Derden, niet direct-betrokken	Onbekend	Minimale inbreuk op rechten meldplichtige, goed functionerende meldfaciliteit, geen herhaling van ordeverstoring door meldplichtige
Bezoekers van betaald voetbalwedstrijden	Derden, niet direct betrokken	Voorstander	Veilig bezoek aan wedstrijden betaald voetbal, relschoppers die op persoonsniveau gevolg dragen van negatief gedrag, geen collectieve maatregelen
De burgemeester van de gemeente Leeuwarden	Verwerkings-verantwoordelijke	Voorstander	Een goed functionerende meldfaciliteit waarmee de naleving van het opgelegde gebiedsverbod kan worden gecontroleerd en bij overtredingen kan worden gehandhaafd, ten behoeve van de openbare orde en veiligheid rond betaald voetbalwedstrijden
Medewerker gemeente	Gebruiker	Voorstander	Een goed functionerende meldfaciliteit waarmee de naleving van het opgelegde gebiedsverbod kan worden gecontroleerd en bij overtredingen kan worden gehandhaafd, ten behoeve van de openbare orde en veiligheid rond betaald voetbalwedstrijden
DV&O	Verwerker	Voorstander	Een goed functionerende meldfaciliteit
Politie	Verwerker	Voorstander	Een goed functionerende meldfaciliteit waarmee de naleving van het opgelegde gebiedsverbod kan worden gecontroleerd en bij overtredingen kan worden gehandhaafd
Openbaar Ministerie/Officier van Justitie	Gezagsdrager strafrechtelijke opsporing, verwerkings-verantwoordelijke	Voorstander	Een goed functionerende meldfaciliteit waarmee de naleving van het opgelegde gebiedsverbod kan worden gecontroleerd en bij overtredingen kan worden gehandhaafd, in het geval van de officier van justitie in strafrechtelijke zin, ten behoeve van de veiligheid rond betaald voetbalwedstrijden
5.1.2i (software leverancier)	Subverwerker	Voorstander	De Mini-ID en de monitoringssoftware 5.1.2i voldoet en ondersteunt het proces in fase 1

1.6 Hoe ga je betrokkenen informeren?

We moeten transparant zijn over het verwerken van persoonsgegevens. Het is dus belangrijk dat de betrokkene weet dat wij gegevens over hem/haar verzamelen en gebruiken. Voorbeelden: informatie op de website, een folder, bijlage bij of informatie in een brief, een privacyverklaring, etc.

Vooropgesteld: de oplegging van een gebiedsverbod in combinatie met de digitale meldplicht gebeurt door middel van een appellabel besluit, zoals bedoeld in artikel 1:3 van de Algemene wet bestuursrecht (Awb). Dat besluit moet voor de inwerkingtreding op de wettelijk voorgeschreven wijze bekend worden gemaakt aan de betrokkene (artikel 3:40 e.v. Awb).

In dat besluit motiveert de burgemeester waarom hij de digitale meldplicht nodig vindt. Verder wordt in het besluit ook uitleg gegeven aan de betrokkene, wat hij moet doen om de digitale meldplicht na te leven. Verder zal bij het besluit een bijsluiter worden gestuurd als bijlage ("Informatieblad Mini ID"), waarin uitgebreide uitleg wordt gegeven over de werking van de Mini-ID.

Vervolgens zal de Mini-ID tijdens een installatie-afspraak door een medewerker van DV&O worden uitgereikt, waarbij ook uitleg over de werking van de Mini-ID wordt gegeven en de koppeling van de biometrische gegevens (vingerafdruk) van de betrokkene zal plaatsvinden.

Vanuit het rijk zal er waarschijnlijk wel algemene informatie worden verstrekt over de werking en gang van zaken in fase 1, dit wordt nog nader bepaald. Lokaal gaan we in fase 1 geen aanvullende algemene informatie verstrekken via onze website. De informatie aan betrokkene is in deze fase voldoende om aan de informatieplicht te voldoen.

2 Persoonsgegevens

2.1 Welke persoonsgegevens ga je verwerken?

Zet in de tabel over wie je persoonsgegevens gaat verwerken (betrokkenen) en welke persoonsgegevens dit zijn. Voorbeelden van betrokkenen zijn: inwoners, cliënten, aanvragers, kinderen, bezoekers en medewerkers. Voorbeelden van persoonsgegevens zijn: naam, adres, woonplaats, telefoonnummer, BSN, e-mailadres, geboortedatum en -plaats, leeftijd, geslacht, nationaliteit, IP-adres, kenteken, inkomen, bankrekeningnummer en -saldo, lidmaatschap vakbond, politieke opvattingen, seksuele voorkeur, gegevens over gezondheid, strafrechtelijke gegevens, een stem, etc.

Betrokkenen	**Persoonsgegevens**
Digitaal meldplichtige	Gewone (NAW) persoonsgegevens: voornaam, achternaam, adres, geboortedatum, geslacht, telefoonnummer, locatiegegevens/tracegegevens op basis van GPS-bepaling. Biometrische gegevens: vingerafdruk. Nb. Het BSN komt niet in 5.1.2i.
Medewerker gemeente	Naam, achternaam, functie en organisatie, telefoonnummer en mailadres.

2.1.1 Mag je bijzondere persoonsgegevens verwerken?

Je mag bijzondere persoonsgegevens alleen verwerken als de betrokkene uitdrukkelijk toestemming heeft gegeven of als er sprake is van een specifieke uitzondering. Bijzondere persoonsgegevens zijn: ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van vakbond, genetische gegevens, gezondheid, seksueel gedrag of gerichtheid, en biometrische gegevens met oog op unieke identificatie van een persoon.

Er is sprake van het vastleggen van bijzondere persoonsgegevens, zijnde biometrische gegevens (de vingerafdrukken van de meldplichtige). Het verbod om dergelijke gegevens te verwerken, is hier niet van toepassing. Daarbij is met name artikel 29 van de Uitvoeringswet AVG (UAVG) van belang, waarin is bepaald:

> *Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.*

Het gebruik van biometrie met de toepassing van de Mini ID is noodzakelijk voor de persoonsverificatie (authenticatie), en valt binnen de uitzondering die in de UAVG is opgenomen.

Deze valt ook binnen de (algemene) uitzondering die de AVG formuleert in artikel 9, tweede lid en onder g: ingeval er een zwaarwegend algemeen belang gediend wordt waar de verwerking van de bijzondere persoonskenmerken (in dit geval: biometrische) noodzakelijk voor wordt geacht.
In dit geval bestaat het zwaarwegend algemeen belang uit de goede uitvoering van de wettelijke bevoegdheid van de burgemeester – gezien artikel 172a van de Gemeentewet - om een gebiedsverbod in combinatie met een digitale meldplicht op te leggen in het belang van de openbare orde, de bescherming van de gezondheid en veiligheid van bezoekers van betaald voetbalwedstrijden.

Nu de verwerking van biometrische gegevens valt binnen de in de AVG en UAVG vastgelegde uitzonderingen, is deze verwerking rechtmatig.

2.1.2 Mag je strafrechtelijke persoonsgegevens verwerken?

Je mag strafrechtelijke persoonsgegevens alleen onder voorwaarden verwerken. Voorbeelden van strafrechtelijke gegevens zijn: strafrechtelijke veroordelingen ('strafblad'), strafbare feiten, verdenkingen en veiligheidsmaatregelen.

In fase 1 wordt in 5.1.2i vastgelegd dat een betrokkene een gebiedsverbod inclusief digitale meldplicht opgelegd heeft gekregen. Dit valt onder 'persoonsgegevens van strafrechtelijke aard' zoals bedoeld in artikel 1 van de Uitvoeringswet AVG (UAVG) jo. artikel 10 van de AVG, en dan specifiek onder 'veiligheidsmaatregelen verband houdende met strafrechtelijke veroordelingen en strafbare feiten'. Daarmee valt deze verwerking onder de uitzondering van artikel 33, eerste lid en onder b, van de UAVG:

> ***Artikel 33 Overige uitzonderingsgronden inzake gegevens van strafrechtelijke aard***
>
> ***1.*** *Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt, indien:*
>
> *(…)*
>
> *b.de verwerking geschiedt door en ten behoeve van publiekrechtelijke samenwerkingsverbanden van verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken, indien:*
>
> *1°.de verwerking noodzakelijk is voor de uitvoering van de taak van deze verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken; en*
>
> *2°.bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad;*

Opmerking daarbij is dat juist deze informatie noodzakelijk is om in fase 1 de digitale meldplicht middels Mini-ID te kunnen uitvoeren, met inachtneming van de wettelijke taak van algemeen belang (de grondslag die hierboven is omschreven), terwijl slechts die gegevens worden verwerkt die strikt noodzakelijk zijn voor de uitvoering van de digitale meldplicht middels de Mini-ID, zijnde de essentiële informatie (duur verbod, verboden gebied).

2.1.3 Mag je het BSN verwerken?

Je mag het BSN alleen verwerken als dit in een wet staat. Maar je moet ook beoordelen of het nodig is.

Niet van toepassing.

2.1.4 Kan je het doel ook met minder persoonsgegevens bereiken?

Een belangrijk begrip bij het beoordelen van de noodzaak is 'proportionaliteit'. Dit betekent dat je afweegt of het nodig is alle persoonsgegevens te verwerken die je eerder in de tabel hebt opgesomd. En dat je deze afweging kan uitleggen.

Bovenvermelde gegevens zijn nodig voor een goede uitvoering van de digitale meldplicht middels het gebruik van de Mini-ID in fase 1. Enerzijds zijn die gegevens nodig voor de noodzakelijk vaststelling van de identiteit/persoonsverificatie, anderzijds zijn deze gegevens – telefoonnummers, mailadressen van medewerkers – noodzakelijk om het proces goed uit te voeren. In de opvolgprotocollen (deels nog in uitwerking) komt naar voren wanneer deze gegevens in het proces worden gebruikt.

2.2 Waar komen de persoonsgegevens vandaan?

Denk aan de betrokkene zelf, een andere organisatie, de gemeente (bijv. burgerzaken/5.1.2i, een andere afdeling/team)

Persoonsgegevens zijn primair afkomstig van de politie, van de gemeente (5.1.2i-gegevens bv.) en mogelijk ook van de betrokkene zelf. Gegevens die afkomstig zijn van de politie worden door middel van een bestuurlijke rapportage aan de burgemeester verstrekt. Daar is ook een expliciete wettelijke grondslag voor, te weten het bepaalde in artikel 16, eerste lid en onder b, van de Wet politiegegevens (WPG):

Artikel 16. (verstrekking aan gezagsdragers)

1. *De verwerkingsverantwoordelijke verstrekt politiegegevens aan:*
   b. de burgemeesters voor zover zij deze behoeven:
   1°. in verband met hun gezag en zeggenschap over de politie, of
   2°. in het kader van de handhaving van de openbare orde.

2.3 Hoe zorg je dat de persoonsgegevens juist zijn en actueel blijven?

Het is belangrijk dat we alleen persoonsgegevens verwerken die juist zijn. En dat we deze actualiseren als dat nodig is.

Ingeval er iets wijzigt aan de zijde van de betrokkene/digitaal meldplichtige (adres, telefoonnummer) dan wel de referent digitaal meldplichtige, dan ligt het primair op de weg van de betrokkene om deze wijziging door te geven aan de gemeente. De betrokkene zal op die verantwoordelijkheid gewezen worden in het appellabele besluit waarbij de digitale meldplicht wordt opgelegd.

Als de betrokkene geen melding van een wijziging doorgeeft, en er bij de gemeente/politie toch een signaal binnenkomt dat er iets is gewijzigd (bijvoorbeeld als de aan hem verzonden besluiten als onbestelbaar retour komen) dan kan dat aanleiding zijn om bv. het adresregister van de 5.1.2i (Basisregistratie persoonsgegevens) te raadplegen om zodoende de adresgegevens 'ambtshalve' te actualiseren. Ten aanzien van telefoonnummers en mailadressen bestaat die mogelijkheid tot verificatie echter niet.

Van belang is nog dat adresverificatie d.m.v. de 5.1.2i in de 'reguliere processen' gebeurt, net zoals bij andere besluiten van de burgemeester. Hij is, als bestuursorgaan, op grond van de Awb verantwoordelijk voor een juiste bekendmaking van het besluit - anders treedt dat niet in werking - en dat gebeurt in deze gevallen door aangetekende verzending aan iemands 5.1.2i-adres.

2.4 Ga je gebruikmaken van geautomatiseerde besluitvorming, profilering of big data?

Geautomatiseerde besluitvorming, profilering en big data kunnen grote gevolgen hebben. Geautomatiseerde besluiten zijn besluiten zonder tussenkomst van een medewerker. Bijv. opleggen snelheidsboete met informatie uit een flitscamera zonder dat een persoon meekijkt in het proces of het opleggen van de boete juist is. Profileren is het opbouwen van profielen waarmee je personen in categorieën kunt indelen. Bijv. beoordelen op basis van gedrag, betrouwbaarheid, prestaties, gezondheid, economische situatie, locatie, persoonlijke voorkeuren of interesses. Big data is een grote hoeveelheid gegevens uit verschillende bronnen analyseren waarbij je geautomatiseerd zoekt naar onderlinge verbanden waarmee je beslissingen kunt nemen op groeps- of individueel niveau. Een voorbeeld is fraudebestrijding. Beschrijf ook wat de gevolgen zijn voor betrokkenen.

Niet van toepassing.
De besluiten tot oplegging van een gebiedsverbod in combinatie met een digitale meldplicht, worden in elke casus door tussenkomst van- en op advies van een medewerker opgelegd. Dit betreft juridisch geschoolde en beëdigde medewerkers van de sector Juridische en Veiligheidszaken, in bezit van een VOG-P, die specifiek zijn belast met de advisering/besluitvorming omtrent bestuurlijke maatregelen in het openbare orderecht. Vervolgens worden deze besluiten geregistreerd in 5.1.2i teneinde de digitale meldplicht door middel van de Mini-ID te kunnen laten verlopen. In het vervolg wordt 'plat' geregistreerd of de meldplichtige zijn/haar meldplicht naleeft. Zo ja: dan gebeurt er verder niets en loopt het proces

door. Overtreedt hij/zij zijn/haar meldplicht daarentegen, dan leidt dat tot een vervolgstap volgens de opvolgprotocollen, zoals bv. het intrekken of verlengen van de digitale meldplicht.

2.5 Ga je gebruikmaken van nieuwe technologieën?

Bij een nieuwe technologie zijn de persoonlijke en maatschappelijke gevolgen niet altijd duidelijk. Nieuwe manieren om gegevens te verzamelen en gebruiken, kunnen grote privacyrisico's hebben. Voorbeelden: robotisering (RPA), kunstmatige intelligentie (AI), algoritmes, slimme apparaten, biometrie (gezichtsafbeelding, vingerafdruk).

De Mini-ID gebruikt een combinatie van GPS en biometrie (vingerafdruk voor persoonsverificatie). Zie toelichting onder 1.2 en 2.1.1.

2.6 Wie heeft toegang tot de persoonsgegevens?

Denk aan medewerkers van de gemeente. Maar ook aan bijvoorbeeld een leverancier van een applicatie of medewerkers van een andere organisatie. Het gaat om (rechtstreekse) toegang tot de persoonsgegevens, niet om personen of organisaties die de persoonsgegevens ontvangen. Deze heb je namelijk al beschreven in de tabel met stakeholders.

De in monitoringssoftware 5.1.2i geregistreerde gegevens zijn toegankelijk voor drie geautoriseerde medewerkers van de gemeente, sector Juridische en Veiligheidszaken, die specifiek zijn belast met de behandeling van deze zaken en de advisering van de burgemeester daarover. Zij beschikken over een VOG-P. Deze medewerkers kunnen in 5.1.2i alleen de Leeuwarder zaken inzien, dus die zaken waarin de burgemeester van de gemeente Leeuwarden een digitale meldplicht heeft bevolen.
Daarnaast zijn deze gegevens in 5.1.2i toegankelijk voor geautoriseerde medewerkers (supply, support, functioneel beheer en monitoring) van (het Monitoringscentrum van) DV&O.
Verder kunnen in bijzondere omstandigheden – zoals uitval of calamiteiten – ook medewerkers applicatie en database van softwareleverancier 5.1.2i toegang krijgen tot 5.1.2i. Dat is dan alleen mogelijk als DV&O toegang verschaft, DV&O houdt supervisie tijdens dat proces (vierogen-principe), de sessie wordt opgenomen en gelogd.

2.7 Hoe en waar ga je de persoonsgegevens opslaan?

Denk bij 'hoe' aan een applicatie of bestand. Maak bij 'waar' een onderscheid tussen binnen en buiten de gemeente. Voorbeelden: op een server, op een afdelingsschijf, in een kantoorapplicatie zoals Outlook. Noem ook altijd het land waar de gegevens staan en de andere partij (organisatie, leverancier) als dit niet de gemeente is. Opslag buiten de EER? Vermeld dan ook wat het beschermingsniveau is (de AVG geldt namelijk niet buiten de EER).

De data in de monitoringssoftware 5.1.2i staat opgeslagen in het overheidsdatacentrum van JIO in Nederland. Er wordt tevens gebruik gemaakt van interne private clouddiensten.
De gegevensverwerkingen in het systeem 5.1.2i in het kader van fase 1 Digitale Meldplicht kan in bijzondere situaties (als er programma-issues zijn) buiten Nederland en buiten de EU (VK) plaatsvinden. Alle soft- en hardware is in Nederland aanwezig. 5.1.2i bevindt zich op het justitienet. Maar de leverancier 5.1.2i, met wie DV&O een contract heeft gesloten, is gevestigd in het VK. Als zich bijzondere situaties voordoen (denk bv. aan technische storingen of uitval van het systeem) dan kan het noodzakelijk zijn dat een medewerker van 5.1.2i inlogt op het systeem en zodoende toegang krijgt tot de daarin aanwezige persoonsgegevens. De hierboven genoemde procedure geldt dan. Het niveau van de gegevens-bescherming is evenwel in het VK gelijkwaardig aan dat in de EU (Brexit | Autoriteit Persoonsgegevens, geraadpleegd op 2 augustus 2024).

2.8 Zijn er koppelingen met andere systemen?

Het kan voorkomen dat er een koppeling is met een ander systeem. De gegevens komen dan (geautomatiseerd) uit dit andere systeem. Of de applicatie voor die jullie gaan gebruiken, heeft een koppeling met een ander systeem. De gegevens gaan dan (geautomatiseerd) naar dat andere systeem.

Er wordt per deelnemende gemeenten met een datapunt ingericht in 5.1.2i. In dit datapunt staan de gegevens van de BVO centraal benoemd. Hierbij moet worden gedacht aan het verboden gebied en de thuiswedstrijden van de club. De data met betrekking tot de wedstrijden wordt geautomatiseerd

ontvangen van Voetbalmedia, de partij die voor en namens de KNVB de data met betrekking tot wedstrijden distribueert. Wanneer er een wijziging in het speelschema plaatsvindt en Voetbalmedia die wijziging aanbrengt, wordt dit automatisch conform de wijzing verwerkt in het datapunt. Om dat mogelijk te maken komt er een koppeling tussen 5.1.2i en Voetbalmedia (een zg. API) die het mogelijk maakt deze wijzigingen zonder menselijke afhankelijkheid correct in 5.1.2i te krijgen.

2.9 Wat is de bewaartermijn en hoe ga je de persoonsgegevens vernietigen?

We moeten gegevens bewaren (archiveren) maar vaak ook na een bepaalde tijd vernietigen. Bewaartermijnen staan in de gemeentelijke selectielijst. Let op: voor politiegegevens (Wpg) gelden specifieke bewaartermijnen. Noem altijd een concrete bewaartermijn en het nummer(s) in de VNG-selectielijst. Beschrijf ook hoe je de gegevens na de bewaartermijn gaat of laat vernietigen, wie dit doet (gemeente zelf, leverancier applicatie, andere organisatie) en wie dit controleert. Ga je je huidige systeem vervangen door een nieuw systeem? Beschrijf dan ook hoe en wanneer je het exportbestand gaat verwijderen en hoe je de gegevens in het oude systeem gaat/laat vernietigen. Vraag altijd advies aan 5.1.2e

De bewaartermijn voor het opleggen van de digitale meldplicht is 5 jaren na vervallen van het besluit. Deze bewaartermijn betreft het 'opleggende' besluit van de burgemeester, dat in ons zaaksysteem wordt bewaard/gearchiveerd.

De gegevens van de betrokkenen worden ook verwerkt in 5.1.2i. In 5.1.2i geldt t.a.v. de gegevens over de digitaal meldplichtige een bewaartermijn van 1 maand na het afsluiten van het traject Digitale Meldplicht. Op dat moment worden de gegevens gearchiveerd. Het verwijderen ervan gebeurt 3 maanden na afsluiten van het totale Digitale meldplichttraject van de betreffende betrokkene.
Het verwijderen werkt als volgt. Bij het verwijderen van een zaak/betrokkene is de eerste stap het archiveren, dat kan alleen als alle bezoekafspraken in 5.1.2i zijn afgerond/geannuleerd en als er geen apparatuur meer op de betrokkene is toegewezen. Als vervolgens wordt gekozen voor archiveren komt er een 'drop down-menu' waar moet worden aangegeven wat de reden is voor het archiveren en een tekstveld waar minimaal 5 karakters in gevuld moet worden (verplicht veld). Als een zaak/betrokkene gearchiveerd is, dient men naar het archief in 5.1.2i te gaan, de betrokkene op te zoeken en een verwijderdatum in te vullen die minimaal 1 dag in de toekomst moet liggen. Als de datum is ingevoerd moet men de volgende dag wederom naar het archief gaan en de betrokkene opzoeken, op het einde van de regel staat een prullenbakje waarmee de betrokkene kan worden verwijderd. Na het selecteren van het prullenbakje klikt krijgt men eerst nog een pop-up venster met een code die in een tekstvlak dient te worden ingevuld. Pas als deze stappen zijn doorlopen, en op 'bevestigen' wordt geklikt, worden de gegevens van de betrokkene verwijderd en zijn deze niet meer terug te halen. Deze opeenvolging van handelingen maakt de kans op het abusievelijk verwijderen heel klein.

Na einde digitale meldplicht d.m.v. de Mini-ID worden alle op de betrokkene betrekking hebbende gegevens i.b. per ommegaande gewist uit 5.1.2i en uit de Mini-ID. Als de digitale meldplicht afloopt, wordt – na registratie stopzetten meldplicht in 5.1.2i door betrokken medewerker van de gemeente – door de gemeente in samenspraak met DV&O een afspraak met de betrokkene gemaakt voor het inleveren van de Mini-ID. Het innemen van de Mini ID gebeurt door een medewerker van DV&O, die de Mini-ID wist/'schoont' van alle gegevens. De Mini ID gaat vervolgens terug naar DV&O zodat deze in een andere zaak kan worden ingezet. De gegevens in 5.1.2i worden vervolgens gewist, na ontvangst van de Mini ID.

3 Baten en data-ethiek

3.1 Wat zijn de baten?

Bij baten kun je denken aan vrijheid, welvaart, duurzaamheid, inclusiviteit en diversiteit, gelijkheid, efficiëntie en kosten-reductie. Deze brede benadering is belangrijk omdat ethische en juridische aspecten invloed kunnen hebben op de relatie tussen onze organisatie en de omgeving.

3.1.1 Wat zijn de baten voor onze organisatie?

Het doel van het project digitale meldplicht is het creëren van een goed functionerende, veilige, digitale meldfaciliteit om uitvoering te geven aan de meldplicht, dit in de context van het tegengaan van (dreiging op) grootschalige ordeverstoringen rond het betaald voetbal.

Daar zijn een aantal 'baten' aan te koppelen:

- Door een goed functionerende digitale meldfaciliteit, kan beter/effectiever gebruik worden gemaakt van deze wettelijke mogelijkheid.
- Efficiëntie en kostenreductie spelen daarnaast ook een rol, zowel aan de zijde van de politie als aan de zijde van de gemeente. Voor de toepassing van de digitale meldplicht is logischerwijs veel minder menskracht vereist van bij de digitale variant.

3.1.2 Wat zijn de baten voor het individu?

Het doel van het project digitale meldplicht is het creëren van een goed functionerende, veilige, digitale meldfaciliteit om uitvoering te geven aan de meldplicht, dit in de context van het tegengaan van (dreiging op) grootschalige ordeverstoringen rond het betaald voetbal.

Aan de zijde van de betrokkene die een digitale meldplicht krijgt opgelegd, speelt het aspect *vrijheid* een grote rol: vergeleken met een fysieke meldplicht – wat eveneens een wettelijke mogelijkheid is – wordt zijn/haar vrijheid immers in veel mindere mate belemmerd door de digitale meldplicht.
In het verlengde daarvan: ook *efficiëntie* speelt bij de betrokkene een rol. Immers, in plaats van melden op het politiebureau kan hij/zij zich nu op elke locatie (behalve de verboden) melden.

3.1.3 Wat zijn de baten voor de mienskip van Leeuwarden?

Hier kan verwezen worden naar het antwoord hierboven bij 3.1.1. Baten voor de Mienskip van Leeuwarden zijn:

- Veiligheid: succesvolle toepassing van een digitale meldplicht draagt bij aan effectiviteit van een opgelegd gebiedsverbod, dat draagt bij aan de veiligheid rond betaald voetbalwedstrijden. Veiligheid als zodanig is een onlosmakelijk onderdeel van de zgn. brede welvaart. Dat is een kernbegrip in de huidige coalitieperiode en de gemeente staat daarvoor aan de lat. Directe verantwoordelijkheid voor de veiligheid rond betaald voetbalwedstrijden ligt bij de burgemeester.
- Gelijkheid en rechtvaardigheid: door een effectieve toepassing van dergelijke persoonsgerichte maatregelen, worden diegenen die zich hebben misdragen rond betaald voetbalwedstrijden geraakt met een proportionele reactie. Daar gaat ook een signaalwerking/generaal-preventieve werking vanuit. Personen die zich niet misdragen, worden ook niet geconfronteerd met dergelijke maatregelen.

3.2 Wat zijn de data-ethische aspecten?

Het verwerken van persoonsgegevens en de hierbij toe te passen techniek heeft invloed (of kan dit hebben) op menselijke waarden en belangen. Hieronder staan de data-ethische waarden, die voor gemeente Leeuwarden gelden. Het is belangrijk om af te wegen welke waarden meespelen voor de stakeholders en dan vooral onze inwoners. Houd bij het beschrijven van de waarden rekening met de rechten, plichten, belangen en wensen van de stakeholders. Wordt een waarde negatief geraakt? Neem deze dan op in het hoofdstuk over de risico's.

3.2.1 Rechtvaardigheid

We dragen bij aan rechtvaardigheid, gelijke kansen en inclusiviteit. Onze digitale oplossingen zijn laagdrempelig en waardevol voor iedereen. We zijn alert op het voorkomen van ongewenste vooringenomenheid bij de selectie van data. Ook letten we erop dat er geen discriminatie, stereotypering of vooroordelen in algoritmes zit (bias).

Een gebiedsverbod in combinatie met de digitale meldplicht kan alleen worden opgelegd aan personen die betrokken zijn bij ernstige openbare ordeverstoringen, dan wel herhaaldelijk zijn betrokken bij ordeverstoringen. Bij de beoordeling van dergelijke incidenten (op basis van politie-informatie veelal) wordt een afweging gemaakt; treft diegenen een verwijt van de betreffende incidenten? Als dat het geval is, pas dan komt deze maatregel in beeld. Dit zijn geen geautomatiseerde beoordelingen, dit is mensenwerk van medewerkers die daartoe opgeleid en beëdigd zijn.

Alleen personen die een verwijt gemaakt kan worden van betrokkenheid bij – kort gezegd – voetbalrellen krijgt deze maatregel inclusief digitale meldplicht opgelegd. Personen die zich misdragen, worden zo geconfronteerd met de gevolgen van dat gedrag. Anderen krijgen niet met zulke maatregelen te maken.

Een andere invalshoek op rechtvaardigheid is de volgende: de wetgever heeft daar in feite al een keuze in gemaakt. Immers, de wettelijke grondslag voor deze besluiten (artikel 172a Gemw) biedt de ruimte voor het opleggen van een meldplicht (fysiek of digitaal). Bij de totstandkoming van deze wetgeving is er door de formele wetgever (regering en Staten-Generaal – 1e en 2e kamer) een afweging gemaakt over de wenselijkheid van dit middel. Expliciet heeft de wetgever daarbij de mogelijkheid open gelaten voor deze digitale variant van de meldplicht. Deze is, afgezet tegen de fysieke variant, minder ingrijpend voor de betrokkene terwijl het tegelijkertijd zeer effectief is in de handhaving van het gebiedsverbod.

V.w.b. laagdrempeligheid: in het besluit waarbij de digitale meldplicht wordt opgelegd, en het daarbij gevoegde informatieblad Mini ID, wordt de betrokkene geïnformeerd over de wijze waarop de Mini-ID werkt, en wat dat voor hem/haar betekent. Daarnaast ontvangt diegene ook een bijsluiter, waarin de werking van de Mini-ID wordt uitgelegd. De installatie van de Mini-ID gebeurt in persoon, met ruimte voor uitleg en vragen van de betrokkene.

3.2.2 Menselijke waardigheid

We behandelen inwoners, ondernemers en bezoekers als mensen, niet als 'nummer'. Onze digitaliseringstrajecten sluiten aan bij de leefwereld en behoeften van de mensen in onze gemeente. De mens is altijd leidend, niet de techniek/data.

Bij de toepassing van de Digitale Meldplicht in deze fase, wordt gezocht naar een goede balans tussen effectiviteit, proportionaliteit, uitvoerbaarheid, eigen verantwoordelijkheid van de betrokkene en ondersteuning door techniek. De inzet van de Mini-ID als meldfaciliteit brengt deze aspecten in balans en zal doorgaans, als het minst ingrijpende middel, vanuit een evenredigheidsperspectief (een juridische afweging dus) als meest passende middel worden aangemerkt. De techniek is uitdrukkelijk een hulpmiddel en niet leidend bij de uitvoering.

Het feitelijk opleggen van een gebiedsverbod inclusief digitale meldplicht in concrete zaken, gebeurt door middel van een appellabel besluit. Bij de besluitvorming moet de burgemeester geschreven en ongeschreven beginselen van behoorlijk bestuur in acht nemen, waaronder de evenredigheid en het gelijkheidsbeginsel. Deze zien ook op een juiste afweging van het algemeen belang in relatie tot het persoonlijk belang van de betrokkene.
De wijze waarop de burgemeester deze belangen afweegt, is toetsbaar voor de bestuursrechter. Dit maakt dat de afweging van belangen van diegenen die met de inzet van de Mini-ID te maken krijgen, in het totale proces is geborgd.

3.2.3 Privacy

We beschermen de privacy van inwoners, ondernemers en bezoekers. Data van inwoners worden geanonimiseerd gebruikt en zijn niet herleidbaar tot een persoon. We gebruiken 'Privacy by design' en doen onderzoek naar de impact van digitaliseringstrajecten op de privacy.

De privacy van diegenen die een digitale meldplicht opgelegd krijgen, wordt geraakt. Van hen worden persoonsgegevens verwerkt (zie boven). Los van het gegeven dat daarvoor ook een wettelijke grondslag bestaat (Gemeentewet, AVG en de WPG – zie ook boven), kan daar nog over worden opgemerkt dat deze omstandigheid moet worden afgewogen tegen het algemeen belang (veiligheid rond betaald voetbal) en eigen betrokkenheid/verwijtbaarheid bij voetbalrellen van deze personen.
In fase 1 van de Digitale Meldplicht worden alleen die persoonsgegevens verwerkt die nodig zijn voor een goede uitvoering.
Waar het gaat over de impact van het gebruik van de Mini-ID: deze onderzoeken we in fase 1, door middel van bovengenoemde evaluatie. Daarin zal naar voren komen in hoeverre onze verwachtingen over de impact overeenkomt met de ervaring van de betrokkenen die er in fase 1 daadwerkelijk mee te maken hebben gekregen.

3.2.4 Veiligheid

We waarborgen de openbare orde en veiligheid, zodat iedereen zich veilig voelt in onze gemeente. We beveiligen onze data. Via cybersecurity bereiden we ons voor op digitale aanvallen.

De toepassing van de Mini-ID als digitale meldfaciliteit bij gebiedsverboden, draagt bij aan de openbare orde en veiligheid rond betaald voetbalwedstrijden in onze gemeente. Immers, met de toepassing van de digitale meldplicht door de Mini-ID, wint een opgelegd gebiedsverbod – dat de burgemeester noodzakelijk vindt ter bescherming van de openbare orde en veiligheid – aan effectiviteit. Dit belang weegt zwaar; gelet op de grote publieke belangstelling en grootschalige ongeregeldheden in het (recente) verleden zijn deze betaald voetbalwedstrijden gebeurtenissen met risico. De persoonsgegevens die in fase 1 worden verwerkt, worden beveiligd (zie 4 Beveiligingsmaatregelen). De betrokkene wordt door middel van het informatieblad dat bij de oplegging van de digitale meldplicht wordt verstrekt, laagdrempelig geïnformeerd over de werking van de Mini ID en het gebruik van de vingerafdruk. Als een betrokkene vervolgens wil weten hoe zijn (biometrische) gegevens worden beveiligd, dan informeren we hem/haar daarover (cf. de informatie in het hoofdstuk informatiebeveiliging in deze depia).

3.2.5 Autonomie

We respecteren menselijke autonomie (vrijheid). We vermijden onbewuste beïnvloeding, manipulatie en stimulering van dwangmatig gedrag of overheidstoezicht ('Big Brother'). We zijn terughoudend met het gebruik van data waarmee we gebruikers kunnen volgen, hun reputatie schaden of hun toekomst negatief kunnen beïnvloeden.

Dergelijke gebiedsverboden in combinatie met de digitale meldplicht kunnen alleen worden opgelegd aan personen die bij betrokken zijn bij ernstige openbare ordeverstoringen, dan wel herhaaldelijk zijn betrokken bij ordeverstoringen. Hen treft een verwijt t.a.v. deze betrokkenheid bij – kort gezegd – voetbalrellen; anders is de oplegging van een gebiedsverbod überhaupt problematisch.
De wettelijke grondslag voor deze besluit (artikel 172a Gemw) biedt de ruimte voor het opleggen van een meldplicht. Bij de totstandkoming van deze formele wet is er door de formele wetgever (regering en Staten-Generaal – 1e en 2e kamer) een afweging gemaakt over de wenselijkheid van dit middel.
Het opleggen van een gebiedsverbod (al dan niet met digitale meldplicht) is een toegestane inbreuk op de persoonlijke levenssfeer van de betrokkene – daar is een formeelwettelijke grondslag voor. Daarbij beperken we de inbreuk tot het hoogst noodzakelijke. De gegevensverwerking in 5.1.2i beperkt zich tot de vraag of iemand zich in verboden gebied bevindt of niet. De exacte locatie is voor ons niet relevant, wordt daarom ook niet in de front-end van 5.1.2i getoond en is voor medewerkers van de gemeente niet vast te stellen.
Verder is hier nog relevant dat de digitale meldplicht, afgezet tegen de fysieke variant, minder ingrijpend is voor de betrokkene. De inbreuk op iemands bewegingsvrijheid is daarmee veel beperkter.

3.2.6 Controle over technologie

We controleren op natuurlijke momenten of onze digitaliseringstrajecten nog goed werken. Door open en transparant om te gaan met data en informatie, kan iedereen deelnemen op basis van dezelfde kennis en inzichten.

Fase 1 van de digitale meldplicht gaat worden geëvalueerd, waarbij de vraag voorop staat of dit een veilig middel is dat daadwerkelijk bijdraagt aan de hierboven omschreven doelen. Deze evaluatie wordt voorbereid in samenwerking met het WODC (Wetenschappelijk Onderzoek en Datacentrum), een onafhankelijk kennisinstituut dat valt onder het Ministerie van JenV. De exacte invulling van deze evaluatie is op dit moment nog niet gedaan. In hoofdlijnen kan wel alvast worden aangegeven dat daarbij een aantal onderwerpen aandacht krijgen: gebruikerservaring van de meldplichtige, duidelijkheid van de werking, evt. storingen in software of bij het gebruik van de Mini-ID (zoals bij het lezen van de vingerafdruk), de mate van naleving van de digitale meldplicht, de uitvoering van opvolgprotocollen bij mogelijke overtredingen, e.a.

3.2.7 Kwaliteit van leven/duurzaamheid

We vinden gezond en duurzaam leven belangrijk in Leeuwarden. We zoeken naar duurzame oplossingen waarbij de gezondheid van inwoners, ondernemers en bezoekers voorop staat. We toetsen of digitale oplossingen echt meerwaarde hebben voor de gemeente.

Dit middel wordt ingezet als dat noodzakelijk is vanwege de bescherming van gezondheid en veiligheid van bezoekers van betaald voetbalwedstrijden. De burgemeester is daar, gelet op het bepaalde in artikel 174 Gw, voor verantwoordelijk. Tegen die achtergrond toetsen we in de evaluatie van fase 1 de meerwaarde van deze digitale meldfaciliteit, deze bevindingen kunnen we meenemen naar de daaropvolgende fase.

3.2.8 Mienskip

We vinden de bescherming van de gemeenschap belangrijk. We zorgen ervoor dat onze digitale toepassingen aansluiten op het gevoel van mienskip. We streven ernaar dat groepen inwoners en ondernemers vertrouwen hebben in de gemeente en onze digitaliseringstrajecten.

Hier kan nogmaals worden gewezen op het zwaarwegende algemeen belang bij het veilig verloop van betaald voetbalwedstrijden in onze gemeente, als massale publieksevenementen met een groot risico. Eenieder heeft immers recht op een veilig verloop van deze gebeurtenissen. Ook van belang (nogmaals): alleen personen die verwijtbaar betrokken zijn bij voetbalrellen, krijgen hier mee te maken als effectief gevolg van hun gedrag. En anderen niet. Succesvolle toepassing van dergelijke maatregelen draagt bij aan vertrouwen in digitale oplossingen van de overheid.

4 Beveiligingsmaatregelen

De gemeente moet passende technische en organisatorische maatregelen nemen om persoonsgegevens te beschermen. Het belangrijkste normenkader waaraan de gemeente moet voldoen, is de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast kan het zijn dat er domein specifieke wetgeving is met nadere maatregelen die de gemeente moet nemen. Geeft de gemeente opdracht aan een andere organisatie om persoonsgegevens te verwerken? Of is er sprake van een leverancier van een applicatie? Dan is de andere organisatie of leverancier van de applicatie een verwerker. Een verwerker moet ook passende maatregelen nemen om persoonsgegevens te beschermen.

4.1 Hoe ziet het toegangsbeheer eruit?

Alleen medewerkers met een taak in het proces, mogen toegang krijgen tot de persoonsgegevens. En zij moeten vervolgens de juiste rechten hebben. Voorbeelden: iedere gebruiker heeft een eigen gebruikersnaam en wachtwoord, inloggen via Single Sign On (eenmalig inloggen, toegang tot meerdere systemen), inloggen via tweefactor authenticatie, periodiek wijzigen wachtwoord, beheerders hebben andere rechten dan gebruikers, autorisatiematrix met rollen en/of autorisaties per gebruiker(sgroep), geen groepsaccounts, documenten (map/ordner) zitten in een afgesloten kast, en periodieke controle op juistheid en actualiteit van de autorisatiematrix, gebruikers en rollen (bijv. ieder half jaar).

5.1.2i
5.1.2i 5.1.2i
5.1.2i
5.1.2i

De autorisaties in 5.1.2i zijn zo ingeregeld, dat medewerkers van onze gemeenten alleen de zaken/meldplichten kunnen inzien die door de burgemeester van de gemeente Leeuwarden zijn opgelegd. Alleen functioneel beheerders van DV&O krijgen toegang tot alle zaken (van de drie deelnemende gemeenten), omdat dit nodig is voor de uitvoering van hun taak.

4.2 Welke encryptie gebruik je?

Encryptie is het versleutelen van informatie (bijv. bestand of netwerkverkeer) zodat deze onleesbaar is voor anderen. Er zijn verschillende manieren om de informatie te coderen. Versleutelen is i.i.g. belangrijk bij gegevensuitwisseling.



4.3 Hoe ziet de logging en monitoring eruit?

Loggen is het geautomatiseerd registreren van gegevens om bij te houden welke gebeurtenissen en handelingen binnen een systeem hebben plaatsgevonden en door wie. Loggen doe je voor analyse of controle. Zo kan je bijv. zien wanneer iemand heeft ingelogd, welke gegevens zijn geraadpleegd en welke wijzigingen zijn doorgevoerd. Monitoren is het continu bewaken van een apparaat of netwerk om te controleren of het nog goed werkt en om eventuele onregelmatigheden, dreigingen of fouten op te sporen. Denk ook aan het (veilig) bewaren van deze gegevens en periodieke controle .

Elke log in en elke klik en wijziging in de software worden gelogd, e.e.a. volgens het bepaalde in de Baseline Informatiebeveiliging Overheid (BIO), wat meebrengt dat de logging een half jaar wordt bewaard en dat op basis van die logging met een hoge mate van zekerheid de handelingen teruggeleid kunnen worden naar een natuurlijk persoon (persoonsniveau).
Alleen op verzoek wordt er op de logging gemonitord, er is geen beleid om dit actief te monitoren.

4.4 Hoe ziet het update en patchbeheer eruit?

Een nieuwe versie van het systeem zorgt voor extra functies (update) maar ook voor het repareren van zwakke plekken en een betere beveiliging (patch). Er moeten ook goede afspraken zijn over wie een nieuwe versie installeert, test en goedkeurt voordat deze in productie gaat.

Jaarlijks vinden 2 grote (major) releases (release beheer: 4.7.0. / 4.8.0./ enz.) plaats waarin de grotere systeem wijzigingen worden doorgevoerd.
Het kan ook voorkomen dat er klant specifieke toevoegingen aan de software worden toegevoegd, dit zijn de zogenoemde minor releases (release beheer: 4.7.1./ 4.7.2./ enz.). Als laatste is er het patch beheer, dit zijn de versies van de release waarop de software draait. In de patches zijn oplossing van bugs en kleine updates van de software. De patches worden gedaan in de zogenoemde mini release, voor de mini release is wekelijks tijd gereserveerd. In de mini release worden wijzigingen doorgevoerd op de Live omgeving die op de acceptatie omgeving zijn getest en goed bevonden, dit zijn o.a. de software patches.

4.5 Hoe is de continuïteit geregeld?

Er zijn verschillende maatregelen om de continuïteit van je proces te waarborgen. Zo kan je na een (grote) storing snel weer aan de slag. Voorbeelden: back-up en recovery/restore, testen uitwijk en herstel van mutaties.

Alle systemen zijn redundant uitgevoerd. Redundant betekent dat er meerdere systemen worden gebruikt om ervoor te zorgen dat een dienst of functie blijft werken, zelfs als één onderdeel faalt. Doel daarvan is het garanderen van continuïteit en het minimaliseren van de kans op dataverlies of systeemuitval.
Mocht er toch een verstoring voordoen, dan is er bij DV&O een BedrijfsContinuiteitsPlan voorhanden (dit betreft dezelfde procedure die bij DV&O voor andere taken wordt gehanteerd, zoals de monitoring van elektronisch toezicht bij TBS-gestraften (de 'enkelbanden')).

4.6 Wat is de procedure van de verwerker bij incidenten?

Een verwerker moet snel handelen bij een beveiligingsincident of datalek. Een beveiligingsincident is iedere gebeurtenis of actie die schade toebrengt of kan toebrengen aan de beveiliging van apparaten, systemen, informatie en gegevens. Het gaat om een inbreuk op de beschikbaarheid, integriteit (juistheid), vertrouwelijkheid en/of controleerbaarheid. Bij een beveiligingsincident zijn geen persoonsgegevens betrokken. Is dit wel het geval? Dan is er sprake van een datalek.

Op de intranet-pagina van DV&O is informatie beschikbaar wat te doen bij beveiligingsincidenten zoals mogelijke datalekken. Daarbij is door middel van een processchema (stapsgewijs) uitgelegd hoe te handelen. Voorts wordt voor een verdiepende beoordeling verwezen naar de site van de Autoriteit Persoonsgegevens (Datalek: wel of niet melden | Autoriteit Persoonsgegevens).

4.7 Wat is het beveiligingsniveau van de verwerker?

We zijn verplicht verwerkers in te schakelen die (ook) passende maatregelen nemen om de persoonsgegevens te beschermen. Daarom is het belangrijk te weten wat het beveiligingsniveau van een verwerker is. Heb je meerdere verwerkers ingeschakeld? Kopieer de tabel en vul voor iedere verwerker een aparte tabel in.

Verwerker	DV&O
☐ Werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten: De BIO (baseline informatiebeveiliging overheid): het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen in Nederland. ☐ Is volgens deze norm niet gecertificeerd. Certificering op basis van de BIO zelf is niet verplicht. ☐ Werkt volgens een andere norm, bijv. de BIO, te weten: BIO ☐ Heeft een actueel en geldig certificaat ☐ Heeft een actuele verklaring van toepasselijkheid (VVT): onbekend ☐ Heeft een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA: Nee. Wel een initieel pen test rapport van Fox -IT (2020) ☐ Is aangesloten bij een goedgekeurde/erkende gedragscode, te weten: standaard DJI gedragscode ☐ Voert jaarlijks een pentest uit: nee, niet op totaal netwerk (wel periodiek op delen). ☐ Beschikt over rapportages van periodieke controles zoals audits, pentesten, TPM's (bijv. ISEA3xxx SOC type II): rapportage van initiële pen test Fox-IT. ☐ Voert eigen controles uit of doet eigen mededelingen over de genomen beveiligingsmaatregelen: mochten zaken geconstateerd worden dan vinden daar acties en gevolg op.	

4.8 Zijn er nog andere beveiligingsmaatregelen genomen?

Het kan zijn dat er nog andere maatregelen zijn genomen, bijv. vanuit bepaalde wetgeving. Denk aan specifiek(e) informatiebeveiligingsbeleid, procedures of controles, eisen voor veilig verwijderen apparatuur en opslagmedia, aanwijzen functionarissen, etc. Beschrijf ook wie de maatregelen heeft genomen: de gemeente of een verwerker.

Een Quickscan ten aanzien van de informatiebeveiliging van de technische oplossing Mini-ID is op moment van schrijven in de afrondende fase, de daaruit voortvloeiende mitigerende maatregelen zullen worden geimplementeerd voorafgaand aan het starten van de verwerking van persoonsgegevens. In een eerdere fase is daarnaast een pentest uitgevoerd. DV&O heeft het volgende laten weten ten aanzien van deze 5.1.2i 5.1.2i

4.9 Heb je een (verwerkers)overeenkomst afgesloten of ga je dit nog doen?

Een organisatie die namens de gemeente gegevens verwerkt of een leverancier van een applicatie is een verwerker. Een andere organisatie kan ook samen met de gemeente verantwoordelijk zijn voor het verwerken van persoonsgegevens. Vaak is dit een ketenpartner. In beide gevallen moeten we een overeenkomst afsluiten. Met een verwerker sluiten we een verwerkersovereenkomst af. Bij gezamenlijke verantwoordelijkheid moeten we ook een overeenkomst afsluiten maar met andere bepalingen. Dit is vaak een convenant, regeling, DVO of samenwerkingsovereenkomst. Vermeld in onderstaande tabel de naam van de organisatie, de rol (verwerker of verantwoordelijke) en wat de status is (al afgesloten of nog afsluiten). Voeg zo nodig meer rijen toe of zet 'Niet van toepassing' neer. Twijfel je of en wat voor soort overeenkomst je moet afsluiten? Neem dan contact op met de Privacy Officer.*

Organisatie	Rol	Status overeenkomst
DV&O	Verwerker	Ligt voor bij DV&O ter ondertekening (status 8 april 2025)

**Leg een concept (verwerkers)overeenkomst altijd vooraf voor advies voor aan de Privacy Officer. Voeg bij een verwerkersovereenkomst ook altijd bewijsstukken van de verwerker bij over de genomen beveiligingsmaatregelen (bijv. een ISO-certificaat, TPM-verklaring of rapportage van een pentest). De Privacy Officer stemt deze stukken af met de ISO. Zijn de andere organisatie en de gemeente gezamenlijk verantwoordelijk? Dan is het niet nodig bewijsstukken over de genomen beveiligingsmaatregelen mee te sturen.*

5 Risico's en maatregelen

Het verwerken van persoonsgegevens kan negatieve gevolgen (risico's) hebben voor de rechten en vrijheden van betrokkenen. Het is belangrijk dat we deze inventariseren en maatregelen nemen om de gevolgen te beheersen (wegnemen of verminderen). Negatieve gevolgen kunnen te maken hebben met beschikbaarheid, integriteit (juistheid), vertrouwelijkheid en/of controleerbaarheid van persoonsgegevens. Maar ook met data-ethische aspecten. De gevolgen kunnen zich afspelen op het vlak van gegevens, medewerkers/organisaties, apparatuur/software en de omgeving.

5.1 Wat zijn de gevolgen voor betrokkenen en welke maatregelen ga je nemen?

In de tabel zijn de meest voorkomende privacyrisico's voor betrokkenen alvast ingevuld. Mogelijk zijn er meer risico's. Denk aan negatieve gevolgen voor betrokkenen vanuit data-ethiek (hoofdstuk 3). Of er zijn niet voldoende beveiligings-maatregelen genomen (hoofdstuk 4). Voeg deze dan toe aan de tabel. Geef ook aan wat de ernst (impact) is van de gevolgen voor betrokkenen: 'Laag', 'Midden' of 'Hoog'. Beschrijf bij ieder risico welke maatregel(en) je gaat nemen, wie dit gaat doen en wanneer. Heb je de maatregel al genomen? Zet dan 'Gereed' in de kolom Wie + Wanneer.

Risico	Impact	Maatregel	Wie + Wanneer
1. Gegevens verwerken voor ander doel dan afgesproken	Midden of Hoog	Werkprocessen (opvolgprotocollen) beschrijven welke gegevens in welke situatie verwerkt mogen worden.	Gemeente/DV&O
2. Betrokkenen kunnen hun rechten niet of onvoldoende uitoefenen	Hoog	Via https://www.leeuwarden.nl/privacy-en-avg/persoonsgegevens/ worden betrokkenen gewezen op hun rechten en via https://www.leeuwarden.nl/beslisboom-persoonsgegevens/ naar het juiste 'loket' begeleid, om de uitoefening van die rechten in goede banen te leiden. Intern wordt ook uitgebreide informatie verstrekt, via het lokale intranet (https://www.mijnwerk.frl/umbraco/leeuwarden/weten-regelen/digitaal-werken-privacy-en-gegevensverwerking/informatieveiligheid-en-privacy-avg/); daar wordt informatie verstrekt m.b.t. privacy en informatiebeveiliging, waarbij ook wordt verwezen naar de rechten van betrokkenen.	Gemeente
3. Betrokkenen zijn onvoldoende geïnformeerd over de verwerking	Midden	Bij installatiemoment en d.m.v. besluit burgemeester (incl. bijsluiter) wordt betrokkene geïnformeerd over de werking van de Mini-ID. Daarnaast zal op een website van de Rijksoverheid informatie (toegankelijk voor eenieder) worden verstrekt met het oog op de transparantieverplichtingen ex. de artt. 12, 13 en 14 van de AVG. Op het moment van schrijven is de inhoud daarvan onder constructie. In de bijsluiter/het informatieblad bij het besluit zal naar deze site worden verwezen. Mocht deze nog niet gerealiseerd zijn bij de oplegging, dan kan deze informatie in een aparte bijlage bij het besluit worden gevoegd. *Aanvulling n.a.v. aanbeveling 3 advies FG's 21 maart 2025*	Gemeente/DV&O
4. Meer gegevens verwerken dan afgesproken,	Hoog	Werkprocessen (opvolgprotocollen) beschrijven welke gegevens in welke situatie verwerkt mogen worden	Gemeente/DV&O

Risico	Impact	Maatregel	Wie + Wanneer
noodzakelijk of toegestaan			
5. Gegevens zijn niet volledig en/of niet juist	Hoog	Check 5.1.2i bij aanvang van de zaak (bij opmaken van besluit en registratie van de zaak in 5.1.2i), evenals 5.1.2i-check bij gebleken onjuiste NAW-gegevens. – dit zijn geen technische maar organisatorische maatregelen.	Gemeente
6. Onbevoegde persoon heeft toegang tot de gegevens	Hoog	Zie voorgaande toelichting over toegangsbeheer (4.1); beperkte toegang monitoringssoftware staat daaraan in de weg. I.c.m. pseudonimisering van de inhoud (namen worden louter met initialen weergegeven) wordt dit risico verder verkleind. Logging is daarnaast ook een technische maatregel om dit risico kleiner te maken. Mocht er onbevoegd toegang tot persoonsgegevens worden verkregen door een datalek, dan wordt procedure voor datalekken gevolgd bij DV&O (zie 4.6) of bij gemeente (zie https://www.mijnwerk.frl/umbraco/leeuwarden/veelgestelde-vragen-leeuwarden/wat-moet-ik-doen-bij-een-datalek/).	DV&O/gemeente
7. Iemand wijzigt of vernietigt gegevens terwijl dit niet de bedoeling is	Hoog	Zie voorgaande toelichting over vernietigen van persoonsgegevens (2.9). De beschreven opeenvolging van handelingen bij het wissen van gegevens, maakt de kans op het abusievelijk verwijderen heel klein.	DV&O/gemeente
8. Gegevens en/of applicatie zijn (tijdelijk) niet beschikbaar	Midden of Hoog	Sluitende afspraken tussen DV&O en 5.1.2i over calamiteiten/uitval 5.1.2i	DV&O/5.1.2i
9. Applicatie of koppeling met andere applicatie werkt niet goed	Midden of Hoog	Sluitende afspraken DV&O en 5.1.2i over functioneel beheer 5.1.2i Bij technisch falen van de Mini-ID/5.1.2i: door werken cf. opvolgprotocollen zal dergelijk technisch falen niet aande mepldichtige worden toegerekend (als zijnde een 'buiten schuld' -situatie). Het monitoringscentrum kan zien in het monitoringswindow of er iets aan de hand is met de werking van de Mini ID en heeft (cf. opvolgprotocollen o.a.) ook een handelingskader om de technische verstoring teniet te doen. Het monitoringscentrum moet in geval van technische verstoring dit ook vastleggen in het systeem dat de meldplichtige zich niet kon melden door technisch falen. Deze handelwijze heeft tot doel dat technisch falen bij ('buiten schuld') uiteindelijk niet op het bord van de medeplichtige wordt gelegd door burgemeester/officier van justitie *Aanvulling n.a.v. aanbeveling 11 advies FG's 21 maart 2025*	DV&O/5.1.2i
10. Gegevens zijn op onjuiste plek of meerdere plekken opgeslagen	Hoog	Door gerichte training op de werking van het systeem 5.1.2i binnen fase 1 van de Digitale Meldplicht zijn medewerkers gemeente goed geïnstrueerd hoe deze zaken te registreren. Bij foutieve registratie kunnen zij ofwel zelf herstellen, ofwel met backup vanuit DV&O (support of FB).	DV&O/Gemeente
11. Gegevens te lang/kort bewaren	Midden	Zie bovenstaande toelichting over het wissen van gegevens in 5.1.2i (2.9). Uitgangspunt is wissen na afloop Digitale Meldplicht (juiste bewaartermijn onderliggende besluit wordt geborgd door gebruik van ons eigen zaaksysteem 5.1.2i).	DV&O/Gemeente

Risico	Impact	Maatregel	Wie + Wanneer
12. Gegevens niet juist vernietigen	Midden	Zie bovenstaande toelichting over het wissen van gegevens in 5.1.2i (2.9).	DV&O/Gemeente
13. Gegevens delen met anderen die hier geen recht op hebben	Hoog	Opvolgprotocollen beschrijven juiste wijze gegevensdeling, i.c.m. toegangsbeheer 5.1.2i en werken met autorisaties wordt dit risico ondervangen. Logging is daarnaast ook een technische maatregel om dit risico kleiner te maken.	Gemeenten/DV&O/politie
14. Gegevens niet veilig uitwisselen/delen met anderen	Midden of Hoog	Opvolgprotocollen beschrijven juiste route gegevensdeling, i.c.m. toegangsbeheer systemen en werken met autorisaties wordt dit risico ondervangen. Ook hier: logging is daarnaast ook een maatregel die wordt ingezet om dit risico kleiner te maken.	Gemeenten/DV&O/politie
15. Taken en verantwoordelijk-heden zijn niet (goed) vastgelegd of niet actueel	Midden	Opvolgprotocollen beschrijven gedetailleerd de rollen en taken (gemeente, DV&O, OM en politie)	Gemeenten/DV&O/politie
Data-ethische risico's:			
16. Menselijke waardigheid: Door technische storing komen 5.1.2i niet binnen en treedt opvolgprotocol in werking	Midden	In opvolgprotocol is opgenomen dat DV&O (EM) bij niet-melden (of mislukte melding) eerst telefonisch contact opneemt met de meldplichtige, om oorzaak te achterhalen en zo mogelijk nieuwe melding uit te vragen. Bevindingen worden vastgelegd door EM, ook t.b.v. eventueel vervolgbeoordeling door politie/gemeente.	DV&O/gemeenten/politie
17. Autonomie: 3 meldingen doen in een periode van 6 uur (2 uur voor, tijdens, 2 uur na wedstrijd) kan als veel controle voelen.	Midden	In het opleggende besluit wordt duidelijk gemotiveerd waarom deze maatregel nodig is en hoe de maatregel in zijn werk gaat. In het informatieblad wordt de werking van de Mini ID uitgelegd. Tijdens de uitreiking (in aanwezigheid van medewerker gemeente en DV&O) is kennis en expertise aanwezig om vragen hierover van de betrokkene vragen te beantwoorden. Na afloop van fase 1 vindt een evaluatie plaats op allerlei onderdelen van de uitvoering.	Gemeenten
18. Veiligheid: Door technische storing kan gevoel van veiligheid mbt persoonsgegevens (vingerafdruk in het bijzonder) afnemen.	Midden	Vooraf uitleg over werking Mini ID (informatieblad, opleggend besluit). Tijdens uitreiking Mini ID kennis en expertise aanwezig om vragen hierover van de betrokkene te beantwoorden. Verder zal op een site van de Rijksoverheid aanvullende informatie – toegankelijk voor eenieder – over de digitale meldplicht worden verstrekt, in het bijzonder de informatie in het kader van de transparantieverplichtingen ex. de artt. 12, 13 en 14 van de AVG. Naar verwachting zal deze informatie in de loop van april/mei beschikbaar zijn. Maatregelen t.b.v. continuïteit (kans storing en effect daarvan beperken), procedure verwerker bij incidenten en informatiebeveiliging in het algemeen zijn in hoofdstuk 4 beschreven (deels met verwijzing naar opvolgprotocollen).	

5.2 Zijn er restrisico's?

Restrisico's zijn negatieve gevolgen die je niet (voldoende) kan wegnemen of verminderen met de maatregelen die je in de vorige paragraaf hebt beschreven. Noem de restrisico's en geef aan of en waarom deze aanvaardbaar zijn. Of licht toe waarom er geen restrisico's zijn.

Op het moment van invullen van deze DEPIA zien we geen overige risico's, zij het dat fase 1 van de Digitale Meldplicht nog een fase van oefenen/testen is. Dat brengt mee dat we op onvoorziene zaken kunnen stuiten die tot aanpassing van het e.e.a. nopen. Dat kan ook privacy- of data-ethische aspecten raken.

6 Beoordeling en advies FG

De FG's van gemeente Rotterdam, Den Haag en Leeuwarden hebben een gezamenlijk advies uitgebracht. De aandachtspunten vanuit dat advies zijn verwerkt in de DEPIA. Daarmee is voldoende aandacht voor de risico's en zijn er mitigerende maatregelen geformuleerd, welke bij de evaluatie meegenomen worden. De adviezen van de FG's dienen als bijlage bij deze DEPIA opgeslagen te worden.	
Datum: 10-04-2025	**Voorafgaande raadpleging AP nodig**: nee

Noot: De hierboven genoemde conclusies en aanbevelingen en het advies van de FG zijn gebaseerd op de informatie zoals in deze DEPIA is beschreven. Ga je hiervan afwijken? Dan is het nodig de DEPIA aan te vullen of te wijzigen (zie ook aandachtspunt 4 onder Tot slot). Vervolgens vindt een nieuwe beoordeling plaats.

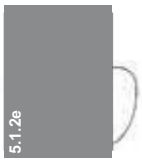
Tot slot

Na de beoordeling en het advies van de FG vul je onderstaande tabel in. Als laatste volgt een beoordeling van de proceseigenaar. De proceseigenaar is de teamleider/manager die verantwoordelijk is voor het project/proces.

Wat is de startdatum van de verwerking?	2 april 2025

Beoordeling proceseigenaar

Akkoord met DEPIA.



Aandachtspunten

1. **Verwerkersovereenkomst**: Heb je een verwerkersovereenkomst afgesloten of ga je dit nog doen? Bewaar de door beide partijen ondertekende verwerkersovereenkomst in 5.1.2i en in 5.1.2i bij het contract met de andere organisatie of de leverancier van een applicatie.
2. **Overeenkomst ketenpartner(s)**: Heb je een overeenkomst afgesloten met (een) ketenpartner(s)? Bewaar de door beide/alle partijen ondertekende overeenkomst (convenant, regeling, etc.) in 5.1.2i.
3. **Bijwerken register van verwerkingen**: Nieuwe verwerking? Of wijziging van een bestaande verwerking? Lever de nieuwe of gewijzigde informatie aan via 5.1.2i @leeuwarden.nl zodat we deze in het register van verwerkingen kunnen opnemen. Twijfel je? Vraag advies aan de Privacy Officer.
4. **Bewaren DEPIA**: Is je DEPIA goedgekeurd? 1) maak een zaak aan in 5.1.2i (tenzij je al een zaak hebt voor de pre-DEPIA), 2) vul datum en zaaknummer in op het voorblad, 3) bewaar de DEPIA in 5.1.2i, 4) geef het zaaknummer door aan 5.1.2i @leeuwarden.nl.
5. **Herbeoordeling DEPIA**: Iedere drie jaar moet je een herbeoordeling van de DEPIA uitvoeren. Dit is ook tussentijds nodig bij ingrijpende wijzigingen van een bestaande gegevensverwerking. Twijfel je of een herbeoordeling nodig is? Vraag advies aan de Privacy Officer.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2, 7, 15, 25
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	4, 5, 6, 10, 11, 12, 13, 14, 15, 18, 19, 20, 21, 23, 24, 26

DEPIA Spraak assistent

Wie zijn betrokken bij DEPIA vanuit expertise
(bijv. ISO, juridische expertise, inkoop, procesontwerper etc.)

Functie	**Naam**
Projectleider	5.1.2e
Proceseigenaar	5.1.2e
Privacy Officer	5.1.2e
Inkoop	
ISO	5.1.2e
FG	5.1.2e
Data-ethiek	5.1.2e

Planning
Vul in wat van toepassing is voor het betreffende project.

	Taak	**Datum gereed**
Fase 1	Uitvoeren Pre-DEPIA	
	Beoordelen Pre-DEPIA door FG	
	Voorafgaande raadpleging van AP (indien van toepassing)	
Fase 2	Uitvoeren DEPIA; invullen door projectleider/beleidsmedewerker	
	Uitvoeren DEPIA; raadplegen PO	
	Uitvoeren DEPIA; raadplegen ISO	
	Uitvoeren DEPIA; raadplegen data-ethiek	
Fase 3	Eerste beoordeling door FG	6-3-2024
	Indien van toepassing; uitvoeren moreel beraad of inzetten data-ethische commissie.	
	Reflectie op de data-ethische waarden vanuit moreel beraad of data-ethische commissie toevoegen aan DEPIA	
	Indien van toepassing; aanpassen DEPIA	
	Beoordeling door FG en Adviseur Data-ethiek	12-4-2024
Fase 4	Eindbeoordeling bestuur/MT/Proceseigenaar	
	Opslaan documenten (Pre-DPIA. DPIA)	
	Bepalen mate van vertrouwelijkheid documenten	
	Toesturen zaaknummer vanuit 5.1.2i naar FG	
	Herziening DEPIA inplannen (3 jaar na datum definitieve versie DEPIA)	

1. Algemeen

Beschrijf het doel, de inrichting en de stakeholders bij het voorgestelde project/proces/experiment

1.1: Wat wil je bereiken met het proces/project? (wat is het doel)

Geef aan welk(e) doel(en) de organisatie met de (nieuwe of gewijzigde) werkprocessen wil bereiken en/of binnen welke context deze gezien moet(en) worden.

wij spreken over een inwoner, hiermee bedoelen wij een gebruiker van het systeem, dit kan dus ook een ondernemer of bezoeker van onze gemeente zijn

Met het implementeren van een spraak assistent willen wij twee dingen bereiken.
1 Dat wij 24/7 bereikbaar zijn. Het is een extra selfservice mogelijkheid om bij de gemeente Leeuwarden een melding woon- werk en leefomgeving te kunnen doen. Daarnaast staat de telefonische bereikbaarheid van onze dienstverlening staat onder druk, en hiermee kunnen we onze bereikbaarheid verbeteren.
2 Onze dienstverlening inclusiever te maken. Doelgroepen die bijvoorbeeld een drempel ervaren bij direct klantcontact, of onze digitale dienstverlening, kunnen gebruik maken van dit kanaal.

Dit is het eerste proces waarbij we gebruik maken van spraaktechnologie. Bij succes, zullen meerdere processen volgen. Het is de bedoeling dat deze technologie ons kan helpen om de bereikbaarheid (14 058) substantieel te verbeteren. Buiten openingstijden bepaalde diensten door te laten lopen. En onze dienstverlening inclusiever te maken.

Advies FG: Doel is duidelijk omschreven.

1.2: Hoe werkt het precies?

Beschrijf het systeem, de applicaties, de in- en output, of er acties worden gedaan zonder tussenkomst/beoordeling van de mens (maak een plaatje van het proces).

De spraak assistent wordt aangeboden wanneer een inwoner naar 14058 belt. De inwoner krijgt een tekst te horen en krijgt de optie aangeboden om een melding via spraak te doen. Deze optie wordt zowel tijdens openingstijden, als buiten openingstijden aangeboden. Ook bij lange wachtrijen, wordt deze optie nogmaals aangeboden.

Als de inwoner kiest voor deze optie in het menu, word je doorverbonden met de spraak assistent. Vanaf dat moment gaat alles via spraak.

- Er volgt eerst een korte uitleg
- Daarna wordt er om de locatie gevraagd
- Daarna spreekt de inwoner de melding in met zoveel mogelijk details
- Daarna vraagt de spraak assistent om gegevens: naam, mailadres en/of telefoonnummer. Dit is niet verplicht. Er wordt uitgelegd waarom we dit vragen. Voor als de melding niet duidelijk is en dat we de melding daarmee in het systeem registeren en dat ze dan via 5.1.2i de melding kunnen volgen.
- De inwoner ontvangt, als ze naam, mailadres ingesproken hebben een bevestiging via 5.1.2i.

De melder kan altijd stoppen, door het gesprek te beëindigen. Omdat de melding dan niet compleet is, nemen we deze ook niet in behandeling.
Als de ingesproken tekst niet compleet is of niet goed verstaanbaar, neemt de S&I medewerker contact op met de inwoner. Als de inwoner geen gegevens heeft achtergelaten, kan de melding niet opgemaakt worden.

Het audiobestand wordt meegestuurd door het systeem naar de S&I medewerker. Als de melding niet opgemaakt wordt omdat hij incompleet is en inwoner niet bereikt kan worden of is wel ingevoerd in het systeem, dan wordt de mail in een mapje in outlook gezet en dit mapje wordt 1x per week op vrijdag automatisch geleegd door gegevensbeheer.

De spraak assistent verstaat nu alleen de Nederlandse taal. Als er toch een andere taal wordt gesproken, kan de medewerker van S&I het audiobestand afluisteren en alsnog de melding invoeren.

De gemeente kan niet meeluisteren tijdens de opnames. Omdat de opnames direct binnenkomen bij 5.1.2i 5.1.2i.

Tekstflow spraak assistent:

Een inwoner belt de voice assistent.

Welkom bij de Gemeente Leeuwarden.
U spreekt met de spraak assistent (naam geven?).
Bij mij kunt u een melding doorgeven als iets kapot is, of beter kan in uw woon-, werk-, of leefomgeving.
Ik stel u een paar vragen.
Als u de vraag beantwoord heeft, gaat u vanzelf door naar de volgende vraag.

Wat is uw melding? Vertel zoveel mogelijk details over wat er aan de hand is.

Inwoner spreekt de melding in.

Wat is de locatie van de melding? Spreek in ieder geval het adres en de plaatsnaam in. Extra details over de precieze locatie mag u ook in spreken.

Inwoner spreekt de locatie in.

Bedankt voor uw melding. Wij sturen de melding door naar de verantwoordelijke afdeling en pakken deze zo spoedig mogelijk op.

Als er nog vragen zijn over de melding, willen wij graag contact met u opnemen. Daarom vragen wij om uw telefoonnummer en e-mailadres. Wilt u dit liever niet, verbreek dan nu de verbinding.

Spreek uw telefoonnummer in.

Inwoner spreekt telefoonnummer in.

Spreek uw e-mailadres in.

Inwoner spreekt e-mailadres in.

Bedankt voor uw melding.

Wij zouden graag uw feedback willen weten over dit gesprek. Vond u het fijn om uw melding door te geven via mij?
Inwoner spreekt feedback in.

Bedankt, wij wensen u een fijne dag.

*dit is de tekst van de huidige flow 17/01/24, over 1 week hebben een laatste gebruikerstest. Het is mogelijk dat we op basis van deze ervaringen nog aanpassing gaan doen.



Wanneer de melding is ingevoerd in 5.1.2i, krijgt de melder een bevestiging vanuit 5.1.2i, met als voorwaarde dat de melder een mailadres heeft ingesproken.

Proces bij S&I administratieve medewerker:
Afdeling S&I Administratieve groep ontvangt deze informatie in een algemene mailbox waar alleen deze specifieke groep collega's toegang tot heeft. Dit is het afgesproken werkproces:*

- Mailsjabloon met melding wordt dagelijks verwerkt.
- Als melding ingevoerd is in 5.1.2i, gaat de mail naar mapje: VERWERKT
- Deze map wordt dagelijks automatisch gewist
- Als de melding niet compleet is wordt er contact opgenomen met de inwoner (telefonisch of per mail)
- Als er gewacht moet worden op antwoord, gaat de mail in het mapje: IN AFWACHTING
- Als de inwoner na 3 dagen nog niet gereageerd heeft gaat er nog 1 herinneringsmail/voicemail naar de inwoner
- Als de inwoner na 7 dagen nog niet gereageerd heeft, gaat er een mail/voicemail naar de inwoner dat we de melding niet op kunnen pakken en dat als de melding alsnog opgepakt moet worden, ze contact met ons op kunnen nemen. Als we gegevens van de inwoner hebben, vermelden we dit in 5.1.2i (KCS). Als er geen gegevens zijn, wordt er niets geregistreerd.

*dit is het afgesproken werkproces op 8-1-24. We gaan dit nog 1x testen voor livegang. En de 3 maanden na livegang blijven we dit werkproces evalueren en indien nodig aanpassen. Dit gaat in samenwerking met de medewerkers van S&I Administratieve groep. Bij wijzigingen DEPIA aanpassen.

Advies FG: goede omschrijving van het proces en ook de risico's hierin zijn opgenomen in het overzicht.

1.3: Hoe worden de persoonsgegevens gebruikt?
Beschrijf alle gegevensverwerkingen (Een verwerking is alles wat je met persoonsgegevens kunt doen: verzamelen, vastleggen, opslaan, bijwerken of wijzigen, opvragen, raadplegen, versturen, combineren, afschermen, vernietigen).

In de gespreksflow worden er om de volgende persoonsgegevens gevraagd, deze gegevens zijn niet verplicht. Er kan dus ook anoniem een melding worden gedaan. Dit heeft wel tot gevolg dat als de melding niet compleet of duidelijk is wij geen contact met de inwoner op kunnen nemen:

- Telefoonnummer
- Mailadres

Het audiobestand van het gesprek wordt bij de externe partij 5.1.2i 5.1.2i direct omgezet naar tekst en in het mailsjabloon gezet. Deze mail wordt direct verstuurd naar het algemene mailadres van S&I (1 mailadres). 5.1.2i 5.1.2i wist direct de bestanden zodra het naar ons gemaild is.

De inbox van de algemene mailbox van S&I wordt dagelijks verwerkt door een persoon die hiervoor ingepland is. En aan het einde van de dienst, worden alle mailtjes verdeeld over twee mappen.

- Navraag bij inwoner
- Afgerond

Map 1: 'in afwachting' zijn mailtjes waarbij de medewerker contact heeft gezocht.
Er is afgesproken dat als we de inwoner gemaild hebben, we 7 dagen wachten en als er geen reactie is, gaat de mail naar afgerond. In het onderwerp van de mail komt de datum dat de mail naar afgerond kan, mits inwoner gereageerd heeft. De medewerker die administratie dienst heeft bij S&I controleert elke dag deze map.
Map 2: 'verwerkt' hierin komen alle afgeronde mailtjes. Ik heb met Gegevensbeheer afgesproken dat de map automatisch dagelijks geleegd wordt.

De stem van de inwoner wordt opgenomen en in een audiobestand bewaard. Het audiobestand wordt per mail door leverancier verzonden. De leverancier verwijdert het verzonden bericht direct.

Veilig verzenden van de mail (encrypten):
5.1.2i 5.1.2i gebruikt 5.1.2i (5.1.2i). 5.1.2i gebruikt encryptie in transit om de e-mails van de email server naar de Gemeente email server te versturen. Dus de e-mails worden al encrypted verstuurd.

Tijdens de evaluatieperiode, gaan we elk bericht controleren zodat we dit goed monitoren en indien nodig actie kunnen ondernemen. Daarnaast mailen we geen gevoelige informatie naar het mailadres. Mocht dit wel nodig zijn, dan mailen we met het verzoek contact met ons op te nemen.

5.1.2i geeft als mogelijke oplossingen aan: *Als in de evaluatieperiode blijkt dat het veelvuldig voorkomt dat de ingesproken mailadressen foutief worden overgenomen, zijn de volgende oplossingen in te bouwen:* - *Inzetten van een large language modellen zoals ChatGPT om teksten te corrigeren.** - *Je kunt de inwoner zijn e-mailadres 2x laten inspreken. Je ziet vaker bij diensten waar een email adres voor nodig is dat je het 2x moet opgeven. Daarmee controleer je of het eerste email adres dat de gebruiker/inwoner opgeeft correct is.* **we informeren* 5.1.2i over de afspraken die we hebben binnen de gemeente, als we gebruik gaan maken van deze oplossing ChatGPT - Digitale werkomgeving van jouw organisatie (mijnwerk.frl)
Advies FG: Akkoord en duidelijk omschreven

1.4: Welke stakeholders zijn betrokken? (klant/client/inwoner, leveranciers, eindgebruikers en andere belanghebbenden)

Maak een stakeholderanalyse omtrent rol, positie, verwachtingen/wensen en hun rol vanuit de AVG: (verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger; vraag bij twijfel de privacy officer)

Stakeholder	Rol	Positie	Verwachtingen/wensen	Rol vanuit AVG
Melder	Gebruiker	Voorstander/ tegenstander	Eenvoudig en efficiënt melding maken	Betrokkene
Medewerkers S&I	Gebruiker	Voorstander/ tegenstander	Invoeren melding in 5.1.2i	n.v.t.
ICT/servicedesk	Onderhoud en support	Neutraal	Ondersteuning software en ontwikkeling	n.v.t.
Adviseur dienstverlening	Adviseur	Voorstander	Extra laagdrempelige optie melding voor inwoners. Mogelijk uitbreiding tbv bereikbaarheid.	n.v.t.
Manager	Proceseigenaar	Voorstander	Implementeren spraakassistent	n.v.t.
Leverancier	Verantwoordelijke software-ontwikkeling	Voorstander	Spraaktechnologie tbv overheid ontwikkelen	Verwerker
College van B&W		Voorstander	Ontwikkeling digitale dienstverlening	Verwerkingsverant-woordelijke
Advies FG: akkoord.				

2. Baten

Bij baten kun je denken aan vrijheid, welzijn, welvaart, duurzaamheid, inclusiviteit en diversiteit, gelijkheid, efficiëntie en kostenreductie. (Deze brede benadering is belangrijk, omdat ethische en juridische aspecten invloed kunnen hebben op de relatie tussen onze organisatie en de omgeving)

2.1: Wat zijn de baten voor gemeente Leeuwarden als organisatie?

De baten voor de gemeente Leeuwarden zijn: - Betere klanttevredenheid - Meer inclusiviteit voor inwoners - Uitbreiding kanaalkeuze - Digitale vooruitgang: gemeente zet innovatieve oplossing in, imagoverbetering - Kostenreductie (vrijwel geen personele uren nodig, alleen investering) - Ervaring opdoen met spraaktechnologie en wellicht daarna techniek breder inzetten tbv bereikbaarheid - Techniek wellicht inzetten tbv interne medewerkers (gespreksverslagen, rapportages ed.)
Advies FG: akkoord.

2.2: Wat zijn de baten voor het individu?

De baten voor het individu zijn: - 24/7 mogelijkheid om melding woon- werk- en leefomgeving te doen - Toegankelijke mogelijkheid om contact met Gemeente te hebben voor het doen van een melding voor de doelgroep: blind/slechtziend en /of inwoners die liever geen persoonlijk contact hebben - Vergroten van keuze mogelijkheden kanalen voor inwoner - Vergroten van inclusiviteit - Wachtrij reductie - Verbreding van de (selfservice) dienstverlening Het voordeel van deze technologie t.o.v. digitale dienstverlening via de website is dat het merendeel van onze inwoners contact blijft zoeken via 14058 (gewoonte gedrag). Dit is dus de ingang waarbij we een grote groep inwoners bereiken. Tijdens het bellen, worden er announcements afgespeeld, hier verwijzen we inwoners ook naar de optie van de website en hier voegen we de spraak assistent aan toe. De inwoner heeft hierdoor een extra mogelijkheid en dus keuze vrijheid. Wij denken aan twee doelgroepen: een groep die minder/niet digitaal vaardig zijn (waaronder zilveren doelgroep) en dan liever voor een spraakoptie kiezen. Ook zien we dat spraak technologie door de jongere doelgroep als 'normaal' worden ingezet. Zij gebruiken veelvuldig spraaktechnologieën: Siri, spraakberichten whatsapp. *Uiteindelijk kan deze technologie ook ingezet worden om de inwoner die belt gelijk op de juiste routering te zetten. Wat betekent dat ze niet eerst hun verhaal/vraag aan een 'algemene' medewerker hoeven te stellen maar gelijk bij de juiste medewerker terecht komen.*
Advies FG: akkoord.

2.3: Wat zijn de baten voor de Leeuwarder samenleving als geheel?

- Mogelijkheid om 24/7 een melding te doen, iedereen heeft een mobiele telefoon mee als ze onderweg zijn. - Verbeterde leefbaarheid en veiligheid omdat inwoners laagdrempelig zaken kunnen melden, welke ze anders niet melden. En er wellicht grotere problemen worden voorkomen (piepsysteem). - Positieve gemeenschapsbeleving: inwoners voelen zich betrokken omdat ze meehelpen de omgeving te verbeteren. - Kostenbesparing en daarmee komt er maatschappelijk geld vrij voor andere belangrijke prioriteiten.
Advies FG: akkoord.

3. Verantwoording; Is het doel en hoe het doel wordt bereikt juridisch en ethisch verantwoord?

Beschrijf de invloed die het gebruik van gegevens of techniek heeft/kan hebben op menselijke en maatschappelijke waarden en belangen.

Wanneer de verwerking invloed heeft op de data-ethische waarden, betekent dit vaak dat de belangen van stakeholders geschaad worden. Dit kan richting geven aan de beoordeling of een toepassing data-ethisch verantwoord is. Hieronder staan de ethische waarden, die voor gemeente Leeuwarden van belang zijn.

- ***Rechtvaardigheid:***
  We dragen bij aan rechtvaardigheid, gelijke kansen en inclusiviteit. Onze digitale oplossingen zijn laagdrempelig en waardevol voor iedereen. We zijn alert op het voorkomen van ongewenste vooringenomenheid bij de selectie van data. Ook letten we erop dat er geen discriminatie, stereotypering of vooroordelen in algoritmes zit (bias).

- ***Machtsevenwicht/machtsverhoudingen:***
  We streven ernaar dat bewoners, ondernemers en bezoekers vertrouwen hebben in de gemeente en onze digitaliseringstrajecten. We toetsen of digitale oplossingen echt meerwaarde hebben voor de gemeente.

- ***Menselijke waardigheid:***
  We behandelen bewoners, ondernemers en bezoekers als mensen, niet als ‘nummer’. Onze digitaliseringstrajecten sluiten aan bij de leefwereld en behoeften van de mensen in onze gemeente. De mens is altijd leidend, niet de techniek/data.

- ***Privacy:***
  We beschermen de privacy van bewoners en ondernemers. Data van inwoners worden geanonimiseerd gebruikt en zijn niet herleidbaar tot een persoon. We gebruiken ‘Privacy by design’ en doen onderzoek naar de impact van digitaliseringstrajecten op de privacy.

- ***Veiligheid:***
  We waarborgen de openbare orde en veiligheid, zodat iedereen zich veilig voelt in onze gemeente. We beveiligen onze data. Via cybersecurity bereiden we ons voor op digitale aanvallen.

- ***Autonomie:***
  We respecteren menselijke autonomie (vrijheid). We vermijden onbewuste beïnvloeding, manipulatie en stimulering van dwangmatig gedrag of overheidstoezicht (‘Big Brother’). We zijn terughoudend met het gebruik van data waarmee we gebruikers kunnen volgen, hun reputatie schaden of hun toekomst negatief kunnen beïnvloeden.

- ***Controle over technologie:***
  We controleren of onze digitaliseringstrajecten nog goed werken. We letten op datastromen en -opslag. Door open en transparant om te gaan met data en informatie, kan iedereen deelnemen op basis van dezelfde kennis en inzichten.

- ***Kwaliteit van leven/duurzaamheid:***
  We vinden gezond en duurzaam leven belangrijk in Leeuwarden. We zoeken naar duurzame oplossingen waarbij de gezondheid van bewoners, ondernemers en bezoekers voorop staat. Dat geldt ook voor onze digitaliseringstrajecten.

3.1: Welke van de eerdergenoemde waarden worden beïnvloed of geraakt door het project/proces?

Beoordeel in de onderstaande vragen of er één of meerdere waarden zijn die mogelijk geraakt worden door het project/proces. (Als de waarde negatief wordt geraakt, neem deze dan op in de risico’s bij vraag 11.3 en 11.4)

- **Rechtvaardigheid**: de spraak assistent draagt bij aan inclusiviteit. Als de inwoner moeite heeft met de Nederlandse taal, als er Fries wordt ingesproken, iemand stottert of iets dergelijks, niemand wordt buitengesloten. Ook deze inwoners mogen hun melding inspreken. We hebben er bewust voor gekozen dit niet in de intro te benoemen. Als de audio niet goed wordt vertaald, gaat de medewerker van S&I de audio afluisteren en de melding aanvullen. Dit hoort bij de dienstverlening, dit is voor ons maatwerk.
- **Menselijke waardigheid:** de spraak assistent draagt bij aan behoeftes in onze gemeente. Een half jaar geleden hebben we een gebruikerstest gedaan onder meer dan 20 inwoners gecategoriseerd in verschillende doelgroepen. NT2, laaggeletterden, blind- slechtzienden, jongeren, ouderen. De resultaten uit deze gebruikerstesten hebben ertoe geleid dat we een aantal zaken hebben aangepast. De tekstflow is aangepast en de focus doelgroep voor laaggeletterden hebben we meer losgelaten. De doelgroep is groter, de insteek is verbreed, het doel is aangepast. Daarnaast is dit een aanvulling op de verschillende opties waarop een inwoner een melding kan doen. De inwoner blijft regisseur in zijn eigen keuze.
- **Privacy**: we beschermen de privacy van onze inwoners. We vragen alleen gegevens die echt nodig zijn voor de melding. Eerst vroegen we de naam van de inwoner, dit hebben we aangepast toen de project-groep van 5.1.2i dit ook heeft gedaan. Ons proces is zoveel mogelijk hetzelfde ingericht als bij 5.1.2i.
- **Controle over technologie:** om te controleren of de techniek het juiste mailadres overneemt gaan we de eerst 3 weken elke melding controleren met dat wat er ingesproken is. Op voorhand gaan we in de laatste gebruikerstest (eind jan 2024) de bevindingen omtrent dit onderwerp nog aanpassen voordat we live gaan. Opties hiervoor zijn: twee keer om het mailadres vragen, of vragen of de inwoner het mailadres wil spellen.
- **Controle over technologie:** 5.1.2e stelt in dat het mapje in de mailbox van S&I eind van de dag automatisch geleegd wordt. In de eerste drie weken, vragen we de medewerker van S&I om aan het begin van de werkdag een controle te doen of hij geleegd is.

Als er een risico is bij 1 van deze waarden, heb ik ze benoemd in de lijst met risico's 11.3.

Advies FG: akkoord, indien er risico's zijn opgenomen in de lijst bij vraag 11.3.

3.2: Welke wet-, regelgeving en beleid is betrokken bij de gegevensverwerkingen?

Denk aan wetten, besluiten, gedragscodes, convenanten of beroepscodes. Ook normenkaders zoals voor de IT General Controls: de internationale norm ISO/IEC 27002 en de BIO. (vraag eventueel de privacy officer/privacy jurist).

Er is geen overkoepelend wettelijk kader voor het beheer van de openbare ruimte. De gemeente heeft te maken met diverse landelijke wet- en regelgeving en met eigen regelgeving (o.a. APV). Algemeen uitgangspunt is dat de gemeente een zorgplicht heeft voor het handhaven en bevorderen van de veiligheid in de openbare ruimte. De onderliggende wet- en regelgeving is ook afhankelijk van de aard van de melding. Belangrijkste landelijke wet- en regelgeving: Gemeentewet, Drank- en Horecawet, Omgevingswet, Wegenwet, Wet milieubeheer, Woningwet en Warenwetbesluit Attractie- en speeltoestellen.
Wij hebben een visie op Dienstverlening, deze sluit aan op een aantal onderwerpen in het coalitieakkoord:

Persoonlijke en passende dienstverlening,
Onze dienstverlening moet aansluiten bij de wensen van inwoners, bezoekers en bedrijven. Mensen willen van de gemeente een snel en duidelijk antwoord op hun vragen. Het maakt niet uit of ze bellen, chatten of online zaken met ons willen doen. Ze zijn hun eigen regisseur in het zoeken naar informatie of ondersteuning en beheren in de toekomst hun eigen gegevens. We gaan onze dienstverlening verbeteren en digitaliseren. Wij denken met meer digitale dienstverlening en een betere (telefonische) bereikbaarheid een eerste aanzet te kunnen geven tot meer ruimte voor persoonlijk contact en maatwerk.

De gemeente is de meest nabije overheid. Juist daarom is het van belang dat onze dienstverlening passend en persoonlijk is. Iedereen moet ermee uit de voeten kunnen. We willen dat de contactmogelijkheden voor inwoners aansluiten bij hun vaardigheden. Met de inzet van ervaringsdeskundigen maken we de toegang voor kwetsbaren laagdrempeliger. Mensen met (complexe) vragen mogen niet vastlopen in onze systemen en daardoor in de problemen komen. Met extra geld van het Rijk (POK-middelen) versterken we de dienstverlening aan deze groep. Daarnaast investeren we de komende periode in eenvoudige (digitale) aanvraagprocessen, betere (telefonische) bereikbaarheid, informatie in begrijpelijke taal en nieuwe technieken (onder andere videobellen). Zo verbeteren we de communicatie met onze inwoners.

Er is een visie op Dienstverlening. Deze is in 2023 vastgesteld door het MT Publieke Dienstverlening en het DT.
Advies FG: Akoord

4. Persoonsgegevens & Betrokkenen

4.1: Van welke type personen worden persoonsgegevens verwerkt? En welke persoonsgegevens worden van elk type persoon verwerkt?

Denk aan medewerkers, consumenten, kinderen, cliënten, bezoekers, gebruikers of inwoners van een gemeente. Denk bij persoonsgegevens bijvoorbeeld aan naam, adres, telefoonnummer, BSN, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, kenteken, bankrekeningnummer en -saldo, functie, opleiding, inkomens-en vermogensgegevens, lidmaatschap vakbond, persoonlijke voorkeuren, loonschaal, gespreksverslagen, gegevens over de gezondheid of strafrechtelijke gegevens (Denk bij risicoklasse I aan NAW, bij II aan bijzondere persoonsgegevens zoals ras, etniciteit en gezondheid en bij III aan strafrechtelijke gegevens).

Persoon	Soort persoonsgegeven	Risicoklasse
Bijv. medewerker	Bijv. emailadres, telefoonnummer	I
Melder	E-mailadres en/of telefoonnummer (alle niet verplicht), stem.	I
Een stem is een biometrisch persoonsgegeven (bijzonder persoonsgegeven - categorie II). Het verwerken van een stem voor de spraak assistent is in dit geval een gewoon persoonsgegeven: 1. Het verwerken van de stem is niet gericht op een bijzonder persoonsgegeven of het maken van onderscheid op basis van dit gegeven. 2. Het is redelijkerwijs niet te voorzien dat iemand onderscheid maakt op basis van een stem. 3. Het is onvermijdelijk een stem te verwerken bij het gebruiken van de spraak assistent. Bovengenoemde is gebaseerd op de redenering van de Autoriteit Persoonsgegevens dat als het maken van foto's en filmpjes aan bovengenoemde drie punten voldoet, het geen bijzondere persoonsgegevens zijn.		
Advies FG: akkoord.		

4.2: Wie hebben er toegang tot de gegevens?

- Beheerder/leverancier (externe organisatie) - Medewerker S&I (Administratieve groep) - Medewerkers 5.1.2i (medewerkers die werken met 5.1.2i: o.a. Medewerker Meldpunt Overlast, Buitendienst) Er is voorlopig nog geen functioneel beheerder. Dit omdat het eerst een proefperiode betreft waarbij de leverancier tevens de beheertaken op zich neemt.
Advies FG: akkoord.

5. Waar worden de gegevens opgeslagen?

Bijvoorbeeld in de 5.1.2i of op onze eigen servers. Benoem ook eventueel in welke landen de gegevensverwerkingen en opslag plaatsvinden. Waar slaan (sub)verwerkers de gegevens op?

Leverancier: De leverancier slaat de audiobestanden op in een bucket die zij hosten op 5.1.2i 5.1.2i. Zij hebben hier volledige controle over, en zij kunnen zelf de security en access levels inzetten. Daarnaast hosten zij de applicatie ook op 5.1.2i 5.1.2i. Voor zowel de bucket voor het opslaan van de audiobestanden als het hosten van de applicatie op 5.1.2i 5.1.2i gebruiken zij: West Europe als Region. Dus alles wordt in West Europe opgeslagen. De audiobestanden worden wel na het versturen meteen verwijderd, zodat we zo min mogelijk risico lopen. Gemeente Leeuwarden: - S&I ontvangt de mail in de algemene mailbox 5.1.2i @leeuwarden.nl. - de melding wordt opgemaakt > mail gaat in mapje die dagelijks automatisch verwijderd wordt

- als melding (nog) niet opgemaakt kan worden en er contact met inwoner gezocht gaat worden. Gaat de melding in mapje 'in afwachting' na 3 dagen wordt er een reminder naar inwoner gestuurd. Na 7 dagen, nog geen reactie, dan wordt de melding niet opgemaakt en gaat de mail handmatig verwijderd worden door medewerker.
Advies FG: akkoord, want ISO heeft akkoord gegeven

6. Hoe lang worden de persoonsgegevens bewaard en vervolgens vernietigd?

De bewaar- en vernietigingstermijnen staan in de Gemeentelijke selectielijst en kun je opvragen bij 5.1.2e

Advies 5.1.2e – Information en records officer De audiobestanden kunnen vrij snel verwijderd worden. Dit kan door bijvoorbeeld de verwerkte mails met audiobestand in een map in de mailbox te plaatsen en hier een vernietigingstermijn op te plaatsen. Een outlook map, wordt ingesteld om wekelijks automatisch te legen. Dit gaan we doorvoeren: De bewaartermijn is 1 dag. Alle mailtjes in een specifieke map, worden eind van de werkdag automatisch verwijderd.
Advies FG: akkoord

7.1 Is er sprake van (semi-) geautomatiseerde besluitvorming en/of profilering? Zo ja, beschrijf deze?

Geautomatiseerde besluiten worden zonder medewerker genomen. Profileren is het opbouwen van profielen waarmee je mensen in categorieën kunt indelen.

Nee

7.2 Wordt er gebruik gemaakt van nieuwe technologieën zoals kunstmatige intelligentie (AI), Robotisering (RPA), biometrie etc? Zo ja, beschrijf deze

Ja, er wordt gebruik gemaakt van AI en ML. Daarnaast worden vanuit de LDA ook experimenten met AI en LLM gedaan. De toepassing van spraaktechnologie wordt via dit programma gestimuleerd. Verder wordt een stem verwerkt. Een stem is een biometrisch gegeven maar deze wordt niet met dit doel vastgelegd (zie nadere toelichting in 4.1).
Advies FG: Akkoord

8. Op welke rechtsgronden zijn de verschillende gegevensverwerkingen gebaseerd?

Als er sprake is van een publieke taak of wettelijke verplichting moet deze (zo veel mogelijk) te herleiden zijn naar specifieke bepalingen in de betreffende wetgeving. (vraag de privacycontactpersoon van jouw domein om deze vraag te beantwoorden)

De gemeente verwerkt de persoonsgegevens voor het afhandelen van Meldingen Openbare Ruimte. Dit is een taak van algemeen belang / openbaar gezag (AVG artikel 6 lid 1 sub e).
Advies FG: akkoord

9. Is de verwerking in lijn met het doel of is er sprake van een verenigbare verdere verwerking?

Gebruik je de persoonsgegevens die je voor dit proces of project hebt verzameld ook nog voor iets anders? Is deze verdere verwerking dan verenigbaar is met het doel waarvoor ze zijn verzameld? Denk bijvoorbeeld aan gegevens voor de bijstand die vervolgens worden gebruikt voor kwijtschelding van belastingen. (vraag de privacy contactpersoon van jouw domein)

Niet van toepassing, we gebruiken de persoonsgegevens alleen voor dit proces.

10. Betrouwbaarheid, veiligheid & transparantie;

Beschrijf de randvoorwaarden zoals betrouwbaarheid, veiligheid, transparantie door de volgende vragen te beantwoorden. Beschrijf welke maatregel welk risico aanpakt. (vraag de security officer)

10.1 Welke technische/organisatorische/juridische (zoals beveiliging, wachtwoorden, een verwerkersovereenkomst) maatregelen zijn genomen om de betrouwbaarheid van de toepassing te borgen?

De volgende maatregelen zijn genomen: - 5.1.2i werkt met meerdere veiligheidsconstructies. Zij werken met o.a. beveiligde platformen, authenticatiecodes voor toegang tot de spraak assistent en zij encrypten alle data in transit. 5.1.2e heeft dit toegelicht in de verwerkersovereenkomst. - De techniek blijven we in ieder geval testen en evalueren gedurende deze eerste fase. - De beveiligingsmaatregelen van de applicatie 5.1.2i valt buiten de scope van deze DEPIA.
Advies FG: akkoord

10.2: Welke technische/organisatorische/juridische maatregelen zijn genomen om de veiligheid te borgen?

Zie 10.1
Advies FG: akkoord

10.3: Welke maatregelen zijn genomen om de transparantie van de toepassing te borgen?

- in de gespreksflow wordt benoemd dat dat wij de persoonsgegevens alleen gebruiken wanneer we vragen over de melding hebben. - we vullen de website aan met een toevoeging over de spraak assistent. Dit gaat z.s.m. geschreven en aangepast worden. https://www.leeuwarden.nl/privacy-en-avg/privacy/
Advies FG: akkoord

11. Afweging;

Afweging van alle onderdelen in het kader van ethiek, privacy en informatieveiligheid.

11.1: Kan hetzelfde doel op een andere manier worden bereikt (subsidiariteit)? Leg uit waarom wel/niet.

We hebben drie doelen vastgesteld. Onze bereikbaarheid verbeteren, onze dienstverlening inclusiever maken en het uitbreiden van de selfservice. Bereikbaarheid verbeteren kan op meerdere manieren worden bereikt. - Melding kan ook fysiek (balie) of via een medewerker S&I worden gemaakt. Inzet van meer FTE is dan een optie. - Uiteindelijke doel is om de algehele bereikbaarheid te verbeteren (niet alleen melding). Deze technologie kan worden ingezet op andere diensten/producten. Bijvoorbeeld het maken van een afspraak, inspreken van je verhuizing, etc. Dienstverlening inclusiever maken - Extra mogelijkheid voor een inwoner om een kanaal te kiezen wat bij hem/haar past op dat moment, en waar hij/zij zich prettig en veilig voelt (zelfregie). Uitbreiden van de selfservice: - Uitbreiding van een 24/7 bereikbare 5.1.2i, er moet wel transparantie komen dat de melding dan niet altijd gelijk opgepakt wordt omdat deze handmatig de volgende dag of na het weekend pas in het systeem ingevoerd wordt. Met de spraak assistent kan de gemeente bovenstaande doelen slimmer, makkelijker en sneller bereiken. Als de nieuwe werkwijze een succes is, kunnen we investeren in de mogelijkheid om de melding rechtstreeks in 5.1.2i te laten landen zodat de melding direct bekend is bij ons.
Advies FG: Duidelijk omschreven

11.2: Kan hetzelfde doel met minder gegevens worden bereikt (proportionaliteit)? Leg uit waarom wel/niet.

We kunnen de doelen, benoemd bij 11.1 niet behalen als we minder/geen persoonsgegevens vragen. Omdat de uitval (meldingen die niet compleet zijn) dan niet compleet gemaakt kunnen worden. Daarnaast komen we dan in het dilemma dat de inwoner verwacht dat hij een melding heeft gedaan, maar wij kunnen hem niet oppakken. En dus is de melding niet gedaan. Hiermee komt de klanttevredenheid in het geding.

De verwerking is gelijk met de melding via 5.1.2i op de website. Het enige verschil is dat de melder in 5.1.2i de locatie heel precies kan aangeven op een kaartje of met een adres. Ook hier geldt het risico bij een anonieme melding dat als de melding niet duidelijk omschreven is, hij niet opgepakt kan worden.

Ik verwacht dat er uitval gaat komen vanwege dialect, andere taal of spraakgebrek. Ook verwacht ik dat we deze grotendeels op kunnen vangen doordat de S&I medewerker het audiobestand gaat afluisteren en dan alsnog de melding in 5.1.2i kan invoeren. We hebben wel de afspraak dat we een half jaar intensief gaan monitoren en bijsturen. En daar is uitval een belangrijk onderdeel van.

Zoals eerder vermeld, wanneer de melder doorverbonden wordt naar de spraak assistent, is alles met spraak. Telefoonnummer wordt niet ingevoerd maar ingesproken.

De keuze in de persoonsgegevens is afgestemd met het proces van 5.1.2i via de website.

Advies FG: akkoord

11.3: Wat zijn de negatieve gevolgen en de genomen maatregelen voor de betrokkenen

Beschrijf en beoordeel risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Noem ook de risico's voor de waarden vanuit vraag 3.1.

Negatieve gevolgen	Oorzaak hiervan	Kans op gevolgen	Impact van gevolgen	Maatregel	Geïmplementeerd door
Melding kan niet worden opgepakt door Gemeente Leeuwarden	Dialecten, onduidelijk ingesproken, stotteren; vertaling door spraak assistent	Matig	Matig	>mdw S&I kan audiobestand afluisteren om melding alsnog compleet te krijgen	Werkproces administratieve groep S&I
Melding kan niet worden opgepakt, melding niet compleet	Mailadres is niet goed te verstaan of niet goed vertaald	Matig	Matig	>na livegang gaan we 3 weken lang 'handmatig' elke melding controleren wanneer er een mailadres vertaald is >bij uitval 2 oplossingen mogelijk: tekstflow aanpassen; melder mailadres laten spellen*	Projectgroep * 5.1.2i
Melding kan niet worden niet opgepakt, melding niet compleet	Anonieme meldingen	Matig	Matig	>inwoner wordt hierop in de gespreksflow attent gemaakt	5.1.2i
Melder neemt geen contact op	Melding niet compleet	Matig	Matig	>er wordt een herinneringsbericht (dag 3) en een afsluitende mail/bericht (dag 7) verstuurd naar inwoner, door mdw S&I	Werkproces administratieve groep S&I
Datalek	Bericht naar foutief mailadres gestuurd door mdw S&I door verkeerde vertaling spraak assistent	Matig	Matig	>Mail/voicemail bericht dat door mdw S&I verstuurd/ingesproken wordt om missende informatie op te halen, bevat geen gevoelige informatie.	Werkproces administratieve groep S&I
Datalek	Bericht naar foutief mailadres gestuurd door typefout mdw S&I	Laag	Laag	>mdw S&I maakt gebruik van copy paste techniek vanuit het mailsjabloon	Werkproces administratieve groep S&I
Mailbox mapje OPGEPAKT loopt vol, waardoor er gegevens in de mailbox blijven staan wat niet nodig is.	Automatisch wissen staat niet goed ingesteld	Laag	Laag	>eerste week controleert mdw S&I begin van de werkdag of mapje leeg is	5.1.2e (Information en records officer)
Inwoner wordt gebeld (lastig gevallen) voor meer informatie over de melding	Melding is niet goed vertaald in het sjabloon	Matig	Matig	>er wordt een audiobestand bijgevoegd, waarmee de mdw het	5.1.2i

				hele gesprek kan naluisteren en aanvullingen kan doen	
*als uit de evaluatie blijkt dat deze maatregel niet dekkend is, heeft onze leverancier nog 2 oplossingen: *Inzetten van een large language modellen zoals ChatGPT om teksten te corrigeren / Je kunt de inwoner zijn e-mailadres 2x laten inspreken. Je ziet vaker bij diensten waar een email adres voor nodig is dat je het 2x moet opgeven. Daarmee controleer je of het eerste email adres dat de gebruiker/inwoner opgeeft correct is.*					
Advies FG: akkoord					

11.4: Zijn er rest-risico's en zo ja, welke? Leg ook uit waarom.

Alle risico's in 11.3 vermeld. Uit de evaluatie na livegang moet blijken of er nog meer risico's zijn. Als er tijdens de evaluatieperiode nog rest risico's bijkomen, wordt de DEPIA aangepast.
Advies FG: Akkoord

11.5: Zijn er (verwerkers)overeenkomsten gemaakt met betrokken externe partijen? Zo ja, voeg deze dan toe als bijlage (en sla deze op in het zaaksysteem en in 5.1.2i onder het contract met de leverancier)

Verwerkersovereenkomst gaan we nog invullen en vooraf voor advies voorleggen via 5.1.2i.

Eindoordeel Functionaris voor Gegevensbescherming: De risico's zijn goed in beeld gebracht en voorzien van mitigerende maatregelen. **Datum: 12-4-2024**

Beoordeling (door management/bestuur)	**Is de beoordeling openbaar of vertrouwelijk**
5.1.2e 5.1.2e 5.1.2e	vertrouwelijk

Waar wordt de beoordeling opgeslagen (5.1.2i zaaknummer toevoegen)
2024-099354

Startdatum verwerkingen (indien van toepassing)	**Wanneer bijwerken register (indien van toepassing)**	**Datum herziening DEPIA (indien van toepassing)**

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 8, 10, 11, 13, 15
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2, 3, 4, 5, 8, 9, 11, 12, 13, 15

DEPIA

Rapport Data Protection Impact Assessment en Algoritme & Mensenrechten Assessment (DPIAMA)

Transcribeertool Sociaal Domein – Gemeente Leeuwarden.

Verwerkingsverantwoordelijke:	<College van B&W / Burgemeester / Raad>
Sector/Afdeling/Team:	<naam sector, afdeling en team>
Pre-DEPIA uitgevoerd:	<'Ja' + datum of 'Nee' plus eventueel toelichting>
Datum DEPIA:	<datum waarop proceseigenaar akkoord is met DEPIA>
Zaaknummer:	<zaaknummer 5.1.2i>

Algemeen

Het verwerken van persoonsgegevens kan een hoog privacyrisico opleveren voor de betrokken personen. Is dit het geval? Dan is het verplicht vooraf de risico's te onderzoeken. En maatregelen in kaart te brengen die deze risico's wegnemen of verkleinen. In Leeuwarden onderzoeken we niet alleen de privacyrisico's maar ook de ethische dilemma's van gegevensverwerkingen. Dit noemen we een DEPIA: Data en Data-ethische Protection Impact Assessment.

Zijn er na het uitvoeren van de DEPIA belangrijke restrisico's? En kunnen we deze niet beperken? Dan moeten we de gegevensverwerking eerst voorleggen aan de Autoriteit Persoonsgegevens (AP). Dit is een voorafgaande raadpleging. Verder voeren we iedere drie jaar een herbeoordeling van de DEPIA uit. Dit doen we ook bij ingrijpende wijzigingen van een bestaande gegevensverwerking.

1 Inleiding, Doelstelling, Aanpak en Scope

Deze rapportage beschrijft de DEPIA van de pilot van de inzet van een transcribeertool binnen Team Werk van het sociaal domein en binnen vergaderingen van informatieadviseurs.

Een DEPIA is een middel om in kaart te brengen welke persoonsgegevens in een proces, systeem of organisatie verwerkt worden en wat de risico's van deze verwerking zijn en kan ook gebruikt worden als middel om in kaart te brengen wat de risico's zijn van het in te zetten AI-middel op fundamentele mensenrechten. Op 17 december 2025, is een sessie gehouden om informatie op te halen over de voorgenomen inzet van de transcribeertool.

Doelstelling

Het doel van deze DEPIA is om inzicht te verkrijgen in de verwerking van persoonsgegevens binnen de inzet van de transcribeertool binnen de pilot, aangezien deze tool tijdens de pilot persoonsgegevens zal verwerken en de daarbij horende privacy risico's en mitigerende maatregelen. De DEPIA richt zich op het beoordelen van de geplande en/of geïmplementeerde maatregelen, waarborgen en mechanismen om de risico's te beperken, de persoonsgegevens te beschermen en aan te tonen dat aan de beginselen voor verwerking uit de AVG is voldaan. Deze DEPIA is een momentopname. Bij nieuwe ontwikkelingen zoals wijzigingen in wetgeving, verandering van processen, inzet van nieuwe functionaliteiten/technologieën, wijziging van het doel van de verwerking, de verwerking van nieuwe of categorieën persoonsgegevens of wanneer het risico verandert moet de DEPIA worden herijkt. Daarnaast vindt periodieke herbeoordeling plaats zolang er sprake blijft van een hoog risico.

1.1 Wie zijn betrokken bij de DEPIA?

Geef aan wie betrokken zijn bij het uitvoeren van de DEPIA. Vul aan waar nodig.

Proceseigenaar (teamleider werk)	5.1.2e
Veranderkundige/Contactpersoon DEPIA	5.1.2e
Informatiemanager	5.1.2e
Informatieadviseur	5.1.2e
Privacy Officer (PO)	5.1.2e
Data-ethiek Officer (DO)	5.1.2e
Recordmanagement	5.1.2e [1]
Information Security Officer (ISO)	5.1.2e

[1] Niet aanwezig bij de DEPIA-sessie; wel schriftelijk betrokken

Functionaris Gegevensbescherming (FG)	5.1.2e [2]
Informatieadviseur/ Adviseur Leren ontwikkelen Digitale Leerlijn	5.1.2e
Senior Data Scientist	5.1.2e
Data Scientist	5.1.2e
Senior Team Werk	5.1.2e
Consulent Team Werk	5.1.2e
5.1.2i Co Founder	5.1.2e

Voor deze risicoanalyse is een zorgvuldig multidisciplinair proces doorlopen. In dit kader heeft een uitgebreide werksessie plaatsgevonden waarin de voorgestelde inzet van de transcribeertool is besproken en beoordeeld vanuit verschillende gezichtspunten. Aan deze sessie namen vertegenwoordigers deel vanuit verschillende invalshoeken (zie hierboven). Deze samenstelling waarborgde dat niet alleen juridische en beveiligingsaspecten werden meegenomen, maar ook de praktische impact op het primaire proces, de technische haalbaarheid, mogelijke ethische implicaties en de gebruikerservaring van consulenten en klanten.

1.2 Wat ga je doen?

Hoe ziet het project/proces eruit, wat zijn de stappen of fasen, de applicatie(s), hoe ga je de persoonsgegevens gebruiken en zijn er acties zonder tussenkomst of beoordeling van een medewerker? Maak bij voorkeur ook een plaatje of schematische weergave van het proces.

Scope

De scope van deze DEPIA wordt bepaald door een pilot waarin de inzet van een transcribeertool wordt getest. Voor de pilot wordt gebruik wordt gemaakt van de software van 5.1.2i die wordt ingezet binnen de context van het sociaal domein van Gemeente Leeuwarden en bij vergaderingen door informatiemanagers en binnen het team RPA. De pilot richt zich op de verwerking van intakegesprekken (1-op-1) gesprekken tussen consulenten voor arbeidsparticipatie van Team Werk en haar klanten, dit zijn inwoners in de bijstand of met een uitkering, via audio-opnames die vervolgens automatisch worden omgezet in transcripten en rapportages. De pilot richt zich daarnaast ook op het transcriberen van gesprekken met collega's onderling in team- of werkoverleggen waarin acties worden vastgesteld waarbij mogelijk de verwerking van gevoelige persoonsgegevens plaatsvindt maar meestal niet[3].

[2] Niet aanwezig bij de DEPIA-sessie; wel schriftelijk betrokken

[3] Beide toepassingen van de transcribeertool zijn binnen één DEPIA beoordeeld. Het interne gebruik tijdens werk- en teamoverleggen is minder vergaand dan het gebruik in klantgesprekken binnen de sociale hulpverlening. Intern gebruik vindt plaats in een professionele context en betreft medewerkers die meestal niet in een afhankelijke of kwetsbare positie verkeren. Daarbij worden doorgaans geen of slechts incidenteel bijzondere persoonsgegevens verwerkt. Eventuele onjuistheden in transcripties hebben geen directe gevolgen voor rechten, voorzieningen of de rechtspositie van individuele betrokkenen omdat de tool slechts wordt ingezet voor zakelijke acties en afspraken.

De inzet in de sociale hulpverlening is daarentegen privacy-ingrijpender, omdat structureel gevoelige en bijzondere persoonsgegevens van burgers worden verwerkt. Daarnaast is er sprake van een afhankelijkheidsrelatie tussen klant en overheid, waarbij vastgelegde informatie kan doorwerken in besluitvorming over uitkeringen of ondersteuning. Fouten of misinterpretaties kunnen hierdoor aanzienlijke gevolgen hebben voor de betrokkene. Daarom is in deze DEPIA uitgegaan van het scenario met het

In deze DEPIA wordt specifiek gekeken naar:

- Het opnemen, transcriberen, deïdentificeren en rapporteren van gesprekken met klanten
- De opslag en verwerking van deze gegevens binnen de 5.1.2i -omgeving
- De interactie tussen consulent, klant en systeem tijdens het rapportageproces
- De juridische, technische en organisatorische waarborgen rondom deze verwerking

Na afloop van de pilot wordt, op basis van evaluatie, besloten of de inzet van 5.1.2i standaard wordt ingezet tijdens gesprekken tussen consulenten en klanten en of de inzet van de transcribeertool van 5.1.2i wordt uitgebreid naar andere teams of klantgroepen. Deze DEPIA kan dan worden bijgewerkt voor de uiteindelijke inzet.

Expliciet buiten scope van deze DEPIA vallen:

- Eventuele verdere verwerking van de rapportages nadat ze in het zaaksysteem van het sociaal domein (5.1.2i) staan opgeslagen
- Andere vormen van automatische transcriptie of rapportage buiten 5.1.2i om

Systematische beschrijving van de verwerking

Het proces van rapporteren met gebruik van de transcribeertool van 5.1.2i ondersteunt consulenten bij het vastleggen van klantcontacten. In plaats van handmatig tijdens of na een gesprek aantekeningen te maken, kunnen zij tijdens het gesprek een opname starten die automatisch wordt omgezet in een transcriptie en vervolgens in een rapport. Deze werkwijze is onder andere bedoeld om de administratieve lasten te verlagen, de verslaglegging te verbeteren en de kwaliteit van hulpverlening te ondersteunen. Hier zal later in het rapport nader op worden ingegaan. Onderstaande beschrijving geeft inzicht in de verwerkingsstappen, de verwerkte persoonsgegevens en de gebruikte middelen. Voor intern gebruik bij vergaderingen werkt de tool op dezelfde manier en dit is daarom niet apart beschreven.

1. **Start audio opname**

De consulent logt in op de 5.1.2i -gebruikersinterface op de laptop of telefoon via de browser. Vervolgens moet een inwoner id worden ingevuld om de opname te starten. Dan kan de consulent de opname starten. Indien nodig kan de opname tijdelijk gepauzeerd worden om delen van het gesprek ‘off the record’ te houden. Informatie die buiten de opname valt, wordt niet verwerkt in het systeem.

2. **5.1.2i to tekst**

De opgenomen audio wordt in realtime verzonden naar de 5.1.2i Transcriber, waar de spraak wordt omgezet naar tekst. Deze verwerking gebeurt in gedeelten van ongeveer 30 – 60 seconden. Zodra een audiodeel is verwerkt, wordt het direct verwijderd uit het geheugen. De verwerking vindt uitsluitend in memory plaats.

5.1.2i maakt gebruik van diverse transcriptiemodellen, waaronder een eigen LLM en de 5.1.2i 5.1.2i 5.1.2i. Deze technologieën analyseren de audio, maken onderscheid tussen sprekers op basis van context, en beogen rekening te houden met accenten en dialecten en voegen timestamps toe. Het resultaat is een tekstuele transcriptie van wat tijdens het gesprek is gezegd.

hoogste risiconiveau, zodat de getroffen maatregelen toereikend zijn voor de meest privacygevoelige toepassing en tevens passend blijven voor minder risicovolle interne inzet.

De gebruiker krijg een samenvatting te zien tijdens de opname, ongeveer elke 30 tot 60 seconden, afhankelijk van de hoeveelheid gegenereerde transcript.

3. **Deïdentificatie**

Na transcriptie wordt elk tekstfragment direct gedeïdentificeerd via de 5.1.2i 5.1.2i. Hierbij worden persoonsgegevens zoals namen, leeftijden, adressen en e-mailadressen automatisch gemaskeerd. Het transcript bevat geen vaste sprekerslabels of roltoewijzingen. Het originele, niet-gedeïdentificeerde transcript wordt daarna direct verwijderd uit het systeem. Het gedeidentificeerde transcript wordt opgeslagen in de transcriptie database van 5.1.2i. De gebruiker krijg een gedeïdentificeerde samenvatting te zien tijdens de opname, ongeveer elke 30 tot 60 seconden.

4. **Rapport generatie**

Op basis van het gedeïdentificeerde transcript wordt een rapport gegenereerd door op de rapporteer knop in de applicatie te klikken. Voor het genereren van deze rapportage wordt gebruikgemaakt van een groter GPT-taalmodel dan het model dat wordt ingezet voor transcriptie en samenvatting.[4] De consulent kan ervoor kiezen om losse onderdelen of het volledige rapport in huisstijl van Gemeente Leeuwarden automatisch te laten opstellen. De rapportage wordt opgeslagen als 'initieel rapport' in de rapportagedatabase van 5.1.2i. Het rapport kan daarna worden bekeken en aangepast.

5. **Rapport aanpassing**

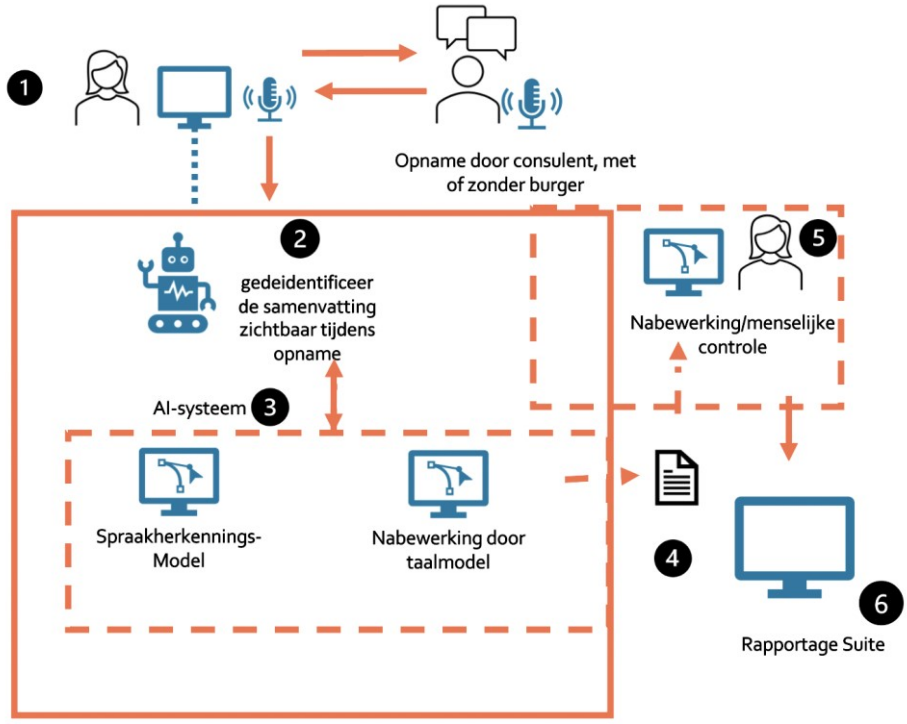
De consulent kan het initiële rapport aanpassen via de gebruikersinterface. 5.1.2i biedt hiervoor een AI-assistent aan waarmee zowel gesproken als getypte instructies kunnen worden gegeven. Voorbeelden daarvan zijn inkorten van onderdelen, samenvatten, herschrijven etc. Voor deze functionaliteiten worden door 5.1.2i ingezette taalmodellen gebruikt. Na bewerking wordt het aangepaste rapport opgeslagen als 'aangepast rapport' in de Rapport database. Het gegenereerde rapport wordt door consulent samen met de klant nagelopen.

6. **Rapport exporteren**

Als de consulent alle gewenste aanpassingen heeft kunnen maken in het rapport, klikt hij op de exporteer knop in de 5.1.2i UI. Dit leidt tot het definitieve rapport, dat als "Definitief rapport" wordt opgeslagen in de Rapport database van 5.1.2i. Het 5.1.2i rapport kan vanuit 5.1.2i met een druk op de knop volledig of per sectie worden gekopieerd en door de consulent geplakt in het dossier van de klant in 5.1.2i.[5]

[4] Dit onderscheid hangt samen met de aard van de functionaliteit. Waar transcriptie en samenvatting gericht zijn op het omzetten en beknopt weergeven van gesproken tekst, vereist het genereren van een rapport dat grotere tekstgedeelten in samenhang worden verwerkt en gestructureerd volgens een vast rapportformat. Hiervoor wordt een taalmodel ingezet dat geschikt is voor het verwerken van meer context en complexere instructies.

[5] Tijdens de pilot ligt de nadruk op het aantonen van de werking van de tool en is nog geen API-koppeling gerealiseerd. Mocht de tool in gebruik genomen worden is dit wel een mogelijkheid.



Beschrijving van de pilot

Binnen Team Werk vindt een intakegesprek tussen de consulent en de klant plaats in een persoonlijk gesprek. Tijdens dit gesprek verzamelt de consulent informatie over de persoonlijke situatie van de klant, zoals de hulpvraag, achtergrond en relevante omstandigheden voor begeleiding naar werk of ondersteuning. De consulent maakte tijdens of direct na het gesprek handmatig aantekeningen, op basis van wat in het gesprek werd besproken. Deze aantekeningen dienden als hulpmiddel voor het vastleggen van afspraken en acties na het gesprek. De manier waarop werd geregistreerd was tot nu afhankelijk van de individuele werkwijze en interpretatie van de consulent. De notities dienen als basis voor als basis voor een plan van aanpak dat de consulent opstelt en met de klant deelt. Dit document vormt de basis voor de verdere begeleiding en vastlegging in het dossier van de klant.

De pilot sluit aan op de hiervoor beschreven werkwijze. Waar de consulent voorheen handmatig aantekening maakt, ondersteunt de transcribeertool tijdens de pilot bij het vastleggen van het gesprek. In de nieuwe werkwijze wordt het eenduidig en gestructureerd vastleggen van samenvatting, acties en afspraken uit het gesprek ondersteund door een automatisch gegenereerd rapport op basis van het format van het rapport dat Gemeente Leeuwarden aanlevert bij 5.1.2i.

Tijdens de pilot wordt de tool ook ingezet in werkoverleggen van informatiemanagement. Dit zijn overleggen waarin in principe geen klanten worden besproken maar bedrijfsvoering gerelateerde informatie. Notulen

die normaalgesproken handmatig werden gemaakt worden tijdens de pilot middels de opname en het transcript gemaakt.

De pilot heeft een looptijd van 8 maanden. Na afloop van de pilot vindt een evaluatie plaats met Team Werk. De beoordeling is kwalitatief van aard: samen met de consulenten wordt gereflecteerd op de doelen van het project, zoals efficiëntie, werkplezier, kwaliteit van rapportage en klant betrokkenheid. Daarnaast staat gebruiksgemak, gebruikerstevredenheid en klant acceptatie centraal. Er wordt besproken in hoeverre deze doelen als bereikt worden ervaren, zonder dat daarbij met harde data wordt gewerkt.

De pilot bevat daarnaast een aantal actieve feedbackloops (zie ook Juistheid). Bij technische of inhoudelijke problemen, zoals herkenningsfouten bij bepaalde accenten (bijvoorbeeld het Friese dialect of gebrekkig Nederlands van statushouders), wordt dit gemeld aan 5.1.2i. Er volgt dan gezamenlijk een analyse en zo nodig bijstelling van het systeem.

1.3 Wat wil je bereiken? (wat is het doel)

Wat is het doel dat je wil bereiken met het project/proces? Dit kunnen uiteraard ook meerdere doelen zijn.

De gemeente voert de pilot met de transcribeertool uit ter ondersteuning van consulenten in het sociaal domein bij het vastleggen van gesprekken met klanten. Deze gesprekken hebben als doel om samen met de klant een plan van aanpak te bepalen en afspraken te maken over de benodigde ondersteuning. De verslaglegging van deze gesprekken vormt input voor het klantdossier en wordt gebruikt om afspraken, besluiten en samenvattingen zorgvuldig vast te leggen.
Vastlegging van informatie uit gesprekken is een essentieel onderdeel van professionele hulpverlening. Door relevante informatie over het klantcontact vast te leggen in het dossier wordt beoogd dat:

- de continuïteit en samenhang in de hulpverlening worden ondersteund, zodat consulenten beter kunnen bepalen welke ondersteuning passend is
- andere betrokken consulenten inzicht hebben in de situatie, voortgang en gemaakte afspraken, zodat zij de ondersteuning kunnen voortzetten
- de klant zelf inzicht krijgt in de geboden ondersteuning en de gemaakte keuzes
- wordt voldaan aan wettelijke verplichtingen ten aanzien van dossiervoering, zoals voortvloeiend uit de Algemene wet bestuursrecht en impliciet uit de Participatiewet.

De pilot heeft nadrukkelijk niet tot doel om deze doelen te wijzigen. De inzet van de transcribeertool verandert niets aan het doel van vastlegging, maar onderzoekt of de wijze van vastleggen van gesprekken kan worden ondersteund door spraakgestuurde technologie.

Doelstelling van de pilot
Het doel van de pilot is om te verkennen of het gebruik van een transcribeertool consulenten kan ondersteunen bij het efficiënter, consistenter en zorgvuldiger vastleggen van gespreksverslagen, zonder afbreuk te doen aan de kwaliteit van de hulpverlening of de positie van de klant. Daarbij wordt onderzocht of de tool bijdraagt aan:

- vermindering van administratieve belasting verhoging van werkplezier voor consulenten
- meer aandacht en ruimte voor het gesprek met de klant
- consistente en beter navolgbare rapportages in het klantdossier
- meer transparantie richting de klant over vastgelegde afspraken en overwegingen
- verhoogde informatieveiligheid omdat niet meer in losse notitieboekjes wordt genotuleerd

Daarnaast wordt de tool in de pilotfase verkend voor gebruik bij interne teamoverleggen, zoals vergaderingen van informatiemanagers. Het doel hiervan is om te onderzoeken of spraakgestuurde verslaglegging ook in deze context kan bijdragen aan efficiëntere vergaderingen, waarin meer ruimte ontstaat voor luisteren en inhoudelijke uitwisseling en minder voor handmatige notulering.

De pilot staat in het teken van het uitgangspunt: *“meer luisteren en minder typen”*, waarbij wordt onderzocht of technologie kan bijdragen aan een zorgvuldiger en mensgerichter gesprek, met behoud van

privacy en gegevensbescherming. Het is op voorhand niet vastgesteld of deze beoogde effecten daadwerkelijk worden bereikt. De pilotfase is bedoeld om ervaring op te doen met de tool en om te beoordelen of en onder welke voorwaarden de inzet ervan wenselijk is.

1.3.1 Ga je de persoonsgegevens ook voor een ander doel gebruiken?

Als je persoonsgegevens ook nog voor een ander doel dan dit project/proces gaat gebruiken, is dat een 'verdere verwerking'. Dit mag als je uitdrukkelijke toestemming hebt van de betrokkenen, de verdere verwerking in een wet staat of als het doel verenigbaar is met het doel waarvoor je de gegevens gaat gebruiken. Voorbeelden zijn gegevens voor de bijstand gebruiken voor kwijtschelding van belastingen of het samenstellen van managementinformatie.

De door de transcribeertool gegenereerde rapportages worden, net als de handmatige notities en notulen nu, gebruikt als ondersteuning bij het opstellen van een plan van aanpak door de consulent of om acties en afspraken vast te leggen. De transcribeertool ondersteunt uitsluitend het rapportageproces en neemt geen beslissingen over klanten. De inzet van de tool heeft geen gevolgen voor de inhoudelijke beoordeling van hulpvragen of de besluitvorming over ondersteuning. De consulent of medewerker van de gemeente blijft verantwoordelijk voor de inhoud van de vastgelegde rapportage of notulen en de consulent bepaalt welke informatie wordt opgenomen in het klantdossier. Daarnaast worden gegevens binnen de pilot in beperkte mate gebruikt voor:

- het evalueren van de werking en bruikbaarheid van de transcribeertool
- het verkrijgen van inzicht in de mogelijke bijdrage van de tool aan kwaliteitsverbetering van rapportages

Deze evaluatie heeft uitsluitend betrekking op het functioneren van de tool en het werkproces van consulenten en is niet gericht op beoordeling of profilering van klanten. Binnen de pilot is afgesproken dat gedeïdentificeerde transcripten incidenteel worden ingezet voor verbetering van het rapportagemodel. Wanneer een gebruiker of team een fout signaleert in de gegenereerde rapportage, wordt dit samen met 5.1.2i geanalyseerd. Op basis van deze feedback past 5.1.2i het onderliggende model aan, bijvoorbeeld door betere contextparameters mee te geven of domeinspecifieke taaluitingen toe te voegen. Vervolgens wordt met behulp van het oorspronkelijke transcript getest of het aangepaste model de fout corrigeert en tot een betere rapportage leidt.

Er wordt geen data gebruikt voor training van modellen of commerciële doeleinden.

1.3.2 Kan je het doel ook op een andere manier bereiken?

Een belangrijk begrip bij het beoordelen van de noodzaak is 'subsidiariteit'. Dit betekent dat je afweegt of het verwerken van persoonsgegevens nodig is en nagaat of je het doel ook op een andere manier (dus zonder persoonsgegevens) kan bereiken. En dat je deze afweging kan uitleggen.

Binnen het sociaal domein en bij interne teamoverleggen is handmatige verslaglegging de gebruikelijke en reeds beschikbare werkwijze. Deze werkwijze blijft gedurende de pilot onverminderd beschikbaar, niet alle teams zullen de transcribeertool testen. De inzet van de transcribeertool wordt in de pilotfase verkend als ondersteunend middel.

Met de pilot wordt onderzocht of spraakgestuurde verslaglegging kan bijdragen aan een efficiëntere en consistentere manier van vastleggen van gesprekken en overleggen, met behoud van menselijke regie en inhoudelijke verantwoordelijkheid, en daarbij aan de kwaliteit van de rapportages. Minder ingrijpende alternatieven, zoals het blijven werken met handmatige notities, worden niet uitgesloten maar juist als referentie gebruikt om de meerwaarde en effecten van de tool te kunnen beoordelen.

Gelet op de beperkte en ondersteunende inzet van de transcribeertool, het ontbreken van geautomatiseerde besluitvorming en de blijvende rol van de consulent bij het vaststellen van de inhoud van rapportages, wordt de gekozen aanpak in deze pilot als subsidiair beschouwd.

1.4 Wat is het juridisch en beleidskader?

1.4.1 Welke wetten, voorschriften, beleid en/of richtlijnen zijn van toepassing?

Geeft hier een opsomming van alle relevante wet- en regelgeving, beleid en richtlijnen van de gemeente.

Europees recht

- **Algemene Verordening Gegevensbescherming (AVG)**
  Regelt de voorwaarden waaronder persoonsgegevens mogen worden verwerkt, waaronder de vereisten van rechtmatigheid, doelbinding, dataminimalisatie, transparantie en de rechten van betrokkenen.
- **Handvest van de grondrechten van de Europese Unie**
  In het bijzonder artikel 7 (eerbiediging van het privéleven) en artikel 8 (bescherming van persoonsgegevens).

Nationaal recht – sociaal domein

- **Participatiewet**
  Vormt het primaire wettelijke kader voor de werkzaamheden van Team Werk. Op grond van deze wet is het College verantwoordelijk voor ondersteuning bij arbeidsinschakeling, begeleiding en besluitvorming over bijstand en voorzieningen (onder meer artikelen 7, 9 en 44a)

Nationaal recht – algemeen bestuursrecht

- **Algemene wet bestuursrecht (Awb)**
  Met name artikel 3:2 (zorgvuldige voorbereiding) en artikel 3:46 (deugdelijke motivering), die eisen stellen aan de voorbereiding en onderbouwing van besluiten.
- **Gemeentewet**
  Regelt de bevoegdheden en organisatie van het gemeentebestuur. Op grond van artikelen 160 en 171 is het College belast met het bestuur en de organisatie van de gemeentelijke taken.
- **Archiefwet 1995**
  Verplicht de gemeente tot het zorgvuldig vastleggen, bewaren en vernietigen van archiefbescheiden die voortvloeien uit de uitvoering van haar taken.

Gemeentelijk beleid en interne richtlijnen

- Intern privacybeleid en informatiebeveiligingsbeleid van de gemeente;
- Interne werkprocessen en werkinstructies van Team Werk;
- Afspraken met verwerkers en subverwerkers (verwerkersovereenkomsten).

1.4.2 Wat is de grondslag vanuit AVG of Wpg?

De AVG kent zes grondslagen: 1) wettelijke verplichting, 2) algemeen belang/openbaar gezag, 3) overeenkomst, 4) toestemming, 5) gerechtvaardigd belang en 6) vitaal belang.
Wettelijke verplichting en algemeen belang/openbaar gezag komen het meest voor; deze staan altijd in een wet. Overeenkomst sluit je met een persoon af, bijv. een arbeidsovereenkomst. Toestemming kan alleen onder strikte voorwaarden, gerechtvaardigd belang alleen voor bedrijfsvoeringstaken van de gemeente. Vitaal belang gebruik je alleen in levensbedreigende situaties. Verwerk je (ook) gegevens op grond van de Wet politiegegevens (Wpg)? De twee meest voorkomende grondslagen zijn dan algemene opsporing (art. 8) of gericht onderzoek (art. 9).

De verwerking van persoonsgegevens van klanten door Team Werk vindt plaats op basis van artikel 6 lid 1 onder c en onder e AVG, afhankelijk van het doel en de context van de verwerking.

Voor intakegesprekken binnen Team Werk vindt de verwerking van persoonsgegevens plaats op basis van artikel 6 lid 1 onder e van de AVG omdat deze verwerking noodzakelijk is voor de vervulling van taken van algemeen belang en de uitoefening van openbaar gezag. Deze taken zijn opgedragen aan het College op grond van de Participatiewet, in het bijzonder artikel 7 waarin het College verantwoordelijk is voor ondersteuning bij arbeidsinschakeling en het aanbieden van voorzieningen. Intakegesprekken zijn noodzakelijk om de persoonlijke situatie van de betrokkene vast te stellen en te beoordelen welke ondersteuningen passend zijn.

Daarnaast sluiten intakegesprekken aan bij artikel 9 van de Participatiewet, waarin de verplichtingen van bijstandsgerechtigden zijn vastgelegd, en artikel 44a van de Participatiewet, dat ziet op de aanvraag en voorbereiden van besluiten over bijstand en bevat de verplichting van de Gemeente om klant te voorzien van een plan van aanpak.

Voor zover bij intakegesprekken incidenteel bijzondere persoonsgegevens worden verwerkt, zoals gegevens over gezondheid of beperkingen, vindt deze verwerking aanvullend plaats op basis van artikel 9 lid 2 onder b van de AVG, omdat deze noodzakelijk kan zijn voor de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van het socialezekerheids- en socialebeschermingsrecht, zoals vastgelegd in artikel 7, artikel 9, artikel 17 en artikel 44a van de Participatiewet. Deze verwerking is beperkt tot het strikt noodzakelijke en vindt plaats met passende waarborgen.

De verwerking van persoonsgegevens in het kader van interne werkoverleggen en interne dossiervorming over de bedrijfsvoering door Team Werk vindt eveneens plaats op basis van artikel 6 lid 1 onder e AVG, voor zover dit noodzakelijk is voor interne organisatie en coördinatie van gemeentelijke werkzaamheden. Deze verwerking vindt haar basis in de Gemeentewet (Artikelen 160 en 171), waarin het College is belast met het bestuur en de organisatie van de gemeentelijke taken.

1.5 Wie zijn de betrokkenen en hoe ga je ze informeren?

We moeten transparant zijn over het verwerken van persoonsgegevens. Het is dus belangrijk dat je weet wie de betrokkenen zijn en dat zij weten dat wij gegevens verzamelen en gebruiken. Voorbeelden van betrokkenen zijn: inwoners, klanten, aanvragers, kinderen, bezoekers en medewerkers. Voorbeelden van het informeren van betrokkenen zijn: informatie op de website, een folder, bijlage bij of informatie in een brief, een privacyverklaring, etc.

De categorieën van betrokkenen zijn klanten (inwoners van de gemeente Leeuwarden met een afstand tot de arbeidsmarkt die een uitkering krijgen) en medewerkers. Ook kunnen er gegevens worden verwerkt over personen uit het netwerk van de klant.

Bij de inzet van de transcribeertool is het belangrijk dat klanten vooraf geïnformeerd worden over het gebruik van deze technologie op een begrijpelijke wijze. Er is nog niet besloten hoe de klant geïnformeerd wordt over de verwerking en de inzet van de technologie. Zie voor een aanbeveling hierover, hoofdstuk 3 en 4. Binnen het interne gebruik van de transcribeertool zijn de betrokkenen uitsluitend medewerkers of zakelijke contactpersonen van de gemeente die deelnemen aan team- of werkoverleggen waarin de transcribeertool wordt ingezet. Er is nog niet besloten hoe zij geïnformeerd worden over de verwerking. Mogelijk is er een aanpassing van het privacy statement voor medewerkers nodig bij ingebruikname van de tool buiten de pilot.

Transparantie in het proces zelf

De werkwijze met spraakgestuurde rapportagesoftware draagt niet alleen bij aan administratieve verlichting, maar versterkt juist ook de transparantie richting klanten in de praktijk. Omdat het verslag direct na afloop van het gesprek beschikbaar is, kunnen klant en consulent het samen inzien en bespreken. Indien nodig kunnen direct aanpassingen worden gedaan, bijvoorbeeld wanneer iets verkeerd is geïnterpreteerd of onvolledig is weergegeven. Hierdoor heeft de klant niet alleen inzage in de verslaglegging, maar ook directe invloed op de inhoud ervan.

Rechten van betrokkenen

Gemeente Leeuwarden beschikt over een regulier proces voor het behandelen van verzoeken van betrokkenen op basis van de AVG, zoals inzage, correctie, verwijdering en het intrekken van toestemming. Deze rechten blijven volledig van kracht bij de inzet van spraakgestuurde rapportage.

2 Persoonsgegevens

2.1 Welke persoonsgegevens ga je verwerken?

Zet in de tabel over wie je persoonsgegevens gaat verwerken (betrokkenen) en welke persoonsgegevens dit zijn. Voorbeelden van betrokkenen zijn: inwoners, klanten, aanvragers, kinderen, bezoekers en medewerkers. Voorbeelden van persoonsgegevens zijn: naam, adres, woonplaats, telefoonnummer, BSN, e-mailadres, geboortedatum en -plaats, leeftijd, geslacht, nationaliteit, IP-adres, kenteken, inkomen, bankrekeningnummer en -saldo, lidmaatschap vakbond, politieke opvattingen, seksuele voorkeur, gegevens over gezondheid, strafrechtelijke gegevens, een stem, etc.

Persoonsgegevens in het proces

Tijdens het proces wordt een breed scala aan (ongestructureerde) persoonsgegevens verwerkt. De inhoud hangt af van wat er tijdens het gesprek wordt besproken. Het kan gaan om:

- **Algemene persoonsgegevens** zoals naam, geboortedatum, en contactgegevens (De stem van de betrokkene kwalificeert als een persoonsgegeven in de zin van artikel 4 AVG. De stem wordt niet verwerkt met het doel personen te identificeren en vormt daarom geen biometrisch gegeven in de zin van artikel 9 AVG. Afhankelijk van de inhoud van het gesprek kan de transcriptie wel bijzondere of strafrechtelijke persoonsgegevens bevatten.)
- **Strafrechtelijke persoonsgegevens** zoals het door de betrokkene zelf benoemen van strafbare feiten uit het verleden of het noemen van beperkingen bij arbeidsinschakeling die samenhangen met eerdere justitiële betrokkenheid. Deze informatie wordt niet actief uitgevraagd en kan uitsluitend incidenteel aan de orde komen wanneer de klant hier zelf melding van maakt tijdens het gesprek
- **Bijzondere persoonsgegevens** zoals gezondheidsgegevens of religieuze of levensbeschouwelijke overtuigingen, bijvoorbeeld wanneer deze samenhangen met beperkingen of aandachtspunten bij arbeidsinschakeling. Deze informatie wordt niet actief uitgevraagd en kan uitsluitend incidenteel aan de orde komen wanneer de klant hier zelf melding van maakt tijdens het gesprek.
- **Gevoelige persoonsgegevens** zoals hulpvragen, verslavings- of ontwikkelproblematiek, financiële situaties of gegevens over personen uit het netwerk van de klant

De gegevens worden verwerkt voor goede dossiervorming in het kader van de hulpverlening.

2.1.1 Mag je bijzondere persoonsgegevens verwerken?

Je mag bijzondere persoonsgegevens alleen verwerken als de betrokkene uitdrukkelijk toestemming heeft gegeven of als er sprake is van een specifieke uitzondering. Bijzondere persoonsgegevens zijn: ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van vakbond, genetische gegevens, gezondheid, seksueel gedrag of gerichtheid, en biometrische gegevens met oog op unieke identificatie van een persoon.

Gezien de aard van de werkzaamheden binnen Team Werk kan het voorkomen dat tijdens gesprekken persoonsgegevens worden gedeeld die als bijzonder kwalificeren, zoals gegevens over gezondheid of religieuze of levensbeschouwelijke overtuigingen. Deze gegevens worden niet structureel verwerkt en maken geen standaard onderdeel uit van de intake, maar kunnen incidenteel aan de orde komen voor zover dit noodzakelijk is voor de beoordeling van de persoonlijke situatie van de betrokkene in het kader van sociale zekerheid en arbeidsinschakeling. Dit kan met name het geval zijn bij de beoordeling van arbeidsverplichtingen of plaatsing bij werkgevers zoals bedoeld in artikel 9 van de Participatiewet, waarbij de belastbaarheid of beperkingen van de betrokkene in beeld moeten worden gebracht.

Voor zover bij gesprekken bijzondere persoonsgegevens worden verwerkt, vindt dit plaats op grond van artikel 9 lid 2 onder b van de AVG, omdat de verwerking noodzakelijk kan zijn voor de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van het socialezekerheids- en socialebeschermingsrecht, zoals vastgelegd in de Participatiewet.

Bijzondere persoonsgegevens, waaronder gezondheidsgegevens of religieuze of levensbeschouwelijke overtuigingen, worden niet standaard vastgelegd in rapportages. Waar dergelijke gegevens uitsluitend contextueel worden genoemd en niet noodzakelijk zijn voor de uitvoering van de wettelijke taak, worden zij niet overgenomen in de definitieve rapportage. Wanneer het wel relevant en noodzakelijk is voor de verdere ondersteuning is het aan de consulent om dat te bepalen en te zorgen voor het zo samenvatten van het gesprek, dat het wel wordt opgenomen in de rapportage of door het zelf toe te voegen.

2.1.2 Mag je strafrechtelijke persoonsgegevens verwerken?

Je mag strafrechtelijke persoonsgegevens alleen onder voorwaarden verwerken. Voorbeelden van strafrechtelijke gegevens zijn: strafrechtelijke veroordelingen ('strafblad'), strafbare feiten, verdenkingen en veiligheidsmaatregelen.

Strafrechtelijke gegevens mogen op grond van artikel 10 van de AVG alleen worden verwerkt onder toezicht van een officiële autoriteit of als er een wettelijke grondslag is in de nationale wetgeving, met passende waarborgen. Voor gemeenten kan verwerking in voorkomende gevallen plaatsvinden in het kader van de uitvoering van wettelijke taken.

Binnen de pilot van Team Werk worden strafrechtelijke persoonsgegevens niet structureel verwerkt. Tijdens gesprekken met klanten kunnen dergelijke gegevens incidenteel ter sprake komen, bijvoorbeeld in relatie tot belemmeringen bij arbeidsinschakeling of plaatsing bij werkgevers. Deze informatie maakt echter geen standaard of noodzakelijk onderdeel uit van de verslaglegging.

Gelet op het incidentele karakter van dergelijke informatie is het naar alle waarschijnlijkheid niet noodzakelijk deze gegevens over te nemen in definitieve rapportage. Indien strafrechtelijke gegevens tijdens een gesprek worden genoemd zal deze informatie in beginsel niet worden vastgelegd in de rapportage. Waar vastlegging in uitzonderlijke gevallen onvermijdelijk is voor de uitvoering van de wettelijke taak wordt de informatie beperkt tot het strikt noodzakelijke en geformuleerd zonder strafrechtelijke details.

2.1.3 Mag je het BSN verwerken?

Je mag het BSN alleen verwerken als dit in een wet staat. Maar je moet ook beoordelen of het nodig is. Het burgerservicenummer (BSN) maakt geen onderdeel uit van de gegevensverwerking binnen de scope van

deze pilot. De transcribeertool wordt uitsluitend ingezet bij intakegesprekken en interne overleggen, waarbij het BSN niet wordt vastgelegd of verwerkt.

2.1.4 Kan je het doel ook met minder persoonsgegevens bereiken?

Een belangrijk begrip bij het beoordelen van de noodzaak is 'proportionaliteit'. Dit betekent dat je afweegt of het nodig is alle persoonsgegevens te verwerken die je eerder in de tabel hebt opgesomd. En dat je deze afweging kan uitleggen. Bij de beoordeling van proportionaliteit is gekeken naar de verhouding tussen het doel van de verwerking en de impact op de privacy van betrokkenen. De inzet van de transcribeertool wordt in het kader van deze pilot als proportioneel beoordeeld, omdat de verwerking van persoonsgegevens zoveel mogelijk is beperkt en gericht is ingericht. Daarbij is van belang dat:

- De uiteindelijke rapportage slechts een samenvatting bevat van voor de hulpverlening relevante informatie en geen volledige of letterlijke weergave van het gesprek
- Overregistratie actief wordt voorkomen door het gebruik van vooraf ingerichte rapportagemodellen, die zijn afgestemd op de context van gemeentelijke hulpverlening en uitsluitend dossierwaardige informatie genereren. De gemeente moet nog besluiten wat voor model voor het sociaal domein gebruikt moet worden. Tijdens de sessie is gesproken over samenvatting, afspraken en acties. Voor intern gebruik wordt aanbevolen het rapportage model te beperken tot een beknopte weergave van de kern van het overleg, zoals een overzicht van gemaakte afspraken en actiepunten.
- Gegevens niet langer worden bewaard dan noodzakelijk voor het verslagleggingsproces en niet worden gebruikt voor modeltraining of andere secundaire doeleinden
- Daarnaast is de werking van de transcribeertool zodanig ontworpen dat dataminimalisatie structureel wordt geborgd. Audiofragmenten en transcripten die nog niet zijn gedeïdentificeerd, worden uitsluitend tijdelijk verwerkt in het werkgeheugen van de systemen en direct verwijderd zodra de technische verwerking is afgerond. Er vindt geen opslag plaats van ruwe audio. De verwerking vindt plaats in realtime en in kleine fragmenten, waardoor het risico op onnodige of grootschalige gegevensverwerking wordt beperkt.
- Na transcriptie worden herleidbare persoonsgegevens automatisch gedeïdentificeerd. Namen, adressen en andere direct identificerende gegevens worden gemaskeerd of vervangen door rolomschrijvingen, waarna het oorspronkelijke transcript met persoonsgegevens wordt verwijderd. De uiteindelijke rapportage wordt gegenereerd op basis van het gedeïdentificeerde transcript en het toegepaste rapportagemodel, waardoor wordt voorkomen dat persoonlijke of niet-relevante details in het klantdossier terechtkomen.

De tool wordt uitsluitend ingezet ter ondersteuning van de verslaglegging van gesprekken met klanten en interne overleggen en niet voor andere doeleinden. Medewerkers blijven verantwoordelijk voor de controle, selectie en vaststelling van de vastgelegde informatie. Er vindt geen geautomatiseerde besluitvorming plaats en de inzet van de tool heeft geen directe gevolgen voor de rechten of plichten van klanten of medewerkers.

De mogelijke voordelen van de inzet van de transcribeertool, zoals vermindering van administratieve belasting en betere navolgbaarheid van rapportages, zijn in de pilotfase nog niet vastgesteld maar vormen aanleiding voor het verkennen van deze technologie. De mogelijke privacy risico's worden beperkt door passende technische en organisatorische maatregelen, waaronder beveiligingsmaatregelen, toegangsbeperkingen en duidelijke afspraken over gebruik en opslag van gegevens. Doordat rapportages snel beschikbaar zijn, kan de betrokkene bovendien direct meekijken of meelezen, wat bij kan dragen aan transparantie in het gesprek en de vastlegging daarvan.

2.2 Waar komen de persoonsgegevens vandaan?

Denk aan de betrokkene zelf, een andere organisatie, de gemeente (bijv. burgerzaken/BRP, een andere afdeling/team)

De persoonsgegevens die binnen deze pilot worden verwerkt, zijn afkomstig van de betrokkene zelf. Deze gegevens worden mondeling verstrekt tijdens gesprekken tussen de betrokkene en een consulent van Team Werk in het kader van de uitvoering van taken binnen het sociaal domein. Het betreft informatie die relevant is voor begeleiding, ondersteuning en verslaglegging.

Ter ondersteuning van de vastlegging van deze gesprekken wordt gebruikgemaakt van een transcribeertool. De mondeling verstrekte informatie wordt tijdelijk vastgelegd in audio en vervolgens automatisch omgezet in tekst. De audio-opname dient uitsluitend als technisch middel om de transcriptie mogelijk te maken en vormt geen zelfstandige bron van persoonsgegevens.

De verdere verwerking vindt plaats op basis van het gegenereerde transcript. Er worden geen persoonsgegevens verkregen uit externe bronnen, koppelingen met andere systemen of geautomatiseerde verrijking. De verwerking blijft beperkt tot de informatie die door de betrokkene zelf tijdens het gesprek wordt gedeeld.

2.3 Hoe zorg je dat de persoonsgegevens juist zijn en actueel blijven?

Het is belangrijk dat we alleen persoonsgegevens verwerken die juist zijn. En dat we deze actualiseren als dat nodig is.

De transcriptie wordt niet automatisch als verslag gebruikt. Zelfs wanneer er fouten in het transcript ontstaan, bijvoorbeeld door spraakherkenning die accenten of woorden verkeerd interpreteert, kan het rapportagemodel op basis van ingebouwde contextkennis en domein specifieke logica alsnog de juiste betekenis reconstrueren. Dit betekent dat het model in zekere zin een correctieslag op het transcript uitvoert door irrelevante of foutieve elementen te filteren of corrigeren in de gegenereerde rapportage.

Daarnaast is de afspraak dat het conceptrapport altijd door de consulent moet worden gecontroleerd en samen met de klant moet worden besproken voordat het definitief wordt gekopieerd en geplakt in het dossier. Gebruikers kunnen de gespreksnotities (samenvattende teksten op basis van het transcript) teruglezen na het gesprek en het rapport hierop aanpassen.

Terwijl de opname loopt krijgt de gebruiker elke +/- 30-60 seconden een samenvatting te zien van het laatste stuk van het gesprek. Hiermee weet de gebruiker dat de opname loopt en dat de software begrijpt waar het gesprek over gaat. Deze gespreksnotities zijn ook tijdens de aanpassingsfase beschikbaar voor de gebruiker om terug te lezen na het gesprek en eventuele aanpassingen hierop te baseren.

De consulent heeft de mogelijkheid om de opname te pauzeren, bijvoorbeeld bij gevoelige onderwerpen om ervoor te zorgen dat de klant zich vrij voelt om volledig te zijn in de informatie de wordt gedeeld.

In het definitieve rapport worden afspraken en actiepunten opgesteld en dit is input voor het plan van aanpak en heeft dus geen directe gevolgen. Deze werkwijze reduceert het risico dat onjuiste of onvolledige informatie leidt tot verkeerde beslissingen en daarmee tot schending van het socialezekerheidsrecht. Het risico is hiermee echter niet volledig uitgesloten en vraagt blijvende aandacht voor zorgvuldige betekenisvolle menselijke controle.

Tijdens de pilot zitten er verschillende feedbackloops verwerkt in de software op basis waarvan de beschikbare kennis en context laag van de rapportagemodellen zullen worden geanalyseerd en waar nodig aangepast en op basis van de transcripten opnieuw getest. De software houdt bijvoorbeeld bij hoe vaak er

aanpassingen worden gemaakt en categoriseert het type aanpassingen. Ook kunnen gebruikers ratings geven en feedback beschrijven in de software. Tevens is er direct contact tussen 5.1.2i en de gebruikers in de pilot om de eisen en wensen zo duidelijk mogelijk inzichtelijk te maken.

2.4 Ga je gebruikmaken van geautomatiseerde besluitvorming, profilering of big data?

Geautomatiseerde besluitvorming, profilering en big data kunnen grote gevolgen hebben. Geautomatiseerde besluiten zijn besluiten zonder tussenkomst van een medewerker. Bijv. opleggen snelheidsboete met informatie uit een flitscamera zonder dat een persoon meekijkt in het proces of het opleggen van de boete juist is. Profileren is het opbouwen van profielen waarmee je personen in categorieën kunt indelen. Bijv. beoordelen op basis van gedrag, betrouwbaarheid, prestaties, gezondheid, economische situatie, locatie, persoonlijke voorkeuren of interesses. Big data is een grote hoeveelheid gegevens uit verschillende bronnen analyseren waarbij je geautomatiseerd zoekt naar onderlinge verbanden waarmee je beslissingen kunt nemen op groeps- of individueel niveau. Een voorbeeld is fraudebestrijding. Beschrijf ook wat de gevolgen zijn voor betrokkenen.

De inzet van de transcribeertool van 5.1.2i valt niet onder geautomatiseerde besluitvorming, profilering of big data.

Geautomatiseerde besluitvorming (Artikel 22 van de AVG)
5.1.2i genereert op basis van een transcript van het gesprek een concept-rapportage. Deze concept-rapportage wordt altijd door de consulent samen met de klant besproken en, waar nodig, aangepast. In het gesprek stelt de consulent afspraken en actiepunten vast en niet op basis van het transcript of de gegenereerde rapportage, deze dienen enkel ter ondersteuning. De transcribeertool neemt geen besluiten en heeft geen zelfstandige beslissingsbevoegdheid. Er is geen sprake van besluiten die uitsluitend geautomatiseerd tot stand komen; de verwerking vindt plaats met betekenisvolle menselijke tussenkomst en onder volledige verantwoordelijkheid van de consulent.

Profilering
Profilering in de zin van de AVG betreft het geautomatiseerd verwerken van persoonsgegevens om persoonlijke aspecten van een betrokkene te evalueren of te voorspellen. De transcribeertool van 5.1.2i bouwt geen profielen op en analyseert geen gedrag, kenmerken of risico's van personen. De verwerking is beperkt tot het omzetten van een gesprek in een samenvatting en rapportage ter ondersteuning van de verslaglegging door de consulent. Er worden geen classificaties, scores of voorspellende analyses toegepast op individuele klanten.

Big Data
Van big data-verwerking is geen sprake. De transcribeertool verwerkt uitsluitend gegevens uit individuele gesprekken tussen klant en consulent of tussen medewerkers. Er vindt geen analyse plaats van grote hoeveelheden gegevens, geen koppeling met externe databronnen en geen patroonherkenning of vergelijking tussen dossiers. De verwerking is kleinschalig, context gebonden en gericht op het specifieke gesprek.

Menselijke controle en borging
Het is de bedoeling dat het conceptrapport altijd door de consulent samen met de klant gecontroleerd en geaccordeerd wordt voordat het definitief wordt opgenomen in het dossier. Tijdens de pilotfase wordt daarnaast het correctiegedrag van consulenten geëvalueerd en wordt aandacht besteed aan bewustwording van hun eindverantwoordelijkheid voor de inhoud van de rapportages. Deze evaluatie heeft uitsluitend betrekking op de werking en kwaliteit van de functionaliteit van het systeem en leidt niet tot geautomatiseerde beoordeling, profilering of besluitvorming over individuele klanten.

2.5 Ga je gebruikmaken van nieuwe technologieën?

Ja, bij deze verwerking wordt gebruikgemaakt van nieuwe technologieën. De gemeente zet een door AI ondersteunde transcribeertool in voor het vastleggen en structureren van gespreksinhoud. Deze

technologie wijkt af van traditionele handmatige verslaglegging doordat gebruik wordt gemaakt van automatische spraakherkenning en AI-gestuurde tekstverwerking.

Hoog-risico toepassing

Onderstaand volgt een korte uiteenzetting of er sprake is van een hoog risico in de zin van de AI-verordening.

Annex III van de AI-verordening bevat een uitputtende lijst van toepassingsgebieden waarin AI-systemen als hoog risico worden aangemerkt in de zin van artikel 6 van deze verordening. Het gaat daarbij op AI-toepassingen die gelet op hun doel, context en potentiële impact, een significant risico kunnen vormen voor fundamentele rechten van natuurlijke personen. De kwalificatie als hoog risico is niet afhankelijk van de technische complexiteit van het systeem, maar van de functie die het systeem vervult binnen een maatschappelijk of bestuurlijk proces.

Voor deze DEPIA is met name Annex III, onderdeel 5 relevant. Dit onderdeel ziet op AI-systemen die door publieke autoriteiten worden gebruikt om de toegang tot essentiële publieke voorzieningen en uitkeringen te evalueren, te beïnvloeden of te administreren, waaronder diensten in het sociaal domein. De beoordeling richt zicht daarbij niet uitsluitend op systemen die formeel besluiten nemen, maar ook op het systemen die een materiële rol spelen in de voorbereiding, vastlegging of onderbouwing van dergelijke besluiten.

Gelet op de inzet van de transcribeertool binnen gemeentelijke processen binnen het sociaal domein in Team Werk, waar verslaglegging een structurele rol speelt in de beoordeling van rechten en plichten van burgers, is een toetsing aan Annex III, onderdeel 5 noodzakelijk om vast te stellen of sprake kan zijn van een hoog risico AI-systeem in de zin van de AI-verordening. De volgende paragrafen bevatten een uiteenzetting van de toepassing van deze regelgeving op de inzet van de transcribeertool.

De gemeente zet de transcribeertool in als ondersteunend hulpmiddel bij gesprekken in het sociaal domein, met als doel het vastleggen van gespreksinhoud in de vorm van transcripties ten behoeve van verslaglegging. De tool neemt geen autonome beslissingen over de toekenning, wijziging of beëindiging van publieke voorzieningen en verricht geen geautomatiseerde beoordeling van de rechtmatigheid of hoogte van uitkeringen.

Hoewel de inzet van de transcribeertool plaatsvindt binnen een context die onder Annex III, onderdeel 5 van de AI –verordening valt, te weten processen die zien op de beoordeling van aanspraken op essentiële publieke voorzieningen, is niet iedere AI-toepassing binnen dit toepassingsgebied automatisch aan te merken als een hoog risico AI-systeem. Op grond van artikel 6, derde lid, onderdeel d, van de AI-verordening geldt een uitzondering voor AI-systemen die uitsluitend worden ingezet voor het verrichten van een voorbereidende taak ten behoeve van een beoordeling van de geschiktheid of aanspraken van klanten op dergelijke sociale voorzieningen. Tijdens de pilot wordt de transcribeertool ingezet als hulpmiddel voor het vastleggen van gespreksinhoud in de vorm samenvatten van transcripties. De gegenereerde output vormt geen zelfstandig besluit. De verantwoordelijkheid voor de vastlegging van de verslaglegging in 5.1.2i en de daarop gebaseerde of opvolgende besluitvorming berust bij de behandelend consulent.

Samenvattend, vindt de inzet van de transcribeertool plaats binnen processen in het sociaal domein die onlosmakelijk zijn verbonden met besluitvorming over essentiële publieke voorzieningen, zoals op grond van de Participatiewet. Hoewel het gegenereerde rapport indirect betekenis kan hebben voor de feitelijke en juridische positie van de klant, wordt de tool tijdens de pilot uitsluitend ingezet ter ondersteuning van administratieve verslaglegging. De output vormt geen zelfstandig besluit en wordt structureel onderworpen aan menselijke controle. Onder deze maatregelen kan de inzet worden aangemerkt als ondersteunend van aard en valt buiten de kwalificatie als hoog-risico AI-systeem in de zin van artikel 6 en

Annex III, onderdeel 5(a) van de AI-verordening. Indien deze waarborgen in de praktijk niet worden nageleefd of de AI-output feitelijke leidend wordt in dossiers die worden gebruik bij (her)beoordelingen kan er alsnog sprake zijn van een hoog-risico toepassing en dient deze kwalificatie te worden herzien.

2.6 Welke applicaties gebruik je en is de informatiebeveiliging beschreven?

De gemeente moet passende technische en organisatorische maatregelen nemen om persoonsgegevens te beschermen. Het belangrijkste normenkader waaraan de gemeente moet voldoen, is de Baseline Informatiebeveiliging Overheid (BIO). Is er sprake van een leverancier van een applicatie? Is een verwerkersovereenkomst (VWO) afgesloten? En zijn de beveiligingsmaatregelen voor een applicatie beschreven? Vermeld dit in onderstaande tabel.

Applicatie + leverancier	**VWO*** (ja + zaaknummer / nee + reden)	**Beveiligingsmaatregelen geïnventariseerd?** (ja + datum + vindplaats / nee + reden)
Transcribeertool 5.1.2i	Ja	

**Leg een concept verwerkersovereenkomst altijd vooraf voor advies voor aan de Privacy Officer via 5.1.2i. Voeg altijd bewijsstukken van de verwerker bij over de genomen beveiligingsmaatregelen (bijv. ISO-certificaat, TPM-verklaring of rapportage van een pentest). De Privacy Officer stemt deze stukken af met de ISO.*

Beveiliging

Authenticatie en autorisatie

Aangewezen medewerkers van de Gemeente Leeuwarden die meedoen aan de pilot loggen in op de 5.1.2i-omgeving via de Gemeente Leeuwarden 5.1.2i tenant via SSO. Gebruikers kunnen alleen via 2FA inloggen op de 5.1.2i tenant. De Gemeente Leeuwarden 5.1.2i omgeving zal niet beschikbaar zijn buiten deze tenant om. 5.1.2i biedt de mogelijkheid om toegang tot het platform te beperken via IP-filtering (IPv4). Hiermee kan worden ingesteld dat alleen verbindingen vanaf vooraf gedefinieerde, vertrouwde IP-adressen toegang krijgen tot de omgeving.

Na inloggen heeft een gebruiker uitsluitend toegang tot zijn of haar eigen rapportages. Gebruikers hebben ook geen toegang tot de transcripten, alleen de gedeïdentificeerde samenvattende teksten.

Toegangsbeveiliging ontwikkelaars

Functionele logs worden gedeïdentificeerd opgeslagen en zijn alleen toegankelijk voor een selecte groep geautoriseerde ontwikkelaars van 5.1.2i. Toegang tot deze logs is beschermd met gebruikersnaam, wachtwoord en verplichte 2FA. De logs worden uitsluitend gebruikt voor:

- Ondersteuning van gebruikers
- Probleemoplossing
- Verbetering van de functionaliteit en prestaties van het systeem

Overige beveiligingsmaatregelen

Alle gegevens die worden opgeslagen of over het internet worden verzonden, waaronder persoonsgegevens, worden versleuteld met actuele encryptietechnologieën. Audio- en tekstverwerking gebeurt bovendien in kleine fragmenten (chunks) die tijdelijk in het geheugen worden verwerkt en daarna direct worden verwijderd. Door deze opzet wordt de risico-expositie tot een minimum beperkt.

5.1.2i 5.1.2i 5.1.2i

De datacenters van 5.1.2i 5.1.2i, 5.1.2i en 5.1.2i die 5.1.2i gebruikt voor hosting zijn eveneens ISO 27001-gecertificeerd.

Alle medewerkers van 5.1.2i hebben een geheimhoudingsovereenkomst getekend.

Beschikbaarheid

5.1.2i garandeert tijdens de pilot een beschikbaarheid van 99,7% en heeft tot op heden geen storingen gehad die langer dan 30 minuten duurden. Bij tijdelijke uitval is dit zichtbaar voor de gebruiker doordat de samenvattende tekstfragmenten niet verschijnen; transcripten worden dan tot 1 uur in memory bewaard, zodat alsnog een rapport kan worden gegenereerd of de gebruiker kan direct overschakelen op handmatige verslaglegging.

2.7 Welke afspraken heb je gemaakt met externe ontvangers?

Een organisatie die namens de gemeente gegevens verwerkt is een verwerker. Bijvoorbeeld omdat zij een wettelijke taak van de gemeente uitvoeren. Een andere organisatie kan ook samen met de gemeente verantwoordelijk zijn voor het verwerken van persoonsgegevens. Vaak is dit een ketenpartner. In beide gevallen moeten we een overeenkomst afsluiten. Met een verwerker sluiten we een verwerkersovereenkomst af. Bij gezamenlijke verantwoordelijkheid moeten we ook een overeenkomst afsluiten maar met andere bepalingen. Dit is vaak een convenant, regeling, DVO of samenwerkingsovereenkomst. Vermeld de gegevens in onderstaande tabel. Zet bij rol verwerker of verantwoordelijke) neer. Voeg zo nodig meer rijen toe of zet 'Niet van toepassing' neer. Twijfel je of en wat voor soort overeenkomst je moet afsluiten? Neem dan contact op met de Privacy Officer.

Organisatie	Rol	Status overeenkomst** + zaaknummer
5.1.2i	Verwerker	Wordt momenteel uitgewerkt

***Leg een concept verwerkersovereenkomst altijd vooraf voor advies voor aan de Privacy Officer via 5.1.2i. Voeg bij een verwerkersovereenkomst ook altijd bewijsstukken van de verwerker bij over de genomen beveiligingsmaatregelen (bijv. een ISO-certificaat, TPM-verklaring of rapportage van een pentest). De Privacy Officer stemt deze stukken af met de ISO. Zijn de andere organisatie en de gemeente gezamenlijk verantwoordelijk? Dan is het niet nodig bewijsstukken over de genomen beveiligingsmaatregelen mee te sturen.*

De software voor spraakgestuurd rapporteren (5.1.2i) maakt gebruik van verschillende technische componenten, gehost bij externe partijen. 5.1.2i huurt naast hosting ook GPU-capaciteit bij 5.1.2i 5.1.2i

Voor de transcriptie worden verschillende (ook open source) modellen ingezet, waarbij de verwerking plaatsvindt binnen de Europees Economische Ruimte (EER).

Gemeente Leeuwarden en 5.1.2i sluiten een verwerkersovereenkomst waarin wordt vastgelegd dat de data uitsluitend wordt gebruikt voor transcriptie- en rapportagedoeleinden en niet voor training van modellen.

- Met 5.1.2i, 5.1.2i en 5.1.2i zijn door 5.1.2i verwerkersovereenkomsten afgesloten. Deze partijen hosten de benodigde infrastructuur, maar hebben geen toegang tot de inhoudelijke data. De data worden uitsluitend verwerkt voor directe transcriptie en rapportgeneratie.
- **De** 5.1.2i 5.1.2i 5.1.2i en 5.1.2i 5.1.2i zijn managed services van 5.1.2i en vallen onder de standaardvoorwaarden van 5.1.2i, die voldoen aan de AVG.
- 5.1.2i wordt door 5.1.2i ingezet voor hosting en dataopslag. 5.1.2i wordt gebruikt voor het afnemen van serverruimte ten behoeve van het hosten en uitvoeren van AI-modellen. 5.1.2i wordt ingezet voor het identity- en toegangsbeheer en 5.1.2i wordt gebruikt voor monitoring en foutdetectie van de 5.1.2i applicatie.

Samengevat:

Partij	Rol onder AVG	Afspraken vastgelegd in/aanvullende maatregelen
Gemeente Leeuwarden	Verwerkingsverantwoordelijke	Intern beleid, hoofdovereenkomst en verwerkersovereenkomst 5.1.2i
5.1.2i	Verwerker	Hoofdovereenkomst en verwerkersovereenkomst
5.1.2i	Subverwerker	Verwerkersovereenkomst via 5.1.2i (standaard voorwaarden)
5.1.2i	Subverwerker	Verwerkersovereenkomst via 5.1.2i (standaard voorwaarden)
5.1.2i	Subverwerker	5.1.2i Data Processing Addendum van 5.1.2i
5.1.2i	Subverwerker	Verwerkersovereenkomst via 5.1.2i
5.1.2i	Subverwerker	Verwerkersovereenkomst via 5.1.2i
5.1.2i	Subverwerker	Verwerkersovereenkomst via 5.1.2i
Functional Software Inc	Subverwerker	Verwerkersovereenkomst via 5.1.2i

2.8 Wat is de bewaartermijn en hoe ga je de persoonsgegevens vernietigen?

We moeten gegevens bewaren (archiveren) maar vaak ook na een bepaalde tijd vernietigen. Bewaartermijnen staan in de gemeentelijke selectielijst. Let op: voor politiegegevens (Wpg) gelden specifieke bewaartermijnen. Noem altijd een concrete bewaartermijn en het nummer(s) in de VNG-selectielijst. Beschrijf ook hoe je de gegevens na de bewaartermijn gaat of laat vernietigen, wie dit doet (gemeente zelf, leverancier applicatie, andere organisatie) en wie dit controleert. Ga je je huidige systeem vervangen door een nieuw systeem? Beschrijf dan ook hoe en wanneer je het exportbestand gaat verwijderen en hoe je de gegevens in het oude systeem gaat/laat vernietigen. Vraag altijd advies aan 5.1.2e

De gegevens die binnen 5.1.2i worden verwerkt, worden uitsluitend bewaard zolang dit noodzakelijk is voor het doel van de verslaglegging en kwaliteitsborging. Zodra een rapportage met behulp van de transcribeertool is afgerond en is opgeslagen in 5.1.2i, is het in principe niet langer noodzakelijk dat deze gegevens ook in 5.1.2i beschikbaar blijven voor het primaire doel van dossiervorming.

Tijdens de pilotfase geldt echter een beperkte verlengde bewaartermijn in 5.1.2i, zodat rapportages tijdelijk kunnen worden geraadpleegd voor evaluatie, feedback en eventuele aanpassing van het model of het werkproces. Deze bewaartermijn is expliciet gekoppeld aan het pilotdoel en niet aan de inhoud van de intakegesprekken.

Voor spraakgestuurd rapporteren met 5.1.2i is onderscheid te maken tussen tijdelijke verwerking (in memory), opslag van rapporten, en het bewaren van gedeïdentificeerde logs (functionele logs) en technische logs (bevatten geen persoonsgegevens).

5.1.2i past het principe van tijdelijke verwerking toe voor de gevoelige onderdelen van het proces:

- Audio-opnamen worden in realtime verwerkt en zijn verdeeld in segmenten van maximaal 60 seconden. Zodra de transcriptie is voltooid, wordt het bijbehorende audiofragment direct verwijderd.

- Transcripties met direct herleidbare persoonsgegevens worden eveneens direct verwijderd zodra het fragment is gedeïdentificeerd. De verwerkingstaak per fragment duurt maximaal één uur.

Na de deïdentificatie kunnen de gedeïdentificeerde transcripten en de gegenereerde rapporten (beide nog steeds persoonsgegevens want indirect herleidbaar) worden opgeslagen in respectievelijk de transcriptiedatabase en de rapportagedatabase van 5.1.2i. Hiervoor geldt het volgende:

- De bewaartermijn van deze gegevens is voor tijdens de pilot vastgesteld op 90 dagen. Deze bewaartermijn is 90 dagen omdat evaluatie en testen van de contextlaag van het rapportagemodel in de pilot extra plaatsvindt. De bewaartermijn van 90 dagen geeft 5.1.2i de mogelijkheid om het model te optimaliseren voor Gemeente Leeuwarden om zo beter aan de doelen bij te dragen. Na ingebruikname kan die bewaartermijn korter worden (dit moet nog wel worden afgesproken). Dit geldt zowel voor de productieomgeving als voor eventuele back-ups.
- Aanpassing van bewaartermijnen is mogelijk, maar alleen via een formele procedure. Een zogeheten *Request For Change* (RFC) moet worden ingediend en goedgekeurd door zowel de directie van 5.1.2i als de informatiemanager van de klant.

2.9 Hoe heb je de data-ethische dilemma's in kaart gebracht?

Als gemeente staan we voor grote opgaven. Hiervoor willen we nieuwe technologische ontwikkelingen en data gebruik op een verantwoorde manier inzetten. Digitalisering kan de publieke waarden beïnvloeden, en heeft daarmee gevolgen voor de kwaliteit van leven van mensen. Neem contact op met 5.1.2e *over hoe je de data-ethische dilemma's in beeld brengt; vul dat hierna in onderstaande tabel en voeg de relevante bijlage toe.*

Tijdens de DEPIA-sessie en in dit rapport is expliciet stilgestaan bij ethische risico's van de inzet van spraakgestuurd rapporteren binnen het sociaal domein, in het bijzonder gelet op de positie van kwetsbare betrokkenen. Daarbij is niet uitsluitend gekeken naar juridische toelaatbaarheid en risico's, maar ook naar mogelijk onbedoelde effecten van het gebruik van AI-technologie en de daarmee samenhangende ethische aandachtspunten. Deze ethische risico's zijn mede beoordeeld in het licht van mogelijke effecten op fundamentele grondrechten. Een nadere uitwerking van de betrokken fundamentele rechten is opgenomen in Hoofdstuk 4 van dit rapport.

3 Risico's en maatregelen

3.1 Wat zijn de gevolgen voor betrokkenen en welke maatregelen ga je nemen?

Elke verwerking heeft risico's met een bepaalde impact op de betrokkenen. De aard en omvang van de verwerking bepaalt de impact. De door de organisatie genomen maatregelen met betrekking tot de AVG-beginselen, zoals hieronder uitgewerkt, hebben invloed op zowel de kans dat het risico zich manifesteert als op de omvang van de impact.

Voor de verwerking in deze DEPIA geldt dat de impact voor de betrokkenen wordt bepaald door een aantal elementen:

- De context van de gesprekken: De inzet van spraakgestuurd rapporteren binnen de Pilot ziet op introductiegesprekken in het sociaal domein. Tegelijkertijd maken introductiegesprekken onderdeel uit van een breder begeleidingstraject dat kan leiden tot formele besluitvorming, zoals een maatregelgesprek.

- De aard van de gegevens: de verwerking betreft opname en transcriptie van gesprekken waarin burgers persoonlijke informatie delen over hun problematiek, wensen, hun netwerk en mogelijk bij uitzondering, bijzondere of strafrechtelijke gegevens.
- De categorie betrokkenen: er worden gegevens verwerkt van personen met een afstand tot de arbeidsmarkt waaronder ook kwetsbare personen. Daarnaast is deze groep aan te merken als kwetsbaar, gezien de afhankelijkheid van de gemeente voor ondersteuning.
- De context waarin de gegevens worden gedeeld: De informatie wordt gedeeld in het kader van ondersteuning, vaak in situaties waarin de burger afhankelijk is van de consulent. Dit creëert een duidelijke afhankelijkheidsrelatie, waardoor de impact bij ongewenste verwerking groter is dan bij verwerkingen in een meer zakelijk of vrijblijvende context.
- De beleving van controle: Anders dan een samenvattende notitie, betreft de basis van de verwerking een volledige opname van wat is gezegd. Ook al wordt dit direct verwijderd, het feit dat er sprake is van opname en inzet van AI kan bij de klant het gevoel oproepen dat zij de controle verliezen, wat kan leiden tot terughoudendheid en minder openheid in het gesprek. Ook kan het de transparantie of begrijpelijkheid van de verwerkingen voor klanten beïnvloeden, zeker wanneer zij niet begrijpen waar de opname en verwerking voor bedoeld zijn en hoe die verwerkingen tot stand komen.

Er zijn onderstaande risico's geïdentificeerd die voor een bepaalde impact op betrokkenen kunnen zorgen.

Voor deze risico's zijn scenario's beschreven, die de impact op de betrokken beter duiden. Er worden bruto risico's beschreven (dus risico's als er geen maatregelen zouden zijn genomen), ook als ze netto, met bestaande maatregelen, al gemitigeerd zijn:

Risicocategorie 1: Vertrouwelijkheid van de gegevens wordt geschonden
Verwerkte gegevens worden beschikbaar voor onbevoegden.

Scenario	Geraakte waarden	Gevolgen voor de betrokkenen	Bruto inschatting	Netto inschatting
5.1.2i wordt gehackt of inloggegevens lekken, waardoor rapportages of transcripten op straat belanden.	Privacy, Veiligheid	Ongeautoriseerde openbaarmaking van gevoelige informatie (gezondheid, thuissituatie, problematiek). Kans op emotionele schade, schaamte, stigmatisering of discriminatie door derden. Ook verhoogde kans op phishing.	Kans: Hoog Impact: Hoog Zonder maatregelen is de kans hoog. Cloudomgevingen zijn bekende doelwitten. Impact is ook hoog want de rapporten bevatten gegevens over persoonlijke situaties van kwetsbare betrokkenen.	Kans: Laag Impact: Midden Audio en niet-gedeïdentificeerde transcripten worden alleen tijdelijk in memory verwerkt en niet opgeslagen. Rapporten en functionele logs worden gedeïdentificeerd (waardoor de impact bij een lek kleiner is) en versleuteld opgeslagen in ISO 27001/NEN 7510 gecertificeerde omgevingen. De leveranciersomgeving van 5.1.2i is afgeschermd met 2FA en voor Gemeente Leeuwarden medewerkers is er enkel toegang via SSO (na 2FA authenticatie voor de tenant). Zie ook overige

				maatregelen bij dataminimalisatie en beveiliging. De gebruikelijke werkwijze binnen gemeente Leeuwarden is dat bij het aangaan van de verwerkersovereenkomst de ISO 27001- verificatielijst van 5.1.2i wordt opgevraagd.
Meer personen dan noodzakelijk hebben toegang tot de gegevens	Privacy, Veiligheid	Zie gevolgen hierboven	Kans: Midden Impact: Midden Kans is midden, zonder maatregelen zijn autorisaties vaak te breed. Impact is vergelijkbaar als hierboven.	Kans: Laag Impact: Midden Kans is laag, gebruikers hebben alleen toegang tot de samenvatting van eigen gesprekken en geen enkele andere toegang.). Pas wanneer de rapportage geplakt is in het klantdossier hebben de door Gemeente Leeuwarden bepaalde consulenten toegang. Impact verandert niet. Zie ook beveiliging.

Risicocategorie 2: Integriteit van de gegevens wordt geschonden of uitkomsten zijn niet betrouwbaar

Gegevens of uitkomsten zijn niet juist, actueel of volledig en op basis van die gegevens wordt onjuist gehandeld (of niet gehandeld)

Scenario	Geraakte waarden	Gevolgen voor de betrokkenen	Bruto inschatting	Netto inschatting
De klant zegt minder of laat dingen achterwege, uit onzekerheid over de opname. (Chilling effect)	Privacy, menselijke waardigheid, autonomie	Er ontstaat een onvolledig of vertekend beeld van de situatie van de klant, wat de hulpverlening negatief kan beïnvloeden.	Kans: Midden Impact: Midden Kans is midden, sommige klanten zullen zich geremd voelen door technologie of opname, zeker bij gevoelige onderwerpen. Impact is ook midden, Incomplete informatie kan leiden tot een minder passend hulpaanbod of verkeerde inschattingen.	Kans: Laag[6] Impact: Midden De consulent heeft ruimte om de opname te pauzeren en bespreekt vooraf het doel van de opname. Opt-out wordt expliciet geboden zowel tijdens als na de pilot. Het doel van de pilot is expliciet om te onderzoeken of dit risico reëel is. De kans wordt nu laag geschat maar dit wordt pas duidelijk na evaluatie van de pilot. Aanbeveling is om vooraf het doel van de opname te bespreken om argwaan in eerste instantie te

[6] 5.1.2i heeft bij elke pilot medewerkers de vraag gesteld of zij het gevoel hebben gehad dat klanten minder open waren door de opnames dan voordat er met opnames werd gewerkt en zij geven aan dat dit bijna nooit voorkomt.

				voorkomen. Aanbeveling is ook om aan de consulent uit te leggen om bij argwaan gevoelige onderdelen desgewenst zonder opname te bespreken. Zie ook Juistheid.
De opname wordt onjuist omgezet naar tekst, bijvoorbeeld door accenten, dialect, persoonsverwisseling of achtergrondgeluid.	Controle over technologie, menselijke waardigheid	Het gegenereerde verslag bevat fouten of mist cruciale onderdelen, doordat uitspraken in de opname verkeerd worden geïnterpreteerd of toegeschreven aan de consulent of de klant. Dit kan leiden tot misverstanden of verkeerde interpretaties die invloed hebben op het verdere traject.	Kans: Midden Impact: Midden Kans is aanwezig. AI-modellen zijn (nog) niet perfect, vooral bij variatie in uitspraak of verstoringen. Impact is midden. Een incorrect verslag kan leiden tot verkeerde keuzes, tegelijk weet de consulent wat er is besproken.	Kans: Midden Impact: Laag De transcriptie wordt niet automatisch als verslag gebruikt, maar middels context geabstraheerd tot een rapportage/verslag, welke door de consulent samen met de klant moet worden gecontroleerd, waarbij de consulent expliciet aandacht heeft voor de zorgvuldige interpretatie van het gesprek. Hierbij is ook aandacht voor situaties waarin de klant zich mogelijk verkeerd begrepen voelt, om onjuiste of confronterende weergaven tijdig te corrigeren. Fouten kunnen direct worden hersteld. Pas daarna mag de rapportage worden geëxporteerd naar het dossier. Terwijl de opname loopt krijgt de gebruiker ook elke +/- 30-60 seconden een samenvatting te zien van het laatste stuk van het gesprek. In pilotfase wordt dit extra gemonitord en voert 5.1.2i analyses van fouten uit. Zie ook Juistheid. Aanbeveling is om ook vast te leggen in het werkprotocol dat het directe controleproces (met de klant) verplicht is.
Inferentie van het rapportagemodel is onvoldoende (b.v. verkeerde conclusies trekken omdat context verkeerd geïnterpreteerd	Controle over technologie, menselijke waardigheid	Er wordt iets gerapporteerd dat niet letterlijk is gezegd of bedoeld. Dit kan leiden tot misverstanden, onjuiste	Kans: Midden Impact: Midden Zie hierboven. Kans is midden. AI-systemen zijn contextgevoelig,	Kans: Laag Impact: Midden Zie maatregelen hierboven. Aanvullend geldt dat bij intern gebruik van de transcribeertool expliciet aandacht is voor

wordt, onterecht iets invullen (hallucinaties) of betekenis verschuiven, doordat het model nuances verkeerd overneemt).		beeldvorming en kan de betrokkene onbedoeld benadelen of bijdragen aan een gevoel van onveiligheid op de werkvloer.	maar kunnen bij onduidelijkheid verkeerde aannames doen. Impact is midden. Een incorrect verslag kan leiden tot verkeerde keuzes, tegelijk weet de consulent wat er is besproken. Intern gebruik van een onjuist weergegeven verslag kan leiden tot beïnvloeding van onderlinge verhoudingen, samenwerking of beeldvorming binnen teamverband.	correcte interpretatie van uitspraken van deelnemers aan het werkoverleg. Zodat onjuiste of verkeerd begrepen uitspraken niet wordt overgenomen en tijdig kan worden herkend en gecorrigeerd.
Twijfel, emotie, sarcasme of dubbele ontkenningen worden niet herkend.	Controle over technologie, autonomie	Rapportage mist nuance, waardoor intenties of gevoelens verkeerd geïnterpreteerd worden. Dit kan leiden tot verkeerde inschatting van hulpvraag of escalatie van problemen.	Kans: Hoog Impact: Midden AI-modellen hebben structurele beperkingen in het herkennen van emotie, sarcasme en contextuele nuances. Dit komt zeker voor in gesprekken met complexe situaties. Impact is hetzelfde als hierboven.	Kans: Midden Impact: Midden Zie maatregelen hierboven. Aanbeveling is ook om consulenten te trainen om AI-output altijd kritisch te beoordelen.

Risicocategorie 3: Gegevens zijn (tijdelijk) niet beschikbaar

Gegevens die verwerkt worden in 5.1.2i zijn (tijdelijk) niet beschikbaar of benaderbaar.

Scenario	Geraakte waarden	Gevolgen voor de betrokkenen	Bruto inschatting	Netto inschatting
Gegevens zijn tijdelijk niet beschikbaar in 5.1.2i, bijvoorbeeld door een	Controle over technologie	Tijdelijke onbeschikbaarheid kan zorgen voor vertraging in verslaglegging en frustratie bij betrokkenen.	Kans: Midden Impact: Laag Online platforms kunnen incidenteel onbeschikbaar zijn door technische	Kans: Laag Impact: Laag Rapporten worden geëxporteerd naar het klantdossier zodra ze definitief zijn. Aanbevolen wordt opname van verplichting in het

storing of uitval van de dienst.			storingen maar de impact is laag. Er kan altijd nog handmatig gerapporteerd worden (mogelijk vanaf het moment dat 5.1.2i onbeschikbaar was).	werkprotocol van een directe export naar 5.1.2i als consulent en klant de output samen hebben doorgenomen. Tijdelijke uitval leidt niet tot verlies van gegevens. 5.1.2i maakt gebruik van betrouwbare infrastructuur (ISO-gecertificeerd). Ook laat 5.1.2i onbeschikbaarheid zien in de interface als 5.1.2i tijdens de opname uitvalt. Aanbevolen wordt te onderzoeken of er een mogelijkheid is een geluid te laten afspelen wat kan bijdragen aan de snelheid dat onbeschikbaarheid wordt ontdekt.
De opname wordt niet gestart of de rapportage mislukt, bijvoorbeeld doordat de deïdentificatie stap faalt.	Controle over technologie	Er ontbreekt verslaglegging van het gesprek, dit kan de hulpverlening negatief beïnvloeden.	Kans: Midden Impact: Laag Kans is midden want er kunnen fouten optreden. Impact is laag, een consulent kan altijd nog overgaan op handmatige verslaglegging.	Kans: Laag Impact: Laag De consulent wordt door het systeem erop geattendeerd als er een fout is ontstaan (doordat de samenvatting niet zichtbaar is) en kan direct overschakelen op handmatige verslaglegging. Transcripten worden tot een uur bewaard als er een fout is opgetreden zodat alsnog rapportage kan plaatsvinden na verhelpen van het probleem. Aanbevolen wordt dit risico expliciet op te nemen in de instructie/training aan consulenten, met aandacht voor wat ze dan moeten doen.

Risicocategorie 4: Gegevens worden onrechtmatig (verder) verwerkt

Er is geen grondslag voor het verwerken of verstrekken van de gegevens, er worden niet-noodzakelijke gegevens verwerkt of geen rekening met proportionaliteit en subsidiariteit gehouden.

Scenario	Geraakte waarde	Gevolgen voor de betrokkenen	Bruto inschatting	Netto inschatting
Er worden meer gegevens gerapporteerd dan noodzakelijk voor de hulpverlening (overrapportage),	Privacy, autonomie, controle over technologie	Niet-noodzakelijke informatie wordt vastgelegd in het dossier, waardoor de belangen van de	Kans: Hoog Impact: Midden Kans: hoog, in gesprekken wordt	Kans: Laag Impact: Midden 5.1.2i maakt gebruik van contextspecifieke

bijvoorbeeld doordat irrelevante of persoonlijke details uit het gesprek in het rapport terechtkomen.		betrokkene onvoldoende geborgd zijn en verlies van vertrouwen kan ontstaan of onbedoelde beeldvorming die het vervolg van het zorgproces beïnvloedt.	regelmatig informatie gedeeld die niet noodzakelijk is voor verslaglegging. Zonder voldoende filtering kan deze informatie in het rapport terechtkomen. Impact: Midden, overrapportage leidt niet direct tot grote gevolgen voor de klant of medewerker. Uiteindelijk kan overrapportage wel leiden tot onbedoelde beeldvorming of mogelijk verlies van vertrouwen in de hulpverlening.	rapportagemodellen die zijn afgestemd op de praktijk van Gemeenten waarin ze worden ingezet. Deze modellen zijn zo ingericht dat zij uitsluitend die informatie selecteren en samenvatten die relevant is voor de professionele verslaglegging in het dossier, op basis van een door de gemeente gewenst rapportageformat. Irrelevante of informele onderdelen van het gesprek worden automatisch buiten het rapport gehouden en audio opnames worden verwijderd. De consulent kan en moet het rapport altijd controleren en aanpassen vóór opname in het dossier, waarbij de consulent actief beoordeelt of de opgenomen informatie noodzakelijk is voor het doel van de hulpverlening. Zie ook eerdere aanbevelingen daaromtrent.
Tijdens interne werk-of team overleggen wordt de transcribeertool gebruikt, terwijl collega's informeel met elkaar gesprekken voeren die niet relevant zijn voor het doel van het overleg. Onnodige informatie of persoonlijke gesprekken worden opgenomen en verwerkt terwijl deze informatie niet noodzakelijk is voor verslaglegging of interne besluitvorming.	Privacy, autonomie, controle over technologie, mienskip	Niet-noodzakelijke informatie van medewerkers wordt vastgelegd, wat kan leiden tot een inbreuk op de persoonlijke levenssfeer en een gevoel van ongemak of verminderde openheid binnen het team. Informatie die niet bedoeld is voor vastlegging (b.v. reden van afwezigheid door	Kans: Hoog Impact: Midden Kans: Tijdens interne overleggen vindt regelmatig informeel contact plaats. Indien de opname al loopt, is de kans reëel dat niet relevante informatie wordt vastgelegd. Impact: De informatie heeft in beginsel geen directe gevolgen	Kans: Midden Impact: Midden De transcribeertool wordt gebruikt voor doelgerichte verslaglegging van interne werkoverleggen op basis van een rapportageformat. De gegenereerde output wordt automatisch gestructureerd volgens dit format waardoor informatie die hier niet bij past, niet wordt opgenomen. Opnames worden direct na omzetten naar een transcript verwijderd.

		ziekte) wordt opgenomen en vastgelegd.	voor betrokkenen, maar kan wel ongemak of verlies van vertrouwen veroorzaken.	Aanbevolen wordt om ook de bewaartermijnen voor transcripten zo kort mogelijk te houden. Om het risico op onnodige verwerking van informele of persoonlijke informatie verder te beperken, wordt aanbevolen om de opname van interne werkoverleggen pas te starten nadat informele bijpraten is afgerond en ook op tijd te stoppen. Medewerkers dienen actief te worden geïnformeerd op het moment dat de opname start zodat voor alle aanwezigen duidelijk is vanaf welk moment het gesprek wordt vastgelegd. Deze werkwijze draagt bij aan bewustwording en voorkomt dat informele gesprekken onbedoeld worden verwerkt.
Gegevens worden op termijn gebruikt voor andere doeleinden dan waarvoor ze zijn verzameld (mission/function creep), zoals productiviteitscontrole van medewerkers of opstellen van klantprofielen	Privacy, autonomie, controle over technologie	De klant verliest de controle over zijn/ haar gegevens. Inzet van informatie buiten het oorspronkelijke doel kan leiden tot onbedoeld hergebruik, verlies van vertrouwen of privacy bezwaren.	Kans: Hoog Impact: Midden Wanneer data technisch beschikbaar is, bestaat de verleiding om deze breder in te zetten, zeker zonder duidelijke interne barrières of toetsmomenten. De impact kan onrechtmatige verwerking zijn.	Kans: Midden Impact: Midden In verwerkers-overeenkomsten is vastgelegd dat gegevens uitsluitend voor rapportage-doeleinden worden gebruikt. Gemeente Leeuwarden heeft een standaard privacy/security by design werkwijze ingericht. Hierin is opgenomen dat elk nieuw doeleinde voor de inzet van AI of verwerking van de gegevens vooraf te toetsen op doelbinding, proportionaliteit en rechtmatigheid.

Risicocategorie 5: Betrokkenen worden beperkt in hun rechten

Verwerking wordt niet transparant uitgelegd aan betrokkenen, betrokkenen kunnen hun rechten niet uitoefenen of weten niet waar.

Scenario	Geraakte waarde	Gevolgen voor de betrokkenen	Bruto inschatting	Netto inschatting
Betrokkenen worden beperkt in hun rechten	Privacy, autonomie, controle over technologie	Betrokkenen oefenen hun rechten niet uit door de beperking die ze ervaren of doordat hun verzoeken niet volledig worden behandeld	Kans: Laag Impact: Midden De kans is laag, er zijn weinig verzoeken en er bestaat een regulier proces voor het behandelen van verzoeken van betrokkenen. Impact is hoog want rechten van betrokkenen is een fundamenteel grondrecht, namelijk: artikel 47 Europees Handvest.	Kans: Laag Impact: Midden Voor de uitoefening van rechten kan het reguliere proces van Gemeente Leeuwarden worden gevolgd. Er bestaat echter een restrisico dat verzoeken niet goed worden behandeld als het bewustzijn van 5.1.2i als opslaglocatie bij reguliere inzage en wijzigingsverzoeken er nog niet is. Aanbeveling is om dit duidelijk te maken aan medewerkers die verzoeken behandelen.
Een klant wil eigenlijk geen opname, maar voelt alsof hij/zijn niet kan weigeren of denkt dat dit verplicht is.	Privacy, autonomie, controle over technologie, menselijke autonomie en rechtvaardigheid	De klant kan het gevoel hebben geen echte keuze te hebben, wat kan leiden tot terughoudendheid of verlies van vertrouwen in de hulpverlener.	Kans: Midden Impact: Midden Zeker in een afhankelijke hulpverleningsrelatie is het voor klanten lastig om bezwaar te maken of "nee" te zeggen. De beleving van vrijwilligheid is essentieel voor vertrouwen.	Kans: Laag Impact: Midden Transparante uitleg over de werkwijze en de mogelijkheid om bezwaar te maken wordt opgenomen in communicatie richting de klanten. Consulenten worden getraind in het voeren van dit gesprek.
De klant is onvoldoende geïnformeerd of begrijpt niet wat er met de opname gebeurt.	Privacy	De klant weet niet dat er opnames worden gemaakt of wat er daarna gebeurt met de gegevens, wat kan leiden tot schrik, bezorgdheid of klachten bij ontdekking.	Kans: Midden Impact: Midden Niet alle klanten lezen folders of begrijpen technische uitleg. Onvoldoende transparantie kan het vertrouwen aantasten.	Kans: Laag Impact: Midden Aanbevolen wordt om klanten zowel schriftelijk als mondeling te informeren over het gebruik van de transcribeertool. Hier kan in worden voorzien door een toelichting door de consulent van Team Werk bij het eerste

Met opmerkingen 5.1.2e: Ik vind dat dit goed is verwerkt in dit rapport. Dit kopje bestaat nog steeds, waarin wordt verwezen naar H3 en H4. Zie ook het volgende scenario waar wordt ingegaan op het informeren van de klanten. Ik stel voor dat deze aanbeveling dan ook even kort moet worden geplaatst onder het kopje hoe de betrokkene worden geïnformeerd. Dan is het wel dubbele informatie.

Vervolgens kunnen we ook bij het aanleveren van de def. versie hen attenderen op het feit dat zij dit intern zelf moeten bedenken en wij hier een aanbeveling op hebben gedaan. [Vermelding is verwijderd]

Met opmerkingen 5.1.2e: Eens, ik zou in de mail het volgende opnemen:

Daarnaast nog een punt over het informeren van betrokkenen. Wij zagen een opmerking van 5.1.2e hierover dat hier betere afspraken over moeten worden gemaakt. Dat juichen we natuurlijk toe maar wij zijn niet degenen die die afspraken voor jullie kunnen maken. We hebben daarop bij 1.5 toegelicht wat er nu aan informatie is en risico's en aanbevelingen opgenomen voor het goed regelen hiervan. Meer dan dat kunnen wij voor deze DEPIA nu niet doen maar jullie kunnen de DEPIA uiteraard zelf aanpassen wanneer jullie wel afspraken hebben gemaakt en die bij 1.5 verder toelichten.

				gesprek. Daarnaast wordt aanbevolen om een begrijpelijk informatievoorziening te ontwikkelen in de vorm van een flyer van Gemeente Leeuwarden, afgestemd op de doelgroep.

Risicocategorie 6: Uitkomsten zijn onvoldoende controleerbaar

Scenario	Geraakte waarden	Gevolgen voor betrokkenen	Bruto inschatting	Netto inschating
Consulenten vertrouwen te veel op het automatisch gegeneerde rapport/ uitkomsten AI-schrijfhulp ter verbetering van rapportage en controleren het niet goed (automation bias)	Controle over technologie, menselijke waardigheid	Menselijke controle is onvoldoende betekenisvol wat kan leiden tot fouten in de hulpverlening en vertrouwenverlies bij klant	Kans: Midden Impact: Hoog In de praktijk neigen gebruikers naar het overnemen van AI-output. De impact is gezien de context hoog als verkeerde feiten in dossiers terecht komen	Kans: Laag Impact: Hoog De kans wordt aanzienlijk lager dat consulenten 1 op 1 vertrouwen op de output van de transcribeertool wanneer controle van het rapport samen met de klant plaatsvindt.
Onvoldoende transparantie over welke delen van de audio zijn 'gecorrigeerd'	Controle over technologie	Achteraf is niet meer vast te stellen wat de tool produceerde en wat de consulent heeft veranderd of dat bewust of onbewust interpretatie is toegevoegd. Dit heeft negatieve gevolgen voor transparantie en vertrouwen van en voor klant.	Kans: Midden Impact: Midden Controleerbaarheid is zeer laag als geen audittrail beschikbaar is van menselijke correcties.	Kans: Impact: Meta data of logging data beschikbaar in 5.1.2i. Actief wordt hier tijdens de Pilotfase op geëvalueerd. De maatregel die wordt aanbevolen om samen met klant het rapport te controleren en te verbeteren reduceert het risico dat consulent op basis van interpretatie bewust of onbewust informatie toevoegt of verwijdert. De klant heeft hier rechtstreekse controle op.

Risicocategorie 7: Rechtvaardigheid en Duurzaamheid

Scenario	Geraakte waarden	Gevolgen voor de betrokkenen	Bruto inschatting	Netto inschatting
Bepaalde personen bijvoorbeeld met een bepaald accent worden structureel nadelig geïnterpreteerd.	Rechtvaar-digheid	Structurele nadelige interpretatie kan leiden tot bias in een transcribeertool wat kan leiden tot ongelijke toegang tot diensten en onjuiste registraties.	Kans: Hoog Impact: Hoog Zonder maatregelen is de kans hoog. Het is bekend dat AI-transcribeertechnieken niet perfect zijn en voorlopig bepaalde accenten niet goed kunnen oppakken. Als dit structureel gebeurt is de kans groot dat voor een bepaalde groep aan individuen gelijke behandeling wordt geschonden. De impact is hoog gezien de hulpverlening op financiële middelen ziet.	Kans: Midden Impact: Hoog Ondanks maatregelen zoals de inzet van LLM-model, training van het model op context, menselijke controle (aanbevolen wordt dit te implementeren in werkprotocol) en feedback tijdens de pilot, blijft het risico bestaan dat het spraakmodel structureel moeite heeft met regionale accenten. Gemeente Friesland kent bovengemiddelde kans vanwege Friese accenten en statushouders. Samengenomen blijft in Gemeentelijke context de impact hoog vanwege gelijke behandeling. Finetuning vereist hoogstwaarschijnlijk veel tijd. Er wordt dan ook aanbevolen om de feedback uit de Pilot samen met 5.1.2i goed te verwerken in de verbetering van de transcribeertool voordat deze werkwijze wordt uitgerold.
Medewerkers worden feitelijk buitengesloten van werkoverleggen als zij niet instemmen met de inzet van de transcribeertool	Rechtvaar-digheid	Medewerkers die niet instemmen met het gebruik kunnen zich sociaal geïsoleerd voelen omdat ze niet meer worden uitgenodigd voor meetings of omdat ze de enige zijn. Het risico	Kans: Midden Impact: Hoog De kans wordt als hoog ingeschat, omdat werkoverleggen een essentieel onderdeel vormen van samenwerking en informatie-uitwisseling	Kans: Laag Impact: Midden Aanbevolen wordt om bewaartermijnen van transcripten zo kort mogelijk te houden en individueel aan elke werknemer transparante communicatie te verstrekken waardoor het gebruik van de

tijdens werkoverleggen.		bestaat dat medewerkers hun privacy ondergeschikt maken aan groepsdruk.	binnen een (gemeentelijke) organisatie. Tegelijkertijd is het reëel dat medewerkers mogelijk bezwaar hebben tegen opname van overleggen. Impact: Uitsluiting van werkoverleggen kan ertoe leiden dat de medewerker informatie mist, minder kan deelnemen aan besluitvorming en zich in de praktijk in een ongelijkwaardige positie bevindt.	transcribeertool wordt genormaliseerd, terwijl ruimte blijft bestaan voor individuele voorkeuren. Aanbevolen wordt een intern document vast te stellen waarin expliciet wordt vastgelegd dat het niet instemmen met de inzet van 5.1.2i tijdens werkoverleggen geen gevolgen heeft voor deelname aan overleggen, informatievoorziening of de arbeidspositie van medewerkers, en waarin tevens wordt opgenomen dat medewerkers zich bij ervaren druk of vragen altijd kunnen wenden tot een vertrouwenspersoon.
Er wordt gebruik gemaakt van AI-services waardoor de ecologische voetafdruk van het proces (mogelijk) niet in verhouding meer staat tot de efficiencywinst die hiermee beoogd werd.	Duurzaamheid	De ecologische voerafdruk van het AI gebruik, voornamelijk van taalmodellen draagt bij aan de maatschappij nadelige klimaatverandering.	Kans: Hoog Impact: Grote taalmodellen hebben veel energieconsumptie. Gemeenteprocessen die frequent transcriptie uitvoeren met een taalmodel kunnen een grotere ecologische voetafdruk veroorzaken. Het trainen en draaien van LLM's draagt bij aan CO2 uitstoot wat mogelijk niet in verhouding staat tot de winst in procesoptimalisatie.	Kans: Impact: Aanbevolen wordt om in de pilot te evalueren hoe de gemeente met dit risico wenst om te gaan.

Risicocategorie 8: Verlies van controle op het gebruik van gegevens (subrisico)

Een sub-risico dat een rol speelt is het **verlies van controle op het gebruik van de gegevens,** zoals geen zicht hebben op de verwerkingslocaties van gegevens, gegevens langer bewaren dan noodzakelijk of geen grip hebben op verwerkers. Dit is een risico dat de risico's hierboven vergroot omdat bijvoorbeeld de rechtmatigheid van de verwerking niet aan te tonen is of omdat de impact bij een datalek groter is.

Scenario	Geraakte waarden	Gevolg voor welke risicocategorie	Maatregelen
Gegevens worden langer bewaard dan noodzakelijk	Privacy, veiligheid	Vertrouwelijkheid: De impact bij een datalek wordt groter als er meer gegevens zijn die al verwijderd hadden moeten worden. Onrechtmatigheid: Gegevens worden langer bewaard waardoor er meer gegevens worden bewaard dan noodzakelijk	Audio wordt direct verwijderd. Transcripten, samenvattingen en rapportages worden tijdens de pilot na 90 dagen verwijderd. Aanbeveling is om in de pilot te bepalen wat een passende bewaartermijn is bij in productie name.
De gemeente wordt niet vooraf geïnformeerd over taalmodel wisselingen waardoor de gemeente geen inzicht heeft in welk taalmodel op welk moment is gebruikt.	Controle over technologie	Onrechtmatigheid: Doordat de gemeente niet vooraf wordt geïnformeerd over wijzigingen in de ingezette taalmodellen, kan zij niet beoordelen of de aard van de verwerking is gewijzigd, of privacyrisico's zijn toegenomen of een herbeoordeling van de DEPIA noodzakelijk is. Hierdoor bestaat het risico dat persoonsgegevens onrechtmatig (verder) worden verwerkt buitende afgesproken kaders. Daarnaast kan het ontbreken van inzicht in ingezette taalmodellen ertoe leiden dat de gemeente niet voldoet aan haar verplichtingen o.g.v. de AI Act, die vereist dat de gebruiksverantwoordelijke[7] van AI-systemen voldoende grip en	Voor het genereren van de samenvatting en de rapportage maakt 5.1.2i gebruik van verschillende taalmodellen. Modelwisselingen kunnen plaatsvinden binnen dezelfde clouddienst. Aanbevolen wordt om in de verwerkersovereenkomst met 5.1.2i expliciet vast te leggen dat: 5.1.2i de gemeente vooraf informeert over wijzigingen in ingezette taalmodellen, ook als deze taalmodellen binnen dezelfde cloudomgeving wordt ingezet.

[7] De AI Act bevat verplichtingen voor 'deployers' (zijnde organisaties die AI-systemen inzetten, in dit geval de Gemeente Leeuwarden)

	inzicht hebben in de werking en inzet van AI en dat overheden transparent zijn over gebruikte algortimen (bijvoorbeeld via het algoritmeregister). Onvoldoende controleerbare uitkomsten: Wanneer niet inzichtelijk is welk taalmodel op welk moment is gebruikt kan de gemeente de totstandkoming en betrouwbaarheid van de gegenereerde transcripties en rapportages onvoldoende controleren en verantwoorden	

Fundamentele grondrechten

Onderstaand is een tabel toegevoegd om inzicht te vergaren, welke fundamentele grondrechten mogelijk worden geraakt door de toepassing van de Transcribeertool.

Fundamenteel grondrecht	Bron (EU-Handvest / EVRM)	Hoe kan dit recht worden geraakt?	Concreet risico bij transcribeertool	Beperkende maatregelen / waarborgen
Menselijke waardigheid	Art. 1 EU-Handvest	Onzorgvuldige vastlegging kan leiden tot stigmatisering of aantasting van eigenwaarde	Context of subjectieve uitspraken worden letterlijk vastgelegd zonder duiding	5.1.2i heeft context ingebouwd in het model. Menselijke eindredactie; instructies “feitelijk correct (juistheid) en noodzakelijk”; geen automatische opslag zonder controle
Privéleven	Art. 7 EU-Handvest / Art. 8 EVRM	Ingrijpende inmenging door vastlegging van persoonlijke gesprekken	Gesprekken bevatten intieme of contextuele informatie die niet noodzakelijk is voor dossiervorming	Dataminimalisatie; geen structurele opslag audio; korte bewaartermijnen tijdelijke data; duidelijke werkinstructies/training
Bescherming persoons-gegevens	Art. 8 EU-Handvest / AVG	Onrechtmatige of disproportionele verwerking	Verwerking van bijzondere persoonsgegevens (financieel, gezondheid) en mogelijk strafrechtelijke gegevens	DPIA(MA); doelbinding; beperkte toegang; verwerkersovereenkomst; toezicht FG; duidelijke werkinstructies/training

Fundamenteel grondrecht	Bron (EU-Handvest / EVRM)	Hoe kan dit recht worden geraakt?	Concreet risico bij transcribeertool	Beperkende maatregelen / waarborgen
Bescherming persoons-gegevens	Art. 8 Eu-Handvest/AVG artikel 17	Onvolledige afhandeling inzage/verwijdering	Verlies van controle over persoonsgegevens	Kennis bij consulenten; afstemming met 5.1.2i; opnemen proces borging rechten van betrokkenen
Sociale zekerheid en sociale bijstand	Art. 34 EU-Handvest	Onjuiste of onevenwichtige verslaglegging kan invloed hebben op toegang tot of voortzetting van ondersteuning/uitkering	Transcriptiefouten of samenvattingen kunnen doorwerken in beoordeling, hercontrole of handhaving	Menselijke eindcontrole vóór opname in 5.1.2i (onderdeel van werkprotocol); scheiding ruwe transcriptie/definitief verslag; alleen noodzakelijke feiten; correctiemogelijkheid; geen automatische besluitvorming; kwaliteitscontroles
Non-discriminatie	Art. 21 EU-Handvest	Ongelijke behandeling op basis van achtergrond of sociaaleconomische positie	Onbedoelde vastlegging of interpretatie van kenmerken kan discriminerend uitwerken	Geen profiling; geen hergebruik voor risicoselectie; bewustwording consulenten d.m.v. training; Periodieke monitoring tijdens Pilot van structurele transcriptiefouten leidt tot samenwerking 5.1.2i structurele verbetering voor definitieve uitrol
Non-discriminatie	Art. 21 EU-Handvest	Ongelijke behandeling op basis van (privacy)voorkeur van de medewerking ten aanzien van persoonlijke gegevensverwerking.	Bij inzet van transcribeertool tijdens werkoverleggen lopen medewerkers die niet instemmen met het gebruik van de tool het risico minder toegang te hebben tot overleggen, relevante informatie te missen, professionele of sociale druk te voelen en anders worden behandeld dan collega's die wel instemmen.	Deelname van werkoverleggen is niet afhankelijk van instemming met de transcribeertool. Schriftelijk kenbaar maken dat bezwaar tegen de transcribeertool geen arbeidsrechtelijke gevolgen heeft.
Eerlijke rechts-bescherming	Art. 47 EU-Handvest	Burgers moeten kunnen begrijpen, betwisten en laten toetsen hoe een besluit of handelen tot stand is gekomen. Dossiervorming en	De transcribeertool beïnvloedt welke informatie wordt vastgelegd en hoe het gesprek wordt samengevat. Dit kan de motivering (en daarmee de toetsbaarheid) sturen:	Transparantie over AI gebruik in de flyer(dat AI wordt gebruikt, welke output en dat het ondersteunend is); inzage voor klant in rapportage; menselijke eindredactie; audit trail (logging) in 5.1.2i

Fundamenteel grondrecht	Bron (EU-Handvest / EVRM)	Hoe kan dit recht worden geraakt?	Concreet risico bij transcribeertool	Beperkende maatregelen / waarborgen
		motivering zijn daarbij cruciaal	fouten/omissies in transcript of samenvatting worden “waar” in het dossier; onduidelijkheid over AI-inzet maakt het proces minder betwistbaar; risico op black-box motivering als output (deels) wordt overgenomen zonder uitleg.	
Transparantie en informatie	Art. 41 EU-Handvest /	Onvoldoende informatie over verwerking ondermijnt vertrouwen	Klant weet mogelijk niet dat transcriptie plaatsvindt	Actieve informatie vooraf; privacyverklaring; mogelijkheid gesprek zonder tool
Vrijheid van meningsuiting en communicatie	Art. 11 EU-Handvest	Terughoudendheid om vrij te spreken door opname/transcriptie	Klant past gedrag aan door gevoel van monitoring	Vrijwilligheid; pauzefunctie; alternatief zonder transcriptie

4 Conclusies en aanbevelingen

Zodra de vragen en opmerkingen vanuit data-ethiek, recordmanagement, informatiebeveiliging en privacy in de DEPIA zijn verwerkt, komen hier de conclusies en aanbevelingen. Daarna volgt de beoordeling (het advies) van de FG.

4.1 Conclusies en aanbevelingen

Risicocategorie	Restrisico (samengevat)	Aanbevelingen
1. Vertrouwelijkheid	Ongeautoriseerde toegang tot rapportages of metadata blijft mogelijk	Verifieer actief de geldigheid en reikwijdte van de ISO 27001-certificering van 5.1.2i door inzage te vragen in de verificatielijst. Borg strikt autorisatiebeheer (least privilege) inclusief duidelijke procedures voor het gebruik van eventuele admin-accounts.
2. Integriteit	Onvolledig beeld doordat klanten zich geremd voelen door opname ("Chilling effect")	Toets het *chilling effect* expliciet in de pilot en leg aan consulenten uit dat zij alert moeten zijn op 5.1.2i van terughoudendheid bij de klant. Instrueer dat gevoelige onderdelen van het gesprek, indien nodig, zonder opname kunnen worden besproken door de opname tijdelijk te pauzeren. Maak deze handelwijze onderdeel van het interne protocol of de werkinstructie en geef in de klantcommunicatie duidelijk aan dat dit altijd mogelijk is.
2. Integriteit	Rapporten bevatten onjuiste of onvolledige informatie door AI-inferentie of nuanceverlies	Stel het directe controleproces samen met de klant verplicht: na ieder gesprek wordt het automatisch gegenereerde rapport gezamenlijk doorgenomen en waar nodig aangepast voordat het definitief wordt opgeslagen. Leg deze werkwijze vast in een werkinstructie en zorg voor bewustwording bij consulenten van hun eindverantwoordelijkheid voor de juistheid en zorgvuldige weergave van het gesprek. Evalueer tijdens de pilot de wijze waarop uitspraken van klant en consulent in de rapportage worden weergegeven en monitor daarbij het correctiegedrag en mogelijke automation bias.
2 / 7. Integriteit & Rechtvaardigheid	Structurele interpretatiefouten bij bepaalde accenten	Bij een mogelijke uitrol na de pilot: signaleer en analyseer structurele fouten in spraakherkenning (met name bij accenten) en bespreek deze periodiek met 5.1.2i. Instrueer consulenten alert te zijn op interpretatiefouten en deze actief te corrigeren en terug te koppelen tijdens de pilot.
3. Beschikbaarheid	Verslaglegging ontbreekt door technische storing of mislukte opname	Neem dit scenario expliciet op in werkinstructies en trainingen, met duidelijke instructies om direct over te schakelen op handmatige verslaglegging. Onderzoek na de pilot de mogelijkheid van een auditieve waarschuwing bij uitval van een opname.
4. Rechtmatigheid	Overrapportage en onnodige verwerking.	Borg het gebruik van contextspecifieke rapportagemodellen, beperkt de modellen bijvoorbeeld tot afspraken, besluiten en actiepunten. Start de opname pas nadat informele bijpraatmomenten zijn afgerond en informeer deelnemers expliciet bij start van de opname. Houd de bewaartermijn van transcripten zo kort mogelijk en verplicht controle en aanpassing door de consulent vóór opname in het klantdossier.

4. Rechtmatigheid	Gebruik van gegevens voor andere doeleinden (function creep)	Borg doelbinding in de verwerkersovereenkomst en leg vast dat ieder nieuw doeleinde vooraf wordt getoetst op rechtmatigheid, proportionaliteit en subsidiariteit.
5. Rechten betrokkenen	Onvoldoende transparantie of effectieve uitoefening van rechten	Zorg voor informatievoorziening bestaande uit een mondelinge toelichting en doelgroepgerichte schriftelijke informatie (b.v. in een privacy statement of flyer). Hierin moet minimaal worden toegelicht: • Dat het gesprek wordt opgenomen met behulp van software • Dat de opname automatisch wordt omgezet in een rapportage die direct beschikbaar is • Dat de originele audio-opname direct wordt verwijderd na transcriptie en direct identificerende gegevens direct uit het transcript worden gehaald. Borg dat 5.1.2i als opslaglocatie bekend is bij medewerkers die inzage- en verwijderverzoeken behandelen.
5. Rechten betrokkenen	Klanten ervaren onvoldoende vrijwilligheid	Train consulenten expliciet op het gesprek over vrijwilligheid en opt-out, met aandacht voor de afhankelijke hulpverleningsrelatie.
6. Controleerbaarheid	Automation bias bij consulenten	Borg betekenisvolle menselijke controle door verplichte gezamenlijke review met de klant en evalueer naleving hiervan tijdens de pilot.
7. Rechtvaardigheid	Medewerkers voelen zich gedwongen tot deelname aan opgenomen overleggen	Leg vast dat het (incidenteel) niet instemmen met de inzet van 5.1.2i geen gevolgen heeft voor deelname aan overleggen, informatievoorziening of arbeidspositie. Informeer medewerkers individueel en transparant over doel en gebruik.
8. Verlies van controle	Onvoldoende grip op bewaartermijnen	Beperk bewaartermijnen van transcripten tijdens de pilot voor in ieder geval de interne overleggen en stel na afloop van de pilot definitieve bewaartermijnen vast en leg deze vast in de verwerkersovereenkomst.
8. Verlies van controle	Onvoldoende grip op taalmodelgebruik en resultaat voor het rapport	Leg in de verwerkersovereenkomst tussen Gemeente Leeuwarden en 5.1.2i vast dat 5.1.2i de gemeente vooraf informeert over wijzigingen in ingezette taalmodellen, ook als deze taalmodellen binnen dezelfde cloudomgeving wordt ingezet.
Overkoepelend	Onvoldoende vaardigheden en bewustzijn bij gebruikers	Voorzie voorafgaand aan gebruik in training gericht op het praktisch gebruik van 5.1.2i, kritisch beoordelen van AI-output, professionele verslagleggingsvaardigheden en het helder samenvatten van gesprekken tijdens het gesprek (zodat voor klant en AI-model duidelijk is wat belangrijke informatie is en geen interpretatieverschillen ontstaan).

4.2 Beoordeling en advies FG

<beoordeling en advies FG> Goed omschreven proces en de risico's en maatregelen zijn duidelijk, zorgvuldig en herkenbaar in kaart gebracht. Eén punt van aandacht: Uit de omschrijving van het doel, kan ik niet meegaan in de grondslag vanuit art 6 lid 1 onder c of e AVG. De grondslag voor de inzet van een transcribeertool bij de opname van gesprekken met als doel oa efficiëntie, kan niet anders dan gerechtvaardigd belang zijn en daarmee dus art. 6 lid 1 onder f AVG. Er zitten vervolgens voorwaarden aan die grondslag, die tijdens de uitvoering van de pilot kunnen worden gemeten: 1. Vaststellen gerechtvaardigd belang 2. Noodzakelijkheid toetsen 3. Belangenafweging uitvoeren (belang afwegen tegen privacy-impact betrokkenen)	
Datum: 28-01-2026	**Voorafgaande raadpleging AP nodig**: nee

Noot: De hierboven genoemde conclusies en aanbevelingen en het advies van de FG zijn gebaseerd op de informatie zoals in deze DEPIA is beschreven. Ga je hiervan afwijken? Dan is het nodig de DEPIA aan te vullen of te wijzigen (zie ook aandachtspunt 4 onder Tot slot). Vervolgens vindt een nieuwe beoordeling plaats.

Tot slot

Na de beoordeling en het advies van de FG vul je onderstaande tabel in. Als laatste volgt een beoordeling van de proceseigenaar. De proceseigenaar is de teamleider/manager die verantwoordelijk is voor het project/proces.

Wat is de startdatum van de verwerking?	<datum>

Beoordeling proceseigenaar

<laat de proceseigenaar hier zijn/haar oordeel over de DEPIA vermelden>

Aandachtspunten

1. **Verwerkersovereenkomst**: Heb je een verwerkersovereenkomst afgesloten of ga je dit nog doen? Bewaar de door beide partijen ondertekende verwerkersovereenkomst in 5.1.2i en in 5.1.2i bij het contract met de andere organisatie of de leverancier van een applicatie.
2. **Overeenkomst ketenpartner(s)**: Heb je een overeenkomst afgesloten met (een) ketenpartner(s)? Bewaar de door beide/alle partijen ondertekende overeenkomst (convenant, regeling, etc.) in 5.1.2i.
3. **Bijwerken register van verwerkingen**: Nieuwe verwerking? Of wijziging van een bestaande verwerking? Lever de nieuwe of gewijzigde informatie aan via 5.1.2i @leeuwarden.nl zodat we deze in het register van verwerkingen kunnen opnemen. Twijfel je? Vraag advies aan de Privacy Officer.
4. **Bewaren DEPIA**: Is je DEPIA goedgekeurd? 1) maak een zaak aan in 5.1.2i (tenzij je al een zaak hebt voor de pre-DEPIA), 2) vul datum en zaaknummer in op het voorblad, 3) bewaar de DEPIA in 5.1.2i, 4) geef het zaaknummer door aan 5.1.2i @leeuwarden.nl.
5. **Herbeoordeling DEPIA**: Iedere drie jaar moet je een herbeoordeling van de DEPIA uitvoeren. Dit is ook tussentijds nodig bij ingrijpende wijzigingen van een bestaande gegevensverwerking. Twijfel je of een herbeoordeling nodig is? Vraag advies aan de Privacy Officer.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	2, 3, 19, 20, 28
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 3, 4, 5, 6, 7, 8, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 28, 29, 30, 31, 32, 33, 34, 36, 37, 38

From: "5.1.2e" <5.1.2e@leeuwarden.nl>
Sent: 4/9/2024 6:53:12 AM +00:00
To: "5.1.2e" <5.1.2e@leeuwarden.nl>, "5.1.2e" <5.1.2e@leeuwarden.nl>
Cc: "5.1.2e" <5.1.2e@leeuwarden.nl>, 5.1.2i@leeuwarden.nl>
Subject: FW: Aanvulling DEPIA mbt data-ethiek defintieve versie vanuit FG C2311 7797

Goedemorgen!
Ik heb de aanvulling doorgenomen en het is zo een goede aanvulling op de DPIA die door 5.1.2e is opgesteld. Het document is ook in de 5.1.2i melding opgenomen, voor de zekerheid.
Wat er nu nog nodig is:
-5.1.2e geeft aan of hij akkoord is en of het document openbaar is of niet
-Datum van de definitieve versie is startdatum, deze graag invullen op het laatste blad van de aanvulling
-Startdatum + 3 jaar is datum van herziening, dan kijken we opnieuw naar de DPIA/DEPIA
-DPIA van 5.1.2e met deze aanvulling opslaan in 5.1.2i
-Zaaknummer aan 5.1.2i@leeuwarden.nl doorgeven, zodat we de datum van herziening ook kunnen monitoren.
Hartelijke groeten,
5.1.2e

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

From: '5.1.2e' <5.1.2e@leeuwarden.nl>
Sent: 6/11/2026 12:20:09 PM +00:00
To: '5.1.2e' <5.1.2e@leeuwarden.nl>
Cc: '5.1.2e' <5.1.2e@leeuwarden.nl>, '5.1.2e' <5.1.2e@leeuwarden.nl>, '5.1.2e' <5.1.2e@leeuwarden.nl>
Subject: FW: link/koppeling naar het register van verwerkingen

Hoi 5.1.2e,
Onderstaande ter info t.b.v. de overdracht. Het onderwerp heeft de aandacht binnen het team V&L en het is goed dat jullie t.z.t. even met elkaar kijken wat de stavaza is etc.
Groet, 5.1.2e.

Van: 5.1.2e
Verzonden: vrijdag 10 april 2026 11:10
Aan: 5.1.2e; 5.1.2e
Onderwerp: FW: link/koppeling naar het register van verwerkingen
Goedemorgen dames,
In aanvulling op de bijgevoegde mail van 5.1.2e.
Het zou fijn zijn als de volgende onderwerpen in de komende periode / maanden opgepakt kunnen worden:

- Het vastleggen van processen op de Engage werkwijze;
- Depia's: o.b.v. het pre Depia formulier checken of er Depia's opgesteld moeten worden en als dit het geval is dit in gang zetten en bepalen hoe we overzicht houden hierop en wie dit bijhoudt;
- Register van verwerkingen: willen jullie de generieke en V&L vermeldingen in het Excel overzicht (beide onder de tab Publieke Dienstverlening) doornemen, actualiseren en waar nodig zaken toevoegen, hoe houden we dit overzicht actueel en wie houdt dit bij namens V&L;
- Afstemmen met functioneel beheer m.b.t. verwerkersovereenkomsten en het algoritme register;
- Zijn we dan zo compleet of missen we nog iets?

Fijn dat jullie dit met elkaar verder oppakken! Hoor graag wat de uitkomst is van jullie acties en of jullie van mij nog iets nodig hebben op dit vlak.
Alvast bedankt,
5.1.2e

Van: 5.1.2e <5.1.2e@leeuwarden.nl>
Verzonden: dinsdag 17 maart 2026 16:22
Aan: 5.1.2e <5.1.2e@leeuwarden.nl>
Onderwerp: link/koppeling naar het register van verwerkingen
Hoi 5.1.2e
Hierbij de link naar het register van verwerkingen, zoals die op Leo staat: Register van verwerkingen.xlsx.
Ik hoop dat je zo toegang kunt krijgen. Anders is hij hier te vinden: Informatieveiligheid en privacy (AVG) - Digitale werkomgeving van jouw organisatie, onder het kopje "Gegevensverwerking" staat dan de link naar het verwerkingsregister.
Hartelijke groeten,

5.1.2e |Functionaris Gegevensbescherming
gemeente Leeuwarden, Vlieland, Terschelling, Ameland, Schiermonnikoog

E fg@leeuwarden.nl
T 5.1.2e | **M** 5.1.2e

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000, 8900 JA LEEUWARDEN
T 14 058 | www.leeuwarden.nl |

GLOBAL GOALS GEMEENTE

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1

From: "5.1.2e" <5.1.2e@leeuwarden.nl>
Sent: 3/20/2026 12:46:58 PM +00:00
To: "5.1.2e" <5.1.2e@leeuwarden.nl>, "5.1.2e" <5.1.2e@leeuwarden.nl>, "5.1.2e" <5.1.2e@leeuwarden.nl>
Cc: "5.1.2e" <5.1.2e@leeuwarden.nl>
Subject: FW: link/koppeling naar het register van verwerkingen

Goedemiddag allen,
Willen jullie, zoals besproken in het overleg met 5.1.2e dit onderwerp agenderen voor jullie BB overleg (incl. 5.1.2e)?
Het zou fijn zijn als de volgende onderwerpen dan besproken kunnen worden:

- Depia's: welke hebben we onderhanden (hebben we overzicht en wie houdt dit bij namens het BB), welke zijn specifiek van het BB (als proces eigenaar), welke moeten (op termijn) overgedragen worden aan andere proces eigenaren;
- Register van verwerkingen: willen jullie de generieke en BB vermeldingen in het Excel overzicht doornemen, actualiseren en waar nodig zaken toevoegen, hoe houden we dit overzicht actueel en wie houdt dit bij namens het BB;
- Hebben we verder nog wat te doen of nodig als het gaat om gegevensbescherming?

Fijn dat jullie dit met elkaar verder oppakken! Hoor graag wat de uitkomst is van jullie bespreking en of jullie van mij nog iets nodig hebben op dit vlak.
Alvast bedankt,
5.1.2e

Van: 5.1.2e
Verzonden: dinsdag 17 maart 2026 16:22
Aan: 5.1.2e
Onderwerp: link/koppeling naar het register van verwerkingen
Hoi 5.1.2e
Hierbij de link naar het register van verwerkingen, zoals die op Leo staat: Register van verwerkingen.xlsx.
Ik hoop dat je zo toegang kunt krijgen. Anders is hij hier te vinden: Informatieveiligheid en privacy (AVG) - Digitale werkomgeving van jouw organisatie, onder het kopje "Gegevensverwerking" staat dan de link naar het verwerkingsregister.
Hartelijke groeten,

5.1.2e |Functionaris Gegevensbescherming
gemeente Leeuwarden, Vlieland, Terschelling, Ameland, Schiermonnikoog

E fg@leeuwarden.nl
T 5.1.2e | **M** 5.1.2e

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000, 8900 JA LEEUWARDEN
T 14 058 | www.leeuwarden.nl |

GLOBAL GOALS GEMEENTE

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1

Gemeente Leeuwarden
Rapportage
Data Protection Impact Assessment
Meldpunt Overlast Leeuwarden (MOL)

Classificatie: Vertrouwelijk
Versie: 1.0 - Definitief
Datum: 03-03-2024

Projectdetails

Projectnaam	DPIA ketenregiesysteem en proces
Opdrachtgever	Gemeente Leeuwarden
Opdrachtreferentie	GELWD-2023.2

Versiegeschiedenis en distributie

Auteur(s)	Versie	Datum	Beschrijving
5.1.2e	0.1 – 0,4	25-11-2023 – 03-12-2023	Uitwerken 1e concept
5.1.2e	0.5	04-12-2023	Aanvullingen op 1e concept
5.1.2e	0.6	07-12-2023	Aanvulling op vorige versie
5.1.2e	0.7	07-12-2023	Review
5.1.2e	0.8	08-12-2023	Verwerken review en toevoegen managementsamenvatting + opleveren concept
5.1.2e	1.0	28-02-2024 03-03-2024	Klantfeedback verwerken en nieuwe versie opleveren

Vertrouwelijkheid

Dit document is opgesteld voor de gemeente Leeuwarden. Dit document bevat eigendomsrecht en gevoelige informatie. Duplicatie, distributie, in gebruik, deels of in zijn geheel, vereist schriftelijke toestemming van de gemeente Leeuwarden.

Over Waker Cyber Security

Waker Cyber Security is een jong en modern securitybedrijf opgericht medio 2021 in Groningen. Onze Noordelijke roots bepalen voor een groot deel onze visie, onze waarden en onze doelen. Onze diensten liggen op het snijvlak tussen (cyber) security en privacy, van advies tot juridische kaders, van menselijk gedrag tot technische zwakheden. Security en privacy zitten in ons hart. Vanuit die passie werken we samen met klanten, relaties en partners aan het bereiken en behouden van passende bescherming en bewaking en staan we klaar om te helpen zodra een (digitale) dijk breekt.

Inhoudsopgave

1. MANAGEMENTSAMENVATTING 4

2. INLEIDING 5

2.1 DPIA-AANPAK 5
2.2 PROCES/SCOPE 5
2.3 LEESWIJZER 5

3. CONTEXT VAN DE VERWERKING 6

3.1 OVERZICHT VAN PERSOONSGEGEVENS 6
3.2 VERWERKINGSMIDDELEN 7
3.3 BIJ DE VERWERKING BETROKKEN PARTIJEN 7

4. TOEPASSELIJK JURIDISCH EN BELEIDSMATIG KADER 8

5. PRIVACY BEGINSELEN 9

5.1 DATAMIMIMALISATIE 9
5.2 GEGEVENSKWALITEIT 9
5.3 RECHTEN VAN BETROKKENEN 10
5.4 DATARETENTIE 10
5.5 AFSPRAKEN MET DERDE PARTIJEN EN LEVERANCIERS 11
5.6 VERANTWOORDING 12
5.7 BEVEILIGING 13
5.8 OVERIGE GETROFFEN MAATREGELEN 13

BIJLAGE A: BETROKKEN PARTIJEN EN GEÏNTERVIEWDE FUNCTIONARISSEN. 15

1. Managementsamenvatting

Gemeente Leeuwarden heeft een project uitgevoerd voor het implementeren van een nieuw ketenregiesysteem – 5.1.2i - om overlastmeldingen in te registreren en af te handelen, waaronder geluidsoverlast, zwerfafval, en overlast door personen. Hierin vindt dus ook de verwerking van persoonsgegevens plaats ten behoeve van de werkzaamheden. Om te beoordelen of het MOL-proces en het gebruik van het ketenregiesysteem voldoen aan de eisen uit geldende privacy wet- en regelgeving en om eventuele risico's van en verbetermaatregelen voor de verwerking te identificeren, heeft Waker Cyber Security een Data Protection Impact Assessment (DPIA) uitgevoerd gedurende de periode van april tot en met september 2023.

Uit het geheel van de verstrekte documentatie en informatie, in combinatie met daarover gevoerde gesprekken en systeemdemonstratie, ontstaat het beeld dat de beveiliging en bescherming van persoonsgegevens gedurende het implementatietraject van 5.1.2i aantoonbaar serieus zijn genomen en dat de gemeente dit vast wil blijven houden.

Als resultaat van de DPIA zijn een aantal aanvullende maatregelen naar voren gekomen om de privacyrisico's tot een acceptabel niveau te brengen. De belangrijkste restrisico's en bijbehorende specifieke verbetermaatregelen zijn opgenomen op de volgende pagina:

Risico	**Impact op betrokkenen**	**Verbetermaatregel**
Betrokkenen worden onvoldoende geïnformeerd over de verwerking van persoonsgegevens in het kader van het melden van overlast.	Midden	1. Voeg een alinea over de verwerking in het kader van het melden van overlast toe aan het privacystatement op de website.
De export van gemigreerde gegevens wordt langer bewaard dan noodzakelijk.	Hoog	1. Vernietig het tijdelijke exportbestand zo spoedig mogelijk na validatie dat de migratie succesvol is uitgevoerd. 2. Zie toe op verwijdering van de gegevens uit 5.1.2i zodra de migratie is afgerond.
Verantwoordelijkheden en verplichtingen zijn niet up-to-date vastgelegd.	Midden	1. Rond de procesbeschrijving(en) af, waarin de uitgangspunten van het behandelen van overlastmeldingen (met behulp van 5.1.2i) operationeel zijn uitgewerkt en vertaald naar praktische werkwijzen; 2. Communiceer de inhoud naar betrokken medewerkers en instrueer hen in de naleving; 3. Voer controles uit op de naleving; 4. Herijk de inhoud bij wijzigingen, incidenten of aan de hand van bevindingen uit controles.

2. Inleiding

Gemeente Leeuwarden heeft een project uitgevoerd voor het implementeren van een nieuw ketenregiesysteem om overlastmeldingen in te registreren en af te handelen, waaronder geluidsoverlast, zwerfafval, en overlast door personen. Het doel van dit proces is om de leefbaarheid in de gemeente te verbeteren door snel en effectief te reageren op meldingen van burgers. Bij het melden van overlast via het gemeentelijke meldpunt worden verschillende persoonsgegevens verzameld en verwerkt in het nieuwe systeem: 5.1.2i van de leverancier 5.1.2i. De afdeling MOL gebruikt 5.1.2i als meld- en regiesysteem, om de registratie van overlastmeldingen en daartoe behorende gegevens bij te houden.

2.1 DPIA-aanpak

Om te beoordelen of het systeem voldoet aan de eisen uit geldende privacy wet- en regelgeving en om eventuele risico's van de verwerking te identificeren, voert Waker Cyber Security een Data Protection Impact Assessment (DPIA) uit aan de hand van de volgende stappen:

- Documentatie onderzoek;
- Interviews en DPIA-workshop(s) ketenregiesysteem;
- Beoordeling en validatie;
- Rapportage;
- Presentatie resultaten.

2.2 Proces/scope

- Het meldproces en de administratieve handeling van overlastmeldingen door MOL, met gebruikmaking van 5.1.2i;
- Deze DPIA strekt zich niet uit over de beveiliging en eventuele risico's van de volledige door de Gemeente Leeuwarden gefaciliteerde IT-infrastructuur. Elementen die relevant zijn voor MOL komen uiteraard wel aan bod.

2.3 Leeswijzer

Hierna volgt een inhoudelijke uitwerking van de verwerkingscontext en processen, het juridisch en beleidsmatig kader; de invulling van privacy principes, gesignaleerde risico's en daarbij behorende aanbevelingen. Dit is per privacy principe in een korte risico- en aanbevelingstabel opgenomen. Risico's die door middel van maatregelen zijn geadresseerd, worden doorgestreept, zoals:

1. ~~Gegevens worden verwerkt zonder welbepaald doel en zonder grondslag (onrechtmatige verwerking),~~

Een overzicht van overige voor de verwerking getroffen maatregelen is opgenomen onder hoofdstuk 5.8.

Risico's waarvoor wij een specifieke aanbeveling of maatregel voorstellen, zijn niet doorgestreept, maar weergegeven als volgt:

1. Gegevens worden blootgesteld aan inzage of manipulatie door onbevoegden.

Hier is vervolgens een aanbeveling of maatregel aan gekoppeld.

3. Context van de verwerking

Onderhavige DPIA is gericht op het proces van het melden van overlast in de openbare ruimte, zoals gehanteerd door de gemeente Leeuwarden. Het meldpunt stelt burgers in staat om diverse vormen van overlast te melden, waaronder geluidsoverlast, zwerfafval, en overlast door personen. Het doel van dit proces is om de leefbaarheid in de gemeente te verbeteren door snel en effectief te reageren op meldingen van burgers. Bij het melden van overlast via het gemeentelijke meldpunt worden verschillende persoonsgegevens verzameld. Dit kan onder meer de naam, het adres, en contactgegevens van de melder omvatten, evenals specifieke details over de gemelde overlast en bijvoorbeeld foto's of video's. Het is belangrijk om te benadrukken dat de verzameling van deze gegevens beperkt blijft tot wat strikt noodzakelijk of anderszins ter zake dienend is voor de behandeling van de melding.

De verzamelde persoonsgegevens worden gebruikt voor het beoordelen en aanpakken van de gemelde overlast. Dit omvat het registreren van de melding, het eventueel opnemen van contact met de melder voor aanvullende informatie, en het doorgeven van de melding aan de relevante afdelingen of externe partijen voor verdere actie. Alle verwerkingsactiviteiten worden uitgevoerd met de nodige zorg voor privacy en beveiliging van de gegevens. Bij de verwerking van gegevens in het kader van het meldpunt overlast zijn verschillende partijen betrokken. Dit omvat de gemeentelijke afdelingen die verantwoordelijk zijn voor de behandeling van de meldingen, eventuele externe organisaties die betrokken zijn bij de aanpak van specifieke soorten overlast, en natuurlijk de burgers die de meldingen doen.

De primaire doelstelling van de gegevensverwerking in het kader van het meldpunt overlast is het effectief aanpakken van overlast in de openbare ruimte. Dit omvat het identificeren van de aard en locatie van de overlast, het communiceren met de melder indien nodig, en het coördineren van de respons van de gemeente of samenwerkende instanties. Het uiteindelijke doel is het verbeteren van de leefbaarheid en veiligheid in de gemeente.

Binnen het meldpunt overlast worden personen over wie een melding wordt gedaan aangemerkt als 'beklaagden', terwijl de personen die de melding doen worden aangeduid als 'melders'. Meldingen kunnen op diverse manieren worden gedaan, zoals via het formulier op de website, per e-mail, telefoon of andere methoden. Na ontvangst van een melding wordt deze vastgelegd in het meldsysteem genaamd 5.1.2i, dat wordt afgenomen van de leverancier 5.1.2i. 5.1.2i voldoet aan de eisen van ISO27001 en is hiervoor gecertificeerd. De leverancier voert ook periodiek pentesten en code reviews uit op de applicatie om de veiligheid te waarborgen. Afspraken over de verwerking en bescherming van persoonsgegevens zijn vastgelegd in een verwerkersovereenkomst, gebaseerd op het VNG-model, dat is afgesloten door de gemeente.

3.1 Overzicht van persoonsgegevens

Type persoonsgegevens	Categorieën betrokkenen	Verwerkingsdoeleinde(n)
• Naam van de melder. • Adres van de melder. • Telefoonnummer van de melder. • E-mailadres van de melder. • Locatie van de overlast. • Datum en tijdstip van de overlast.	• Burgers: • Personen die overlast veroorzaken (beklaagde) • Personen die overlast melden (melder)	Gegevens worden verzameld om de melding van sociale overlast adequaat te kunnen behandelen en opvolgen.

• Omschrijving van de overlast. • Naam van de beklaagde (indien bekend). • Adres van de beklaagde (indien bekend). • Overige kenmerken die de beklaagde kunnen identificeren. • Eventuele foto's, video's of documenten ter ondersteuning van de melding. • E-mailadressen van medewerkers.	• Medewerkers (als gebruikers van het systeem)	

3.2 Verwerkingsmiddelen

De gegevens worden verwerkt in 5.1.2i, het regiesysteem. Verder wordt gebruik gemaakt van e-mail, apparatuur en IT-infrastructuur zoals gefaciliteerd door de gemeente Leeuwarden, waaronder ook de website van de gemeente en GIS, het gemeentelijke informatiesysteem.

3.3 Bij de verwerking betrokken partijen

Bij de verwerking van gegevens in het kader van het meldpunt overlast zijn de volgende partijen betrokken:

- **Meldpunt Overlast Leeuwarden**: De afdeling binnen de gemeente die verantwoordelijk is voor de behandeling van de meldingen;
- **Leverancier van het Meldsysteem**: 5.1.2i, die het meldsysteem 5.1.2i levert en onderhoudt, en verantwoordelijk is voor de beveiliging en bescherming van de daarin opgeslagen gegevens;
- **Melders**: Burgers die meldingen van overlast doen;
- **Beklaagden**: Personen over wie een melding van overlast wordt gedaan;
- **Externe Organisaties**: Eventuele externe organisaties die betrokken zijn bij de aanpak van specifieke soorten overlast, zoals politie, gezondheidsdiensten of sociale diensten, te weten;;
  - Politie Noord Nederland (basisteam Leeuwarden);
  - Wijkteams (Amaryllis);
  - De woningcorporaties Elkien en Woonfriesland);
  - GGD-Fryslân;

Gemeente Leeuwarden is Verwerkingsverantwoordelijke voor onderhavige verwerking. De leverancier van 5.1.2i, 5.1.2i, treedt voor de gemeente Leeuwarden op als Verwerker.
De betrokkenen zijn: melders, beklaagden en medewerker.

4. Toepasselijk juridisch en beleidsmatig kader

De doelen en grondslagen voor de verwerking, met inbegrip van de noodzakelijkheid en evenredigheid van de verwerking moeten worden bepaald door de gemeente Leeuwarden. Het is belangrijk om te vermelden dat reeds aanwezige grondslagen en verwerkingsdoeleinden, noodzakelijkheid en evenredigheid niet zijn gewijzigd door de vervanging van het regiesysteem. De volgende verwerkingsdoeleinden kunnen worden geïdentificeerd voor het gemeentelijke meldpunt overlast:

- **Registratie van Meldingen**: Het verzamelen en vastleggen van details over de gemelde overlast, inclusief informatie over de melder en de beklaagde.
- **Communicatie**: Het onderhouden van communicatie met de melder voor aanvullende informatie of updates over de afhandeling van de melding.
- **Coördinatie van Respons**: Het doorgeven van de melding aan relevante afdelingen of externe partijen voor verdere actie.
- **Veiligheid en Handhaving**: Het gebruiken van de verzamelde gegevens voor het verbeteren van de openbare orde en veiligheid binnen de gemeente.

Op grond van art. 172 Gemeentewet, is de burgemeester belast met het handhaven van de openbare orde. Dit artikel luidt als volgt:

1. De burgemeester is belast met de handhaving van de openbare orde.
2. De burgemeester heeft het bevel over de Politie.
3. De burgemeester is bevoegd in het belang van de openbare orde bevelen te geven.

Bovenstaande geeft de burgemeester en daarmee de gemeente de bevoegdheid om actie te ondernemen in situaties van overlast in de openbare ruimte. Om de openbare orde effectief te kunnen handhaven, moet informatie worden verzameld, waaronder ook meldingen van overlast. Dit wordt gedaan door de afdeling MOL. Het aannemen en behandelen van meldingen van overlast is dus onderdeel van de verantwoordelijkheden van de gemeente in het kader van de handhaving van de openbare orde. De verwerking zoals die in de praktijk (en met behulp van 5.1.2i) wordt uitgevoerd, is nodig om dit te bewerkstelligen. De verwerkingsgrondslag valt hiermee onder art. 6 lid 1 sub e AVG jo. art. 172 Gemeentewet.[1]

Daarnaast is de wijze waarop dit door de mogelijkheden die 5.1.2i biedt, te realiseren op een manier die meer rekening houdt met de rechten en belangen van betrokkenen (en daarmee minder ingrijpend is), dan voorheen het geval was, mits de beheersingsprocessen hierop zijn ingericht. Vóór de implementatie van 5.1.2i, werd gebruikt van het systeem 5.1.2i, maar dat was niet specifiek gericht op zaak- of casusgericht werken en sloot daarmee niet helemaal aan op de wensen en praktijk van MOL.

Mogelijke risico's		**Mogelijke impact**
Juridisch en beleidsmatig kader	~~1. Gegevens worden verwerkt zonder welbepaald doel en zonder grondslag (onrechtmatige verwerking),~~ 2. ~~Gegevens worden gebruikt voor andere doelen dan waarvoor ze zijn verkregen (doelbinding);~~	~~Hoog~~ ~~Hoog~~
Aanbeveling:	**Verantwoordelijke**	**Prioriteit**
N.v.t.	N.v.t.	N.v.t.

[1] Sub e van artikel 6 lid 1 AVG bevat de grondslag: *de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;*

5. Privacy beginselen

5.1 Datamimimalisatie

In hoeverre de verwerkte gegevens zich beperken tot dat wat noodzakelijk en/of ter zake dienend is, dient primair te worden bepaald aan de hand van de verwerkingsdoelen.
Deze doeleinden zijn in lijn met de algemene doelstelling van het meldpunt om de leefbaarheid en veiligheid in de gemeente te verbeteren, terwijl tegelijkertijd de privacy van de betrokkenen wordt beschermd. De vastlegging van informatie in 5.1.2i en gedurende het proces is beperkt tot dat wat noodzakelijk en ter zake dienend is ter uitvoering van de werkzaamheden van MOL.

Tijdens de migratie naar 5.1.2i een verificatie- en validatieslag plaatsgevonden op de noodzaak van informatie. Dit heeft ertoe geleid dat informatie die niet langer noodzakelijk en ter zake dienend was, niet is overgenomen in 5.1.2i.

Het is belangrijk om te benadrukken dat de verzameling van deze gegevens beperkt blijft tot wat strikt noodzakelijk of anderszins ter zake dienend is voor de behandeling van de melding. Hieronder vallen ook foto's of video's. Hoewel hieruit mogelijk meer gegevens af te leiden zijn dan een melder in reguliere zin dient in te vullen via het meldformulier, is deze informatie uiterst relevant voor het beoordelen van overlastmeldingen, de ernst daarvan, en het aan de hand daarvan afstemmen of escaleren met andere afdelingen of partijen. De beelden worden op eenzelfde wijze beschermd als andere persoonsgegevens en ook enkel gebruikt voor de doeleinden zoals hierboven beschreven,

Mogelijke risico's		**Mogelijke impact betrokkenen**
Dataminimalisatie	~~Er worden meer gegevens verwerkt dan noodzakelijk is ter verwezenlijking van het verwerkingsdoel (dataminimalisatie);~~	Hoog
Aanbeveling:	**Verantwoordelijke**	**Prioriteit**
N.v.t.	N.v.t.	N.v.t.

5.2 Gegevenskwaliteit

Gegevenskwaliteit en dan met name de juistheid, volledigheid en integriteit van gegevens is belangrijk voor de werkzaamheden van MOL. Hiervoor wordt gewerkt met informatie die burgers zelf aanleveren, bij het doen van de melding. Hoe uitgebreider en volledige de informatie over een overlastsituatie, des te beter is het voor MOL mogelijk om hiermee aan de slag te gaan. Dit is echter afhankelijk van de juiste en volledige aanlevering door melder. Als hier onvolkomenheden of onjuistheden voorkomen, kan dit mogelijk negatieve gevolgen hebben voor betrokken personen. Meer specifiek kan dit leiden tot een langere of intensere overlastsituatie. Dit wordt in de praktijk doorgaans snel gesignaleerd, omdat de medewerkers van MOL regelmatig contact hebben met de melders en eventuele betrokken ketenpartners, om vragen of onduidelijkheden te bespreken en recht te zetten. Verder zijn in 5.1.2i de nodige beveiligingsmaatregelen getroffen om onbevoegde inzage of manipulatie te voorkomen, zie daarvoor paragraaf 5.5.

Mogelijke risico's		**Mogelijke impact betrokkenen**
Gegevenskwaliteit	~~1. Gegevens worden blootgesteld aan inzage of manipulatie door onbevoegden;~~ ~~2. Gegevens zijn mogelijk niet volledig~~	~~Hoog~~ ~~Middel~~
Aanbeveling:	**Verantwoordelijke**	**Prioriteit**

n.v.t.	n.v.t.	**n.v.t.**

5.3 Rechten van betrokkenen

Het faciliteren van de uitoefening van rechten van betrokkenen ten aanzien van hun persoonsgegevens ligt bij de gemeente Leeuwarden. De gemeente Leeuwarden heeft hiertoe procedures opgesteld en processen ingericht. Indien een betrokkene zich met een verzoek meldt bij MOL, dan zullen zij de privacyfunctionaris(sen) van de gemeente Leeuwarden op de hoogte stellen van het verzoek en het verzoek daarna overdragen. Met 5.1.2i is in de afgesloten verwerkersovereenkomst vastgelegd dat zij alle medewerking verlenen om uitvoering te geven aan een verzoek van een betrokkene. Verder licht de gemeente Leeuwarden de verwerking en bescherming van persoonsgegevens toe middels een privacyverklaring op de website. Deze voldoet aan de hiervoor geldende eisen, echter ontbreekt hierin een alinea over het melden van overlast, hier kan dus verbetering worden bewerkstelligd.

Mogelijke risico's		**Mogelijke impact betrokkenen**
Rechten van betrokkenen	~~1. Betrokkenen worden niet in staat gesteld hun rechten uit te oefenen;~~ 2. Betrokkenen worden onvoldoende geïnformeerd over de verwerking van persoonsgegevens in het kader van het melden van overlast.	~~Hoog~~ Midden
Aanbeveling:	**Verantwoordelijke**	**Prioriteit**
Voeg informatie over de verwerking in het kader van het melden van overlast toe aan op de website.	Privacy Officer/FG i.c.m. communicatie	N.v.t.

5.4 Dataretentie

Het oude systeem 5.1.2i wordt uitgefaseerd en alle daarin opgenomen data wordt gemigreerd. Deze DPIA richt zich echter alleen op het waarvan MOL gebruik maakt en niet op de volledige inhoud van 5.1.2i. Om gegevens uit te migreren van 5.1.2i naar 5.1.2i, is een export gemaakt uit 5.1.2i, die wordt ingeladen in 5.1.2i. Dit gebeurt in nauwe samenwerking tussen Leeuwarden en 5.1.2i. De betreffende export blijft enige tijd 'lokaal' staan, totdat de migratie is gevalideerd. Als onderdeel van het migratieproces, zal deze dataset moeten worden verwijderd nadat is gevalideerd dat de migratie is geslaagd en dat de data goed is overgekomen. Hierop moet door betrokken adviseurs en analisten worden toegezien. Hierbij moet ook rekening worden gehouden met het verwijderen van de gegevens uit 5.1.2i,

Ten aanzien van het bewaren van gegevens geldt het volgende:

- Lopende meldingen worden bewaard zolang deze actief zijn. Na sluiting van een melding worden de gegevens 5 jaar bewaard;
- Tijdens de migratie van naar 5.1.2i, zijn alleen meldingen gemigreerd die minder dan 5 jaar afgesloten zijn. Meldingen die langer dan 5 jaar gesloten zijn, zijn niet gemigreerd.
- De retentietermijn wordt in 5.1.2i technisch afgedwongen als volgt:
  - Zodra een melding wordt gesloten, wordt deze gearchiveerd. Dit betekent dat de melding niet langer zonder meer kan worden gewijzigd en pas dan als de beheerder met 5.1.2i contact heeft gehad over het opnieuw openzetten.

– Na verstrijken van de termijn van 5 jaar, worden de gegevens automatisch verwijderd.

Mogelijke risico's		**Mogelijke impact betrokkenen**
Dataretentie	De export van gemigreerde gegevens wordt langer bewaard dan noodzakelijk	Hoog
Aanbeveling:	**Verantwoordelijke**	**Prioriteit**
1. Vernietig het tijdelijke exportbestand zo spoedig mogelijk na validatie dat de migratie succesvol is uitgevoerd. 2. Zie toe op verwijdering van de gegevens uit 5.1.2i zodra de migratie is afgerond.	Projectgroep: Informatiearchitect, informatieadviseur & betrokken leveranciers.	Dient te hebben plaatsgevonden voor eind Q1 2024.

5.5 Afspraken met derde partijen en leveranciers

Met de leverancier 5.1.2i is ten behoeve van 5.1.2i een verwerkersovereenkomst overeengekomen, op basis van het VNG-format dat door de gemeente Leeuwarden standaard wordt gehanteerd. 5.1.2i heeft zich gedurende deze beoordeling zeer meewerkend opgesteld. De ingevulde overeenkomst is getoetst op de vanuit de AVG verplichte elementen door de gemeente Leeuwarden. Er is geen sprake van doorgifte van persoonsgegevens naar partijen buiten de Europese Unie of anderszins landen die naar AVG-standaarden niet beschikken over een 'passend c.q. adequaat beveiligingsniveau' ter bescherming van persoonsgegevens. In de verwerkersovereenkomst die door de gemeente Leeuwarden is afgedwongen zijn verplichtingen vastgelegd over de toepasselijkheid en naleving van beveiligingseisen, het (laten) uitvoeren van periodieke audits, de melding van datalekken, de locatie van verwerking en ondersteuning bij de afhandeling van verzoeken van betrokkenen. Naast de verwerkersovereenkomst is er met 5.1.2i een 5.1.2i Level Agreement afgesloten over het te verwachten niveau van dienstverlening, support en back-ups en is voorzien in exit-afspraken met behulp van een escrowovereenkomst.

De beveiliging van (persoons)gegevens in 5.1.2i vindt plaats volgens algemeen erkende beveiligingsnormen, meer specifiek ISO27001 en NEN7510. De leverancier beschikt over een geldige certificering voor beide normen. Als onderdeel van de DPIA is een beoordeling gedaan op de toereikendheid van het certificaat in combinatie met de bij de certificering behorende Verklaring van Toepasselijkheid. Verder zijn resultaten ingezien van een recent door een onafhankelijke partij uitgevoerde penetratietest en codereview op 5.1.2i. Eventueel gesignaleerde risico's zijn opgevolgd. De verwerkte informatie wordt opgeslagen op servers in de EU. De applicatie faciliteert het gebruik van multifactor authenticatie. Ook is er in het ontwerp van de applicatie bewust gekozen voor beperktere functionaliteit om overbodige verwerking en opslag van gegevens te voorkomen.

Uit het geheel van de door 5.1.2i en gemeente Leeuwarden verstrekte documentatie en informatie, in combinatie met daarover gevoerde gesprekken, ontstaat het beeld van een partij die de beveiliging en bescherming van persoonsgegevens aantoonbaar serieus neemt. Extra zekerheid over de maatregelen kan eventueel nog worden verkregen middels het opvragen of

laten opstellen van een assurance verklaring over de werking van maatregelen (bijvoorbeeld conform de ISAE 3000 – standaard.) Dit is gelet op de huidige situatie niet noodzakelijk.

Mogelijke risico's		**Mogelijke impact betrokkenen**
Beveiliging/ Afspraken met derde partijen en leveranciers	~~1. De bij de verwerking ingeschakelde partijen nemen de beveiliging van persoonsgegevens niet serieus;~~	Hoog
Aanbeveling:	**Verantwoordelijke**	**Prioriteit**
N.v.t.	N.v.t.	N.v.t.

5.6 Verantwoording

Als onderdeel van uitvoer van de werkzaamheden wordt gerapporteerd aan de Manager Veiligheidsdomein. Op de verwerking van persoonsgegevens wordt toezicht gehouden door de FG van de gemeente. Deze DPIA dient daarnaast als verantwoording over de verwerking en getroffen maatregelen. Ten aanzien van rollen en verantwoordelijkheden, wordt in de nieuwe procesbeschrijving(en) ook aandacht besteed aan de betrokken rollen en verantwoordelijkheden, van zowel het primaire proces, als bijvoorbeeld het functioneel beheer. Dit is op dit moment nog niet voltooid, dus levert dit een risico op. De verwachting is dat dit op korte termijn wordt opgelost, als stok achter de deur hebben wij daarom opgenomen dat dit voor eind Q1 gereed moet zijn.

Verder besteedt het team van MOL in werkoverleggen aandacht aan de zorgvuldige omgang met informatie en in het bijzonder persoonsgegevens.

Mogelijke risico's		**Mogelijke impact betrokkenen**
Verantwoording	1. Verantwoordelijkheden en verplichtingen zijn niet up-to-date vastgelegd; 2. ~~Er wordt geen verantwoording afgelegd over de verwerking en bescherming van persoonsgegevens~~.	Midden
Aanbeveling:	**Verantwoordelijke**	**Prioriteit**
1. Rond de procesbeschrijving(en) af, waarin de uitgangspunten van het behandelen van overlastmeldingen (met behulp van 5.1.2i) operationeel zijn uitgewerkt en vertaald naar praktische werkwijzen; 2. Communiceer de inhoud naar betrokken medewerkers en instrueer hen in de naleving; 3. Voer controles uit op de naleving; 4. Herijk de inhoud bij wijzigingen, incidenten of aan de hand van bevindingen uit controles.	Procesanalist	**Punt 1 en 2**: afgerond voor eind Q12024. **Punt 3**: uitvoeren voor eind Q2 2024. **Punt 4**: uitvoeren in Q3 2024.

5.7 Beveiliging

- De gemeente Leeuwarden heeft beleid en procedures ingericht om te voldoen aan de AVG en ook de Baseline Informatiebeveiliging Overheid. Tijdens de selectie van de leverancier is door de gemeente Leeuwarden in het inkooptraject ook getoetst op deze elementen.
- Voor het melden en afhandelen van datalekken en bijvoorbeeld verzoeken van betrokkenen, wordt aangesloten bij de door de gemeente Leeuwarden geïmplementeerde processen en vastgestelde beleidsstukken en procedures.
- Voor de toegang tot 5.1.2i wordt het gebruik van multifactor authenticatie afgedwongen. Gemeente Leeuwarden hanteert voor de toegang tot en in 5.1.2i een gelaagd autorisatiebeleid om toegang te verlenen tot de informatie. Accounts worden gekoppeld aan een individu (ook beheeraccounts), waarna dit account een specifieke rol krijgt toebedeeld, in lijn met de werkzaamheden die de medewerker verricht – zo is onderscheid tussen beheerder en een 'gewone' gebruiker. Aan de hand van de toegewezen rol, krijgt de betreffende gebruiker toegang tot bepaalde dossiers en onderwerpen. Dit geeft toegang tot die specifieke dossiers en bijvoorbeeld lees- of schrijfrechten.
- De controle van autorisaties en gebruikersaccounts wordt op dit moment ingericht en zal met een vaste frequentie moeten plaatsvinden. 5.1.2i registreert alle gebruikershandelingen die in het systeem plaatsvinden, van inlog tot raadpleging van of mutaties in specifieke casus. Dit biedt de mogelijkheid om deze activiteitenlogging te raadplegen en te (doen) controleren op bijzonderheden. Op dezelfde wijze waarop gemeente Leeuwarden een periodieke autorisatiecontrole moet uitvoeren, zal ook de logging moeten worden gecontroleerd.
- Op het moment van schrijven wordt voor MOL gewerkt aan een nieuwe procesbeschrijving. Deze nieuwe beschrijving moet de oude vervangen en daarmee aansluiten bij de werkwijze zoals die nu met gebruikmaking van 5.1.2i plaatsvindt.

5.8 Overige getroffen maatregelen

Specifieke maatregelen zijn reeds opgenomen in de uitwerking in hoofdstukken 4 en 5. Hieronder is een overzicht van de overige genomen maatregelen waarmee de in hoofdstuk 4 en 5 genoemde risico's zijn geadresseerd.

Beschrijving Maatregel	**Inhoud Maatregel**	**Verantwoordelijke**	**Aanwezig**
Functioneel beheer	Houd dagelijks toezicht op het systeem om ervoor te zorgen dat het naar behoren functioneert en om eventuele problemen op te lossen.	Leverancier en beheerder.	Ja, is onderdeel van de processen van gemeente Leeuwarden en 5.1.2i.
Autorisatie-verdeling	Draag zorg voor het opzetten en bijwerken van een rol gebaseerd toegangscontrolesysteem.	MOL i.c.m. functioneel beheer.	Ja, is onderdeel van de processen van gemeente Leeuwarden.
Autorisatie-controle	Voer regelmatige controle van de toegangsrechten van gebruikers uit om ervoor te zorgen dat ze nog steeds passend zijn en dat er geen ongeautoriseerde toegang is.	Functioneel beheer, IT-beheerorganisatie.	Ja, is onderdeel van de processen van gemeente Leeuwarden.

Logging-controle	Organiseer regelmatige controle van logs om eventuele ongebruikelijke, niet-legitieme of verdachte activiteiten te identificeren.	IT-beheerorganisatie	Ja, is onderdeel van de processen van gemeente Leeuwarden.
Beveiligings- en AVG Controles	Voer een jaarlijkse controle uit op naleving van AVG, beveiligingsbeleid en andere relevante wetgeving.	FG/PO/CISO	Ja, Is onderdeel van de processen van gemeente Leeuwarden.
Training	Organiseer een training van alle gebruikers in veilige werkwijzen bij onboarding en daarna minstens één keer per jaar.	FG/PO i.s.m. MOL	Ja, krijgt aandacht in werkoverleggen en het inwerkproces. De nieuwe procesbeschrijving moet hierbij helpen.
Bewust-wording	Organiseer een opfrismoment privacy en security als onderdeel van werkoverleggen	FG/Privacy Officer	Ja, krijgt aandacht in werkoverleggen/inwerk proces
Back-ups	Verzorg periodieke back-ups van alle gegevens in 5.1.2i.	Leverancier	Ja, is onderdeel van de dienstverlening door 5.1.2i
Data minimalisatie	Periodiek controleren of er alleen noodzakelijke gegevens worden verzameld en bewaard.	MOL	Ja, is onderdeel van processen gemeente Leeuwarden.
Encryptie	Borg het versleutelen van alle verzonden of opgeslagen gegevens, incl. versleutelde e-mail	Leverancier en gemeente Leeuwarden	Ja, is onderdeel van de dienstverlening door 5.1.2i Ja, is onderdeel van maatregelen gemeente Leeuwarden.
Regelmatige updates	Installeer regelmatige updates van het systeem om het te beschermen tegen de nieuwste bekende beveiligingsrisico's.	Leverancier en gemeente Leeuwarden	Ja, is onderdeel van de dienstverlening door 5.1.2i

Bijlage A: Betrokken partijen en geïnterviewde functionarissen.

Als onderdeel van deze DPIA hebben wij interviews gehouden met de volgende functionarissen;

Gemeente Leeuwarden:
Projectgroep MOL/5.1.2i.
Projectleider.
Medewerkers MOL.
Procesanalist.
Functioneel applicatiebeheerder.
Informatieanalisten en adviseurs.
Informatie architect.

5.1.2i
Managing partner.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15

Herbeoordeling DEPIA: <Gegevensdeling Sociaal Domein>

Naam DEPIA	Gegevensdeling Sociaal Domein
Datum DEPIA	22-5-2023
Datum herziening DEPIA	22-05-2026 – 17-06-2026
Is de verwerking gelijk aan die van de oorspronkelijke DPIA	o Nee, voer een nieuwe DEPIA uit X Ja, ga verder o Gedeeltelijk; beschrijf het verschil
Wat zijn de vastgestelde risico's	Autorisatie Betrouwbaarheid Bewaartermijnen Accountability Gevoel van autonomie en invloed kan afnemen bij inwoners Gevoel dat inwoner toestemming MOET geven Vooringenomenheid bij medewerkers. Komen tot een 'profiel' op basis van DAT informatie Big Brother gevoel bij inwoners. Veiligheid gegevens? Systeem/proces werkt niet meer zoals bedoeld
Welke maatregelen zijn vastgesteld	**Autorisatie** Een groot risico is dat onbevoegde personen onnodige toegang krijgen tot de gegevens. Het is dringend aanbevolen om een strikte autorisatiematrix te formuleren en daarop toezicht te houden. Dit is tevens vereist op grond art. 5 lid 1 onder f AVG. Het risico is namelijk dat er onnodige medewerkers deze informatie te kunnen raadplegen. **Betrouwbaarheid** Een vereiste van de AVG is dat de gegevens juist en actueel zijn. Dit zou kunnen worden gerealiseerd door een applicatie te gebruiken die de betreffende systemen (die gebruikt worden voor de losse dienstverleningen) 'realtime' aan elkaar koppelt (Datawarehouse). **Bewaartermijnen** Risico is dat geen juiste bewaartermijn wordt gehanteerd, doordat er bijvoorbeeld te snel wordt verwijderd of doordat het juist te lang wordt bewaard. Dit levert strijdigheid op met art. 5 lid 1 onder e AVG. Ook dit kan worden geminimaliseerd door na het raadplegen van de lijst/het rapport in het datawarehouse deze weer te verwijderen. De medewerker heeft nu voldoende informatie om gericht actie te ondernemen. **Accountability** Om te kunnen spreken van een rechtmatige verwerking moet de gemeente onder andere aantonen dat (maar niet beperkt tot): o Betrokkenen deugdelijk zijn geïnformeerd;

	o Er een helder triagekader is samengesteld; o Het proces helder vastleggen om aan te kunnen tonen welke informatie op welk moment en voor wie inzichtelijk is. o Een strikte autorisatiematrix is gemaakt en daar streng toezicht op is o Hoe er voor gezorgd is dat de dataset juist, actueel is en hoe er voor wordt gezorgd dat de bewaar- en vernietigingstermijnen in acht worden genomen o Welke technische en organisatorische maatregelen zijn genomen. **Gevoel van autonomie en invloed kan afnemen bij inwoner** Zorg ervoor dat de inwoner regie blijft houden op de ingezette ondersteuning. Voorkom profilering en vooringenomenheid door de inwoner vooraf te vragen naar voorzieningen. Pas daarna kijken of er idd voorzieningen ingezet zijn via andere teams/organisaties. Dit is opgenomen in de procesbeschrijving/werkinstructie. **Gevoel dat inwoner toestemming MOET geven** Bespreek met de inwoner dat hij/zij geen toestemming hoeft te geven en dat de keuze geen invloed heeft op de rest van het proces. Dit is opgenomen in de procesbeschrijving/werkinstructie. **Vooringenomenheid bij medewerkers. Komen tot een 'profiel' op basis van DAT informatie** Vooringenomenheid en profilering moet voorkomen worden. Inwoner moet leidend blijven, invloed houden op het proces en niet gestuurd worden door ondersteuning. Dit is opgenomen in de procesbeschrijving/werkinstructie. **Big Brother gevoel bij inwoners. Veiligheid gegevens?** Zorg voor een goede logging, autorisaties en werkprocessen. Dit moet het gevoel van veiligheid van inwoners vergroten. Uitleg over de werkprocessen en periodieke controle op de werking van het proces en daarbij de bereidheid hebben om het proces aan te passen of te stoppen waar nodig, hoort daar ook bij. Logging, autorisatie en een goede procesbeschrijving/werkinstructie is geregeld inclusief periodieke controle op de werking van het proces dmv voorlichtingen. **Systeem/proces werkt niet meer zoals bedoeld** Borgen dat het systeem nog doet waarvoor het bedoeld is en medewerkers de procesbeschrijving blijven volgen.

	Transparantie naar de inwoner Bij het eerste contact worden de inwoners geïnformeerd over de aanpak en de bedoeling. Dit is expliciet opgenomen in de aangescherpte procesbeschrijving/werkinstructie. In het gesprek kan het volgende worden aangegeven: 'De Gemeente heeft als taak het bieden van een goede dienstverlening in combinatie met de inzet van de noodzakelijke ondersteuning aan alle inwoners. De huidige dienstverlening kan in sommige gevallen versnipperd zijn. We vinden het heel belangrijk dat u de beste ondersteuning en dienstverlening van ons krijgt. Daarom vinden we het van belang om bij alle inwoners de in te zetten ondersteuning/voorziening op elkaar af te stemmen'. Wij kijken of u als inwoner al ondersteuning/voorzieningen/trajecten heeft binnen het Sociaal Domein van de gemeente. Zo ja, dan wordt aan u voorgesteld om in overleg met u , waar nodig, af te stemmen met de andere afdeling(en) . We kunnen hierbij samen met u kijken naar de juiste combinaties van ondersteuning/dienstverlening en voorkomen hiermee dat er onnodig voorzieningen naast elkaar lopen. Daarnaast hoeft u niet dezelfde informatie bij verschillende afdelingen aan te leveren. De inwoner/het gezin heeft de reguliere basisrechten zoals inzage in stukken, het recht om zaken aan te passen enzovoort. Ook het recht op bezwaar is afgedekt middels mediaton of indien dit niet aansluit het recht op bezwaar middels de reguliere wettelijk bezwaar- en beroepsprocedure. Verder is de klachtenprocedure van toepassing. De overige rechten kunnen door betrokkene worden uitgeoefend door middel van een verzoek aan de verantwoordelijke; Gemeente Leeuwarden.
Welke maatregelen zijn toegepast	Alle bovengenoemde maatregelen zijn toegepast en aangescherpt in de procesbeschrijving/werkinstructie. We werken met een specifieke autorisatiegroep waardoor alleen de medewerkers die toegang moeten hebben, ook toegang hebben. De technische en organisatorische maatregelen rondom het 5.1.2i zijn volledig afgestemd met de informatieadviseur Sociaal Domein, ISO/TISO, architectuur. Alle PPM stappen zijn doorlopen. De gegevens in het 5.1.2i (data rapport) zijn actueel en juist. Hier is continu controle op vanuit de functioneel beheerders. Het 5.1.2i is bedoeld om te raadplegen (gegevens worden getoond na invoering BSN). De informatie wordt na raadpleging niet opgeslagen.

	In de procesbeschrijving /werkinstructie staat het proces beschreven en wordt toegelicht hoe de medewerkers kunnen werken met het 5.1.2i. De procesbeschrijving is aangescherpt op basis van deze herbeoordeling.
Wat was het effect van de toegepaste maatregelen (waren deze voldoende/ zijn er aanpassingen geweest etc.)	Geen aanpassingen. Effect tot dusver voldoende.
Zijn er nieuwe risico's ontstaan	X. Nee, zie onderstaande toelichting o Ja De lijst/ het rapport met de data is inmiddels 'in house' gebouwd in een portaal. In de testfase is de lijst/ het rapport in 5.1.2i gebouwd. Hieruit bleek dat het niet mogelijk was om in 5.1.2i alle autorisaties goed in te regelen. Het portaal is toegankelijk voor de geautoriseerde interne medewerkers via het startmenu binnen de 5.1.2i werkomgeving. De autorisatie gaat via beheerde groepen. Het portaal is een database in eigen beheer (in ons eigen netwerk), deze staat niet in de 5.1.2i. In 5.1.2i is uitlijsting in excel mogelijk en in het portaal niet. Er is dus met de komst van het portaal minder risico. Het portaal voldoet aan alle gestelde eisen vanuit privacy/security etc. Voor het bouwen van het portaal is dit opnieuw uitgebreid getoetst bij de ISO/TISO/Privacy etc. Op dit moment wordt gewerkt aan het toegang verlenen van het 5.1.2i aan Amaryllis medewerkers. Dit is conform de Depia. Er is echter, ten opzichte van de interne livegang, een veranderde architectuur nodig om de toegang te verlenen. Dit wordt op dit moment opnieuw getoetst door alle betrokkenen. T.z.t. wordt de uitkomst toegevoegd aan deze herbeoordeling Depia.
Welke maatregelen zijn daarvoor ingericht	Er is gekozen voor het bouwen van een portaal waarbij de autorisatie en ook de logging nog beter in te regelen is.
Zijn er andere inzichten ontstaan	X Nee o Ja, leg uit
Zijn er wijzigingen in wet- en regelgeving? (stem af met de Privacy Officer voor de AVG en met de privacy contactpersoon binnen jouw domein voor de domeinspecifieke wet- en regelgeving). Zo ja, noteer deze dan hierbij.	Nee. In de Depia wordt de invoering van de Wet aanpak meervoudige problematiek Sociaal Domein (WAMS) genoemd. De Wet aanpak meervoudige problematiek sociaal domein (Wams) bevindt zich in de eindfase van de parlementaire behandeling. Het wetsvoorstel, dat gegevensdeling voor een integrale aanpak in het sociaal domein regelt, werd begin 2023 ingediend. Na vertraging en wijzigingen (door de val van het kabinet en

	privacyzorgen), is het doel een gecoördineerde aanpak (één plan, één regisseur) voor burgers met meervoudige problematiek. **Stand van zaken (april 2026):** • **Wetsstatus:** De Wams is nog onderwerp van discussie in het parlement, met recente updates in maart 2026. De inwerkingtreding is meermaals verschoven.
Welke ethische vraagstukken spelen een rol bij deze verwerking (zie de ethische waarden op blad 2) Als de verwerking een of meerdere waarden raakt, moeten deze als risico worden opgenomen en moeten er ook maatregelen voor in kaart worden gebracht	**Cruciale waarden uit de casus:** • **Autonomie;** Voorop staat dat de inwoner centraal moet blijven staan. Kunnen we de autonomie garanderen, als vooraf al bekend is dat een inwoner bekend is bij meerdere teams/organisaties? Kunnen we de inwoner vooraf vragen welke ondersteuning hij al krijgt. Niet iedere client is verstandelijk beperkt en kan best uitleggen wat er allemaal speelt. • **Menselijkheid;** Dat de inwoner een gevoel van serieus genomen wordt kan krijgen, doordat hij slechts 1 keer zijn verhaal hoeft te doen, is een breed gedeeld beeld. Maar ook wordt erkend dat er vooroordelen of vooringenomenheid kan ontstaan doordat er veel meer bekend is over een inwoner. • **Veiligheid;** Zorgen voor een goede logging, autorisaties en werkprocessen moet het gevoel van veiligheid bij inwoners vergroten. Uitleg over de werkprocessen en periodieke controle op de werking van het proces en daarbij de bereidheid hebben om het proces aan te passen of te stoppen als dat niet het geval is, hoort daar ook bij. • **Kwaliteit van leven/duurzaamheid;** 1 plan en een regisseur op het proces is een ideaalbeeld. Dat kan ook nog eens kostenbesparend zijn. Daar staat tegenover dat de inwoner leidend moet blijven, invloed moet houden op het proces en niet wordt gestuurd door de ondersteuning. **Maatregelen op basis van de eerdergenoemde risico's die kunnen ontstaan doordat de verwerking 1 of meerdere waarden raakt:** **Autonomie;** zorg ervoor dat de inwoner regie blijft houden op de ingezette ondersteuning. Voorkom profilering en vooringenomenheid door de inwoner vooraf te vragen naar voorzieningen. Pas daarna kijken of er idd voorzieningen ingezet zijn via andere teams/organisaties. •**Veiligheid;** goede werkprocessen, logging op invoer van het BSN en periodieke controle of het proces nog werkt zoals vooraf bedacht, zijn cruciaal voor het gevoel van veiligheid bij de inwoner. •**Menselijkheid;** 1 regisseur op het geheel is nodig. Niet alleen voor het gevoel van serieus genomen te worden, maar ook voor de kostenoverweging. Tegelijkertijd moet vooringenomenheid en profilering voorkomen worden, waardoor het gevoel van vertrouwen weer afneemt. **Actuele stand van zaken:** Met ingang van 17 juli 2025 hebben de interne medewerkers toegang tot het 5.1.2.2i. De verwachting is dat rond de zomer 2026 Amaryllis en de Hulp bij Huishouden aanbieders toegang krijgen. Hiervoor worden opnieuw de stappen rondom privacy/security (PO/ISO/TISO etc) doorlopen. Voorafgaand aan de interne implementatie is veel tijd besteed aan gerichte voorlichtingsbijeenkomsten. Tijdens deze bijeenkomsten is uitgebreid aandacht gegeven aan 'hoe te werken met het 5.1.2.2i'. Na de implementatie hebben we deze voorlichting bij diverse teams herhaald. Ook is er een duidelijke procesbeschrijving/werkinstructie opgesteld die is opgenomen in de eigen werkinstructies van de verschillende uitvoeringsteams. Vanuit de

	verandermanager Expeditie 2030 is het 5.1.2i tot slot meerdere keren ingebracht op de MT's. Begin 2026 is er een korte enquête uitgezet binnen de teams over het gebruik van het 5.1.2i. Hieruit kwam naar voren dat 5.1.2i steeds meer wordt gebruikt maar nog lang niet door iedereen. Het is echt een stukje verandering voor het werk van een consulent. Men is blij met de informatie, men begrijpt de voordelen in de dienstverlening aan de inwoner maar is tegelijkertijd nog zoekende in het breed uitvragen/integraal werken. Het 5.1.2i is een mooi hulpmiddel, maar het echt integraal werken vergt meer: een verandering van het werk van de professional en de sturing hierop. Ook regie pakken in casuïstiek is nog geen 'gewoonte'. Vanuit het project **Toegang in Beeld** wordt hier Sociaal Domein breed naar verwachting een verandering in doorgevoerd. We zijn tot slot op dit moment bezig om de periodieke controle en monitoring op het proces structureel te borgen in de lijn. Dit wordt besproken in het kernteam van de Expeditie 2030. Tot die tijd pakt 5.1.2e samen met 5.1.2e 5.1.2e hierin een rol en worden de teamleiders hier ook op gevergd.
• **De gegevensverwerking;** Wordt er een nieuwe technologie gebruikt? Worden de persoonsgegevens voor een ander doel gebruikt? (zo ja, dan verandert de gegevensverwerking feitelijk in een nieuwe gegevensverwerking. En dan kan een DEPIA ook weer verplicht zijn. Zijn er aanpassingen in het werkproces? Of het doel van de verwerking? • **De risico's van de verwerking;** Verandert het privacyrisico van de verwerking? Dat kan voorkomen omdat een onderdeel van het verwerkingsproces wijzigt. Ook gaan technologische ontwikkelingen snel, waardoor kunnen nieuwe kwetsbaarheden ontstaan. • **De ingezette maatregelen voor het mitigeren van de risico's;** Zijn alle maatregelen effectief? Of zijn deze al veranderd in de loop van de tijd?	Nee, is niet gewijzigd. Nee, de verwerking van gegevens is gelijk aan hoe dit staat beschreven in de Depia. Ja, de maatregelen zijn nog steeds afdoende. Wel is de procesbeschrijving/werkinstructie aangescherpt. De maatregelen zijn effectief maar vragen wel periodieke herhaling en evaluatie.

• **de context van de verwerking.** Is de context van de organisatie of de maatschappelijke context veranderd? Zijn bijvoorbeeld nieuwe categorieën mensen kwetsbaar geworden voor discriminatie.	Nee.
In ieder geval is het signaal, dat er vóórdat er een gesprek wordt aangegaan met een client, alvast in 5.1.2i gekeken om meer te weten te komen over de situatie. Daarmee kan vooringenomenheid ontstaan en ontneem je de client de autonomie. Dat is intensief besproken en zijn ook maatregelen voor ingezet. Dat kun je natuurlijk niet halen, uit de beoordeling van de werkprocessen, maar veel eerder door collega's hierop te bevragen.	Uit de enquête die recent is uitgezet in de uitvoerende teams kwam naar voren dat er inderdaad medewerkers zijn die het 5.1.2i wel eens vooraf checken. Het werd als volgt verwoord: *In het geval dat er onduidelijkheden zijn en om te achterhalen wie er bij persoon/gezin betrokken is* Er is veel aandacht besteed tijdens de voorlichtingen aan de ethische waarden. Daar zijn de medewerkers zich dus van bewust. Zij maken zelf de afweging, met toepassing van de werkinstructie, wat goed is in die betreffende situatie In de werkinstructie staat hierover het volgende: **Hoe gebruik je 5.1.2i?** 1. Een inwoner of een gezin meldt zich bij jou met een hulpvraag. Laat de inwoner eerst zoveel mogelijk zelf het verhaal vertellen. 2. Je raadpleegt 5.1.2i en kijkt of de inwoner gebruik maakt (of heeft gemaakt) van andere voorzieningen of werkprocessen. Als het nodig is, kun je ook de gegevens van ouders, kinderen of partner inzien. De informatie in 5.1.2i is voor ons als medewerker bedoelt. Laat de inwoner niet meekijken. ***Vooraf aan het gesprek raadplegen van 5.1.2i:*** *Raadpleeg 5.1.2i **alleen** voorafgaand aan het gesprek bij bijzonderheden (bijvoorbeeld een vermoeden van meervoudige problematiek).* *Of raadpleeg 5.1.2i als je een signaal wilt afgeven aan bijvoorbeeld de medewerker van Amaryllis omdat een inwoner niet op een afspraak verschijnt of geen stukken aanlevert en je je zorgen maakt. Je deelt alleen de DAT-informatie met elkaar: je geeft aan dat er een aanvraag voor een uitkering is ingediend, dat de inwoner niet verschijnt op de afspraak en dat we het recht op een uitkering zo niet kunnen vaststellen.* ***Tijdens het gesprek raadplegen van 5.1.2i:*** *Raadpleeg 5.1.2i tijdens het gesprek als je ziet dat de inwoner het lastig vindt om zelf te vertellen wat er speelt. Het kan ook zijn dat de inwoner tijdens het gesprek dingen vertelt waardoor je weet dat er meer*

	speelt en er een noodzaak lijkt te zijn om afstemming te zoeken met andere collega's of hulpverleners. Kijk vooral naar de zaken die relevant zijn voor de hulpvraag die aan jou wordt gesteld. Hoewel je ervaring je misschien een direct beeld geeft van de inwoner, is het belangrijk om met een open blik naar de situatie te blijven kijken. Realiseer je ook dat 5.1.2i niet altijd een volledig beeld geeft. Het jongerenwerk door Amaryllis vind je bijvoorbeeld niet terug in 5.1.2i. De volledige werkinstructie wordt als bijlage meegestuurd bij deze herbeoordeling Depia. We hebben de werkinstructie aangescherpt op basis van deze herbeoordeling. Toevoegingen/aanpassingen zijn in het rood opgenomen. De aangepaste werkinstructie zal, na akkoord op deze herbeoordeling, worden gedeeld met de uitvoerende teams.
Waar ik verder nog benieuwd naar ben, is hoe de autorisaties zijn ingericht. Het gaat weliswaar om "dat" informatie, maar zelfs "dat" informatie kan teveel zijn, als je die informatie niet nodig hebt voor het uitvoeren van je werk. (bijvoorbeeld dat er een uitkering is, terwijl het gaat om schoolverzuim).	Iedereen die onder de geautoriseerde toegangsgroep valt, ziet dezelfde informatie. Daar is nu geen onderscheid in gemaakt. Het gaat inderdaad om de DAT informatie. Wel is in afstemming met de uitvoerende teams ervoor gekozen om soms andere termen te gebruiken. Bij leerplicht is bijvoorbeeld in afstemming met de teams bewust gekozen voor het tonen van de term 'leerplicht/doorstroompunt' in plaats van de term schoolverzuim of iets dergelijks. Men ziet dus alleen dat er een collega van leerplicht/doorstroompunt betrokken is, verder niets. Verder zijn er diverse werkprocessen en voorzieningen die niet worden getoond vanwege teveel risico (bijv. fraude onderzoeken). Alle informatie die wordt getoond is in afstemming met de betreffende teams. Het doel van 5.1.2i moeten we voor ogen houden: betere dienstverlening aan onze inwoners, betere afstemming van voorzieningen. Sommige voorzieningen hebben niet direct iets met elkaar te maken en kunnen separaat worden afgehandeld. De professional (consulent) kan dit prima inschatten. Je kunt alleen niet op voorhand zeggen dat je de informatie niet nodig hebt voor je werk. Dit hangt namelijk af van de wensen van de inwoner. Als een inwoner bij de leerplicht ook begint over de uitkeringsproblemen die invloed hebben op de situatie thuis, is het juist heel fijn om wel die verbinding te kunnen zoeken. De inwoner is dus leidend. Toevallig is er een medewerker die in de enquête ook iets heeft genoemd hierover: *Voor jeugdigen die vanuit absoluut schoolverzuim binnenkomen kan ik kijken wat er aan hulp in zit om een inschatting te maken of een vrijstelling misschien van toepassing is. En voor relatief schoolverzuim is het ook belangrijk om te kunnen zien of er hulpverlening betrokken is om zo makkelijker te kunnen schakelen.*

Aanpassingen in de oorspronkelijke DEPIA d.d. 8 juni 2023	*Pagina 2, vraag 1.1: bij de uitleg van de doelen is een aantal wetsartikelen genoemd.* *art. 2.3.2 lid 4 onder b Wmo aangepast naar art. 2.3.2 lid 4 Wmo 2015, art. 1.1.1 Wmo 2015 en art. 2.2.4 Wmo 2015)* *Art. 2.3 lid 1 onder c Jeugdwet aangepast naar art. 2.3 Jeugdwet* *Pagina 5, bij vraag 1.3 staat de gemeente Leeuwarden genoteerd als verwerker. De rol van verwerker is weggehaald.* *Pagina 12, vraag 4.3 staat* 5.1.2i *genoemd. Dit is aangepast naar het* 5.1.2i *met verwijzing naar deze herbeoordeling voor de toelichting.*
Aamdachtspunt voor de volgende herbeoordeling van deze DEPIA in juni 2029.	Voor de volgende herbeoordeling is het goed om het oude format over te nemen in het nieuwe format

ADVISERING FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING (FG)
Herbeoordeling DEPIA: Gegevensdeling Sociaal Domein
Aan: Sectormanager 5.1.2e
Van: 5.1.2e, Functionaris voor de Gegevensbescherming
Kenmerk DEPIA: 2024-192760
Datum: 17-06-2026
Status: Definitief Advies

---

1. MANAGEMENTSAMENVATTING & CONCLUSIE
Status oordeel: Akkoord

- De verwerking voldoet aan de AVG. De afgesproken maatregelen zijn geïmplementeerd. Daarnaast zijn de werkinstructies aangescherpt om eventuele risico's verder te mitigeren. De verwerking kan ongewijzigd worden voortgezet.

---

2. AANLEIDING EN SCOPE

- **Historie:** Op 8 juni 2023 is de initiële DEPIA voor deze verwerking afgerond.
- **Reden van herbeoordeling:** Dit advies betreft de 3-jaarlijkse herziening.
- **Scope:** In deze herbeoordeling is specifiek getoetst of de destijds afgesproken maatregelen effectief zijn en of er wijzigingen zijn geweest in werkprocessen en/of wet- en regelgeving.

---

3. EVALUATIE EN CONCLUSIE
Status eerder vastgelegde maatregelen

- Alle in de initiele DEPIA opgenomen maatregelen zijn geimplementeerd en werken naar behoren.
- Er is onderzoek gedaan naar aanleiding van een signaal over een andere werkwijze dan afgesproken. Dit heeft geleid tot aanscherping van de werkinstructie en geeft ook aan dat er ruimte is om (waar noodzakelijk) afgeweken kan worden van deze werkinstructie.

- Dit getuigt van een zorgvuldige afweging om waar nodig, de gegevensdeling toe te passen.

---

4. ONDERTEKENING
Dit advies is uitgebracht op basis van de op dit moment aan de FG verstrekte informatie en is opgesteld vanuit de wettelijke, onafhankelijke toezichthoudende rol conform artikel 39 van de AVG.

Voor akkoord door de verantwoordelijke (management):
5.1.2e, 5.1.2e Inkomen en Wmo
Datum: 17-06-2026

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	6, 9, 10
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	3, 4, 5, 6, 7, 8, 9

C2412 1390 naam auteur in metadata standaard aanpassen in Gemeente Leeuwarden

5.1.2e (Gemeente Leeuwarden)

Aanmelder

Naam	5.1.2e
Locatie	Gemeente Leeuwarden
Inlognaam netwerk	5.1.2e
Aanspreekvorm aanmelder	[Naam]
Telefoonnummer	5.1.2e
E-mail	5.1.2e @leeuwarden .nl
Kostenplaats	EP110138.9200 - CS-Middelen
Organisatie	Gemeente Leeuwarden

Details

Korte omschrijving	naam auteur in metadata standaard aanpassen in Gemeente Leeuwarden
Soort 'Melding'	Informatieverzoek
Categorie	Bedrijfsvoering
Subcategorie	Leeuwarden
Extern nummer	42365

Object

Object ID	Templafy Leeuwarden
Soort	Software

Planning

Impact	Normaal
Urgentie	Normaal
Prioriteit	Prio 3
Streefdatum	22 juni 2026 14:04
Doorlooptijd	3 dagen
On hold	Nee

Afhandeling

Behandelaar	5.1.2e
Behandelaarsgroep	IM ST Bedrijfsvoering
Status	Aangemeld
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2e — 5 december 2024 11:24

Waar wilt u een melding over maken?
- Software

Welke software betreft het?
- Microsoft Word en/of Excel

Nummer (computer/printer/)
-

Uitgebreide omschrijving
- Ik wil weten of het technisch mogelijk is om de naam van de opsteller van een document standaard aan te passen in "gemeente Leeuwarden". Of vervolgens deze keuze ook gemaakt wordt, is de volgende stap. Mijn vraag heeft nu alleen te maken met de techniek

Actie

5.1.2e — 6 juli 2026 9:44

Hallo 5.1.2e ,

Ik dacht dat ik je al een reactie had gestuurd, maar kennelijk alleen in gedachten....
Ik heb eerlijk gezegd geen idee welke templates er allemaal zijn, maar dan gaat het vooral om die templates, die extern gaan (ofwel naar inwoners ofwel worden gepubliceerd) die voorrang hebben. Dus alles die te maken hebben met bestuur en communicatie?

5.1.2e — 1 juli 2026 15:27

Hi 5.1.2e ,

Er geen functioneel beheer op de office programma's, dus op dit moment is het zo dat iedereen dit zelf zou moeten aanpassen.

Indien het wenselijk is de naam onder Auteur aan te passen naar een standaard voor documenten die vanuit

Templafy worden opgesteld, dan hoor ik het graag.
Aangezien het voor elk template apart moet worden ingesteld, zit er wel even wat werk in. Als er templates zijn die 'voorrang' moeten krijgen, veelgebruikte templates bijvoorbeeld, dan ontvang ik graag een lijstje daarvan.

5.1.2e 16 juni 2026 11:15
Heel duidelijk! ik heb het al even getest en dat werkt inderdaad. Is dit dan iets, dat vanuit het SSC aangepast kan worden voor iedereen? of moet iedereen dit zelf aanpassen

5.1.2e 16 juni 2026 11:10
Dat zijn de instellingen die standaard in de Office programma's gebruikt wordt, in dit geval welke naam er bij Auteurs en bij laatst opgeslagen staat.
Dus als in Templafy een standaard Auteurs naam is ingesteld, dan staat onder 'Laatst opgeslagen door' nog wel de naam van de persoon omdat dat de instelling is vanuit Word.

Dit kan ook aangepast worden, maar niet via Templafy. Ook voor bestanden die buiten Templafy worden aangemaakt, kan Auteur en Laatst opgeslagen door aangepast worden.
Hier staat uitgelegd hoe dat moet: De naam van de auteur wijzigen voor documenten, presentaties of werkmappen | Microsoft Support

Hopelijk is dit duidelijk!

5.1.2e 16 juni 2026 10:02
Hoi 5.1.2e, Ik ben niet zo technisch op dat gebied, dus ik begrijp niet zo goed wat er wordt bedoelt met de lokale office-instellingen.

5.1.2e 16 juni 2026 10:00
Goedemorgen,
Ik heb de melding van 5.1.2e overgenomen en het antwoord van Templafy is als volgt:
Het is mogelijk om de naam onder Auteur aan te passen, dit moet voor ieder template dat in Templafy staat apart ingesteld worden.
Echter heeft Templafy geen controle over lokale Office-instellingen, waardoor gebruikers nog steeds de laatst gewijzigde gebruiker zijn en hun eigen naam in opmerkingen zien.

5.1.2e **onzichtbaar voor aanmelder** 9 juni 2026 14:53
5.1.2e, kun jij uitzoeken of dit te doen is?

5.1.2e 19 maart 2025 16:27
Hoi 5.1.2e, excuus voor de late (re)actie. Er is op dit moment geen vaste Templafy beheerder (komt er wel weer) dus ik doe het er even bij.

Ik heb de vraag al wel reeds uitgezet bij de leverancier.

Met vriendelijke groet,

5.1.2e

5.1.2e **onzichtbaar voor aanmelder** 19 maart 2025 16:26
Van: Incident Response <support@templafyincident.zendesk.com>
Verzonden: woensdag 19 maart 2025 16:24
Aan: 5.1.2e <5.1.2e@leeuwarden.nl>
Onderwerp: [Request received] Is it possible to change the name of the author in the help texts to an general name or comany name?

U ontvangt niet vaak e-mail van support@templafyincident.zendesk.com. Ontdek waarom dit belangrijk is

##- Please type your reply above this line -##
Thank you for reaching out to Templafy Support!
Your support ticket (42365) has been received and is being reviewed by our support team. We'll be in touch as soon as possible.
If you want or need to add additional comments, please reply to this email.
While we're working on your support ticket, a reminder that we have the following resources available for you:
Templafy Knowledge Base
Templafy Academy
This email is a service from Incident Response.

5.1.2e 16 december 2024 15:27

Ik had dus al een mailtje gestuurd, maar tot op heden geen reactie gehad. Ik ga via onze privacy officers nog wel even proberen. Zij hebben sws al meer contacten met de privacy officers van die gemeente. Maar jij mag gerust ook contact opnemen hoor!

5.1.2e 13 december 2024 10:10

We moeten er denk ik rekening mee houden dat er stukken via Templafy in Word maar ook buiten Templafy in Word worden aangemaakt, net zo goed dat er stukken in andere Office applicaties buiten Templafy om worden aangemaakt.

Ik zal gaan uitzoeken wat Templafy hierin kan betekenen maar ook wat we vanuit de policies die zijn ingesteld door ICT, kunnen bewerkstelligen.

Ik heb geen contact met collega's van de gemeente Smallingerland, wellicht dat we via die privacy-groep wat contactgegevens van Office-/sjabloonbeheerders kunnen krijgen? Ik wil wel contact zoeken mochten we er zelf niet uitkomen.

5.1.2e 13 december 2024 8:43

Goedemorgen 5.1.2e, dat weet ik niet. Ik dacht in mijn onwetendheid ook, dat het ging om microsoft (aangezien het gaat om word en excel).
Ik heb wel een vraag gesteld aan de privacy-groep van Smallingerland, maar nog geen antwoord gekregen. Misschien heb jij contact met collega's van die gemeente?

5.1.2e 13 december 2024 8:40

Goedemorgen 5.1.2e, dan is de vraagstelling duidelijk. Ik zal de vraag uitzetten bij leverancier Templafy.

Gemeente Smallingerland werkt ook met Templafy?

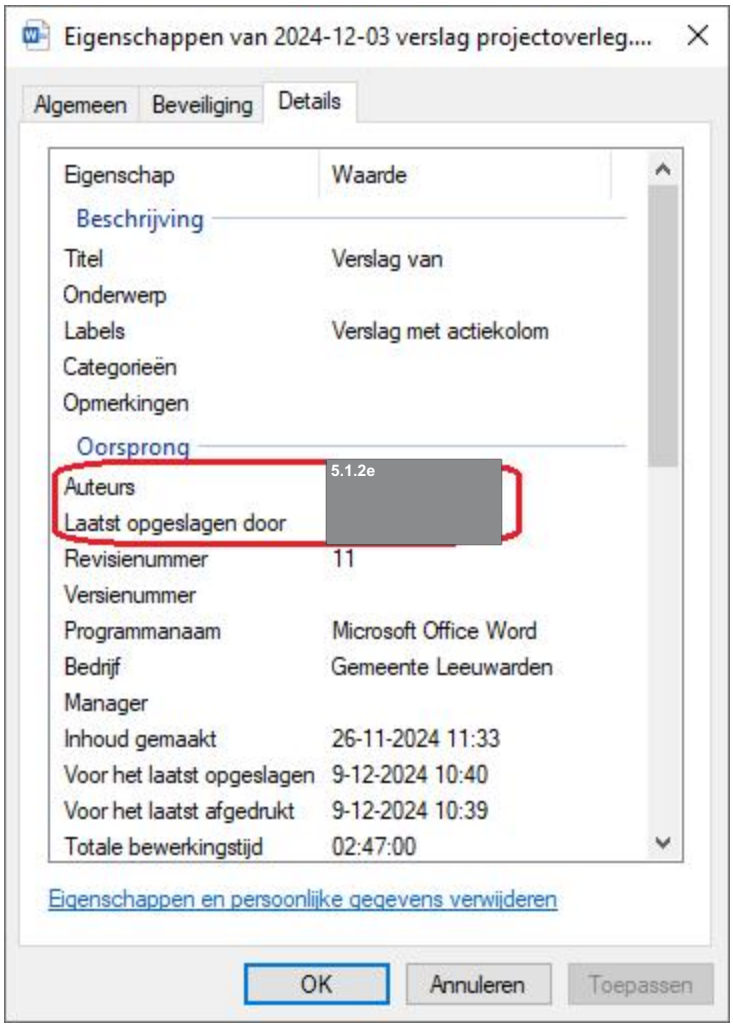
5.1.2e 13 december 2024 8:33

Goedemorgen 5.1.2e, Ja die gegevens bedoel ik inderdaad. Ik heb begrepen dat oa gemeente Smallingerland dit ook toepast, dus het moet mogelijk zijn. Kun je ook nagaan hoeveel "werk" dat is en op welke termijn dat in te richten zou zijn?

Nogmaals; 5.1.2e is op de hoogte en het is nu alleen nog inventariseren. Het besluit volgt later of we dit wel of niet gaan doen.

5.1.2e 12 december 2024 16:18

Hoi 5.1.2e, dan bedoel je de naam die op deze plek in de eigenschappen/details van het document wordt vastgelegd?



5.1.2e **onzichtbaar voor aanmelder** 5 december 2024 11:26

Voor templafy beheerders.

Informatie

Aanmelddatum	5 december 2024 11:24	Standaardoplossing	Er is geen standaardoplossing gekoppeld
Gerealiseerde doorlooptijd	00:00		
Doorlooptijd 'On hold'	2806:22		
Aangepaste doorlooptijd	00:00	Geëscaleerd	Ja
Doorlooptijd 'Afgerond'	00:00	Behandelaar (de-)escaleren	Servicedesk SSC
Doorlooptijd 'Uitvoering'	00:00	Bestede tijd	00:00
Geregistreerde tijd	00:00		

Extra informatie

Informatie

SSP Formulier	LWD-SSC, Melding Servicedesk

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2, 3, 4

Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 14058

Gemeente Leeuwarden

M E M O

Aan: 5.1.2e

Van: 5.1.2e

Datum: 27 mei 2024

Onderwerp: Hoog aantal datalekken door onvolledig anonimiseren

Inleiding

Bij een datalek worden persoonsgegevens vernietigd, verloren, gewijzigd of gedeeld terwijl dat niet de bedoeling was. Hoewel een datalek natuurlijk altijd vervelend is, biedt dit ook een kans om de processen eens goed tegen het licht te houden. En ook of het betreffende team wel voldoende kennis heeft van de regels rondom privacy en informatiebeveiliging. Zodra het datalek een risico oplevert voor 'de rechten en vrijheden van betrokkenen, zoals de bescherming van hun persoonsgegevens en persoonlijke levenssfeer', moet deze gemeld worden bij de Autoriteit Persoonsgegevens.

Via deze memo stel ik je op de hoogte van de stijging in het aantal datalekken bij het online publiceren ten opzichte van vorig jaar. En waardoor deze verhoging vooral wordt veroorzaakt. Uiteraard volgt daarop de acties die we hebben ingezet om het risico zo klein mogelijk te houden.

1. Aantallen datalekken

In de tabel hieronder staan de aantallen datalekken van de eerste 4 maanden van 2023 en die van 2024. Ook staat er het aantal datalekken dat gemeld moest worden aan de AP:

Januari-april 2023		**Januari-april 2024**	
Totaal datalekken	**Gemeld aan AP**	**Totaal datalekken**	**Gemeld aan AP**
13	2	39	28

Het aantal interne meldingen, dus datalekken die niet gemeld hoefden te worden, is gelijk gebleven. Het aantal datalekken dat gemeld moest worden aan de AP is enorm gestegen. Meer dan de helft (15 namelijk) van deze 28 datalekken is veroorzaakt door het niet of niet volledig geanonimiseerd publiceren van documenten op internet. Een aantal van deze datalekken heb ik samengevoegd, waardoor het totaal aantal gemelde datalekken met als oorzaak “teveel persoonsgegevens gepubliceerd” bij de AP 8 stuks is en geen 15.

Hieronder volgt per afdeling/team de onderverdeling van deze datalekken. Deze verdere uitsplitsing heeft geen andere functie dan om in te zoomen op het meest kwetsbare proces en de hoeveelheid publicaties:

Team/Afdeling	Aantal datalekken
PD-Vergunningen en Leefomgeving	11
Griffie/Concern	2
SD-Beleid en Strategie	1
AFAC/Omrin/Buitendienst	1

1.1 Autoriteit Persoonsgegevens (AP)
Omdat gemeente Leeuwarden een veel hoger aantal datalekken heeft gemeld dan voorheen, waarvan een groot deel gaan over het onterecht online publiceren van persoonsgegevens, kunnen we een reactie hierover verwachten van de AP (overigens is de stijging te verklaren, omdat er pas dit jaar gestart is met het online publiceren van vergunningsaanvragen).

Daarbij verwacht ik dat er gevraagd wordt om de DEPIA, welke nog niet is afgerond. Dit kan mogelijk gevolgen hebben, zoals extra aandacht voor de gang van zaken rondom privacy binnen gemeente Leeuwarden of mogelijk een boete.

2. Ingezette acties

2.1 DEPIA op DigiEplan
Het proces van anonimiseren via DigiEplan, welke medio 2023 al voor Wet modernisering electronisch bestuurlijk verkeer in gebruik is genomen, is lange tijd niet beschouwd als een proces waarbij (hoogrisico) persoonsgegevens worden verwerkt. Daardoor is dus ook vóór ingebruikname geen DEPIA uitgevoerd en zijn dus ook de risico's niet in kaart gebracht, noch maatregelen daarvoor ingesteld.

Het invullen van de DEPIA heeft daarnaast intern discussie opgeleverd, waardoor deze lange tijd is blijven liggen. Via teamleider 5.1.2e wordt nu de verdere uitvoering/invulling van de DEPIA opgepakt. Ook was mij tot medio maart niet bekend, dat DigiEplan al in gebruik was genomen voor de online publicaties.

2.2 Griffie/Concern
Bij Griffie/Concern is inmiddels bekend dat er in het verleden een vorm van anonimiseren is gebruikt, welke niet onomkeerbaar is. Dat betekent dat de volgende acties in gang zijn of worden gezet:

- Er is een cursus "AVG in Vogelvlucht" geweest, om meer bewustzijn te creëeren en om uitleg te geven over wat nu wel en niet geanonimiseerd moet worden vóór publicatie;
- De checklist voor anonimiseren bij online publicatie is gedeeld en besproken;
- Er vindt controle plaats in alle door de Griffie gepubliceerde documenten vanaf 2022;
- De documenten tussen 2019 en 2022 moeten verwijderd worden vanaf de internetpagina van gemeente Leeuwarden. Dit project zal binnenkort opgestart worden.

2.3 PD-Vergunningen en Leefomgeving
Sinds 1 januari 2024 is het team van Vergunningen en Leefomgeving gestart met de publicatie van alle vergunningsaanvragen. Hierbij wordt de applicatie DigiEplan gebruikt om de documenten te anonimiseren. Deze applicatie kan voorstellen doen voor anonimisering en dit wordt vervolgens door een medewerker gecontroleerd. Het probleem bij deze werkwijze is, dat het lang duurt, voordat een document is geanonimiseerd.

Het gevolg is, dat medewerkers zelf de soms grote hoeveelheid documenten doornemen via DigiEplan en dus handmatig anonimiseren. Met fouten tot gevolg; er zijn tot 1 mei 2024 11 vergunningsaanvragen niet volledig geanonimiseerd gepubliceerd geweest. En in mei zijn er ook alweer 2 datalekken gemeld.

Vooruitlopend op de mogelijke reactie van de AP, heb ik contact gehad met 5.1.2e rondom het proces van online publiceren. Ik heb geadviseerd om het proces van online publiceren aan een kritische blik te onderwerpen. Ik begrijp de visie op dienstverlening en transparantie, deze is ook zeer belangrijk en we moeten ook echt niet terug naar het opvragen van de documenten via de balie van Vergunningen en Leefomgeving.

Het nadeel op dit moment is dat onze applicatie de medewerkers niet op de juiste manier ondersteunt. Hierdoor bestaat het risico dat onze inwoners negatief geraakt worden door de publicatie van teveel persoonsgegevens.

Hieronder staan de al ingezette acties, gevolgd door de aanvullende afspraken die we hebben gemaakt:

- Er is een cursus “AVG in Vogelvlucht” geweest, om meer bewustzijn te creëeren en om uitleg te geven over wat nu wel en niet geanonimiseerd moet worden vóór publicatie;
- DigiEplan is geoptimaliseerd;
- De checklist voor anonimiseren bij online publicatie is gedeeld en besproken.

2.3.1 Aanvullende afspraken

- We gaan verder in gesprek met de applicatie-eigenaar over verdere doorontwikkeling van DigiEplan;
- Inzetten van collegiale toets; leren van elkaar;
- Onderzoeken of mensen dedicated inzetten op anonimiseren een optie is;
- Onderzoeken of de aanvrager documenten geanonimiseerd aan kan leveren;
- Onderzoeken of een aantal gegevens achterwege gelaten kunnen worden.

Het laatste aandachtspunt is ontstaan door een opmerking/klacht die is ingediend over de publicatie van de kosten van een verbouwing. Er waren door buren van de vergunningaanvrager opmerkingen gemaakt over de kosten van de verbouwing. De vergunningaanvrager voelde zich daardoor in zijn gevoel van privacy aangetast. Ook dit punt zal dus meegenomen worden in de herbeoordeling van het proces van online publicaties.

Conclusie

We hebben de nodige acties in gang gezet om het risico bij datalekken zo klein mogelijk te krijgen. Uiteraard is nooit uit te sluiten dat er een datalek ontstaat bij het online publiceren. Maar dat we er alles aan doen, om het risico dat daardoor ontstaat bij onze inwoners zo klein mogelijk te houden, mag van een organisatie als de gemeente verwacht worden. Ik heb er alle vertrouwen in, dat we richting de AP een complete uitleg kunnen geven rondom de aanpak van dergelijke datalekken.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2, 3

Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 14058

Gemeente Leeuwarden

M E M O

Aan:	Directeur bedrijfsvoering, 5.1.2e
Van:	5.1.2e
Datum:	2 september 2024
Onderwerp:	Datalekken in raads- en informatiesystemen door niet anonimiseren metadata
Zaaknummer:	2024-192096

Inleiding

In de metadata (de eigenschappen) van documenten staan vaak persoonsgegevens van de opsteller van het document. Dat is geen probleem, zolang deze niet openbaar worden gemaakt. En dat is het geval bij documenten die opgenomen worden in de raads- en informatiesystemen. Als het gaat om namen van ambtenaren is dat minder risicovol, dan wanneer het gaat om een ingekomen stuk waarbij de metadata dus gegevens van de inwoner bevat. Of, wanneer het een stuk is, dat door een ambtenaar is opgesteld, en gevoelige informatie bevat.

Aan het einde van de vakantie is een melding gedaan door de IBD, om gemeenten (opnieuw) te attenderen op de risico's bij niet-geanonimiseerde metadata in onder andere Ibabs. De leverancier van Ibabs heeft daar in eerste instantie op gereageerd door de download-optie te deactiveren. Daarmee is alle metadata niet langer toegankelijk en het probleem opgelost. Helaas is Ibabs daarop teruggekomen door deze optie per 28 augustus weer te activeren.

In deze memo vraag ik je besluit op mijn advies om alle documenten in Ibabs tot 1 jaar geleden (tot 1 september 2023) te controleren op persoonsgegevens van inwoners in de metadata en indien nodig te anonimiseren. Daarnaast om te besluiten alle overige documenten buiten beschouwing te laten, vanwege het lage risico voor de betrokkenen ten opzichte van de grote inspanning die hiervoor geleverd zou moeten worden.

Reactie leverancier Ibabs en VNG

Contact met de leverancier van Ibabs heeft (nog) geen resultaat gehad. De servicedesk van Ibabs heeft aangegeven, dat de verantwoordelijkheid voor het anonimiseren bij de opsteller van de documenten ligt en niet bij de leverancier. Bovendien staan zij voor "transparantie en beschikbaarheid van documenten" en daar hoort voor hen ook de optie van downloaden bij. Annuleren of deactiveren van de optie tot downloaden per gemeente is ook niet iets waar zij voor open staan.

Contact met de VNG heeft (vooralsnog) ook nog geen resultaat opgeleverd richting de leverancier, want de VNG wordt door deze leverancier niet gezien als klant. Zij gaan derhalve niet in gesprek met de VNG. Andere leveranciers hebben juist wél positief gereageerd en meegedacht over aanpassingen in hun applicatie. Want hoewel de leverancier van Ibabs gelijk heeft, dat wij als opstellers van documenten verantwoordelijk zijn voor de inhoud, heeft de leverancier de verantwoordelijkheid om een applicatie te leveren die ons in staat stelt aan de AVG te voldoen. Niet langer te kunnen downloaden, is de meest ideale oplossing daarvoor.
In afwachting van een landelijke vuist richting deze leverancier, is er vanuit de gemeente een tweetal acties nodig; ervoor zorgen dat er geen nieuwe datalekken bij komen en ervoor zorgen dat de

metadata in de huidige bestaande documenten worden beoordeeld op risico en deze vervolgens anonimiseren waar dat nodig is.

1. Voorkomen van nieuwe datalekken

Voordat een document wordt gepubliceerd, moet er een publicatie-zaak in het zaaksysteem worden aangemaakt, waarin de documenten geanonimiseerd worden opgenomen (dus ook de metadata). Pas dan kan een document opgenomen worden in Ibabs. Dit hoort de verantwoordelijkheid te zijn van de opsteller/indiener van het document of dossier. Een werkinstructie wordt gemaakt en gedeeld via intranet.

2. Beeindigen van de bestaande datalekken in Ibabs

De IBD/VNG, die daarover met een aantal gemeenten contact heeft gehad, adviseert om alle documenten tot 1 jaar terug, dus tot 1 september 2023, te beoordelen op risico voor betrokkenen en dan over te gaan tot controle op persoonsgegevens in de metadata en deze, indien aanwezig, te anonimiseren.

Alle overige documenten, ouder dan 1 jaar geleden, worden daarbij buiten beschouwing gelaten. Het risico voor betrokkenen is al klein en bij oudere documenten nog kleiner. Daarbij weegt de inspanning die hiervoor gedaan moet worden, niet op tegen het risico voor de betrokkenen. Dit is dan in overeenstemming met artikel 33 en 34 AVG.

Ik adviseer om daarbij een onderscheid te maken tussen inwoners en ambtenaren. Dus een controle op ingekomen stukken. Eventueel kan er bij een gevoelig dossier ook een controle uitgevoerd worden op de naam van een ambtenaar in de metadata. Hoewel deze beperkte controle nog steeds een behoorlijke tijdsinvestering zal gaan kosten, is deze inspanning vele malen lager, dan alle documenten binnen Ibabs te controleren.

Het datalek moet vervolgens opgenomen worden in het register van datalekken, waarbij de genomen maatregelen vastgelegd worden, inclusief het besluit op het al dan niet uitvoeren van een controle op de metadata van documenten in Ibabs.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1

M E M O

Aan:	Gemeentesecretaris Eelke de Jong
Van:	5.1.2e
Datum:	24 september 2024
Onderwerp:	Datalek in raads- en informatiesystemen door niet anonimiseren metadata
Zaaknummer:	2024-192096

Inleiding

Aan het einde van de vakantie is een melding gedaan door de IBD, om gemeenten (opnieuw) te attenderen op de risico's bij niet-geanonimiseerde metadata in onder andere Ibabs. In de metadata (de eigenschappen) van documenten staan vaak persoonsgegevens van de opsteller van het document. Dat is geen probleem, zolang deze niet openbaar worden gemaakt. En dat is het geval bij documenten die opgenomen worden in de raads- en informatiesystemen.

De metadata is te vinden, zodra een document vanaf de publieksportaal wordt gedownload, waarna deze via de document-eigenschappen op te zoeken is. In eerste instantie was ik geneigd om te vinden, dat de naam van een ambtenaar minder risicovol is, maar na het lezen van deze blog (metadata, een onbekend risico voor criminaliteit), denk ik daar iets anders over.

Het risico voor de ambtenaar persoonlijk mag dan klein zijn, de naam van een opsteller staat vaak ook wel in het document zelf, voor de organisatie kan dit wel degelijk een groot risico opleveren. Er kan namelijk phishing ingezet worden om toegang tot de organisatie te krijgen. Overigens kan bijvoorbeeld LinkedIn voor hetzelfde doeleinde ingezet worden, want je kunt zoeken op organisaties en personen die daar werken. Het risico bij de metadata is groter, omdat een aanvaller documenten als referentie kan gebruiken, wat een spear-phishing geloofwaardig kan maken.

In deze memo vraag ik je besluit op mijn advies:

1. Alle documenten in het publieksportaal van Ibabs tot 2 jaar geleden (tot 1 september 2022) te controleren op persoonsgegevens van inwoners en ambtenaren in de metadata en indien nodig te anonimiseren.
2. Alle overige documenten in het publieksportaal te verwijderen en alleen via een Woo-verzoek ter beschikking te stellen.

Reactie leverancier Ibabs en VNG

De servicedesk van Ibabs heeft aangegeven, dat de verantwoordelijkheid voor het anonimiseren bij de opsteller van de documenten ligt en niet bij de leverancier. Bovendien staan zij voor "transparantie en beschikbaarheid van documenten" en daar hoort voor hen ook de optie van downloaden bij. Annuleren of deactiveren van de optie tot downloaden per gemeente is ook niet iets waar zij voor open staan.

Contact met de VNG heeft ook geen resultaat opgeleverd richting de leverancier, want de VNG wordt door deze leverancier niet gezien als klant. Zij gaan derhalve niet in gesprek met hen. Andere leveranciers hebben juist wél positief gereageerd en meegedacht over aanpassingen in hun applicatie. Want hoewel de leverancier van Ibabs gelijk heeft, dat wij als opstellers van documenten verantwoordelijk zijn voor de inhoud, heeft de leverancier de verantwoordelijkheid om een applicatie te leveren die ons in staat stelt aan de AVG te voldoen. Niet langer te kunnen downloaden, is de meest ideale oplossing daarvoor. In afwachting van een landelijke vuist richting deze leverancier, is er vanuit de gemeente een tweetal acties nodig; ervoor zorgen dat er geen nieuwe datalekken bij komen en ervoor zorgen dat de metadata in de huidige bestaande documenten worden beoordeeld op risico en deze vervolgens anonimiseren waar dat nodig is.

1. **Voorkomen van nieuwe datalekken**

Voordat een document wordt gepubliceerd, moet er een publicatie-zaak in het zaaksysteem worden aangemaakt, waarin de documenten geanonimiseerd worden opgenomen (dus ook de metadata). Pas dan kan een document opgenomen worden in Ibabs. Dit hoort de verantwoordelijkheid te zijn van de opsteller/indiener van het document of dossier. Een werkinstructie wordt gemaakt en gedeeld via intranet.

2. **Beeindigen van de bestaande datalekken in Ibabs**

De IBD/VNG, die daarover met een aantal gemeenten contact heeft gehad, adviseert om alle documenten tot 1 jaar terug, dus tot 1 september 2023, te beoordelen op risico voor betrokkenen en dan over te gaan tot controle op persoonsgegevens in de metadata en deze, indien aanwezig, te anonimiseren. Alle overige documenten, ouder dan 1 jaar geleden, worden daarbij buiten beschouwing gelaten. Het risico voor betrokkenen is al klein en bij oudere documenten nog kleiner. Daarbij weegt de inspanning die hiervoor gedaan moet worden, niet op tegen het risico voor de betrokkenen. Dit is dan in overeenstemming met artikel 33 en 34 AVG.

Na het lezen van eerder genoemde blog, adviseer ik om het aantal documenten dat inzichtelijk is via het publieksportaal te beperken. Niet vanwege het risico voor de ambtenaren of inwoners, maar veel meer vanwege het risico voor de organisatie. Dus, hoewel het een enorme klus zal zijn, alle documenten in de publieksportaal van Ibabs ontdoen van de metadata.

Daarnaast alle documenten die horen bij het vorige college/gemeenteraad, niet langer rechtstreeks beschikbaar te houden. Dat betekent dat er een lijst wordt gemaakt van documenten die bij de betreffende agenda horen, welke via een Woo-verzoek opgevraagd kunnen worden.

Om een indicatie te geven; hieronder het aantal dossiers in Rex, met als zaaktype Collegevoorstel of Raadsvoorstel. In deze dossiers kunnen meerdere documenten zitten, die dan op persoonsgegevens gecontroleerd moeten worden en vervolgens geanonimiseerd:

Zaaktype	1-9-2023 tot heden	1-9-2022 tot heden	1-1-2018 tot heden
Collegevoorstel	547	943	1896
Raadsvoorstel	158	260	503

Overleg met RPA voor het bouwen van een robot

Er is overleg geweest met het team van RPA om de mogelijkheden voor het inrichten van een robot die documenten kan controleren en kan komen tot een overzicht van te anonimiseren documenten. De conclusie is, dat dit niet gaat helpen, omdat de documenten op verschillende plekken in de publieksportaal te vinden zijn. Ook gaat het om PDF-documenten, welke niet door een robot gecontroleerd kunnen worden.

Het datalek wordt opgenomen in het register van datalekken, waarbij de genomen maatregelen vastgelegd worden, inclusief het besluit op het al dan niet uitvoeren van een controle op de metadata van documenten in Ibabs.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1

Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 14058

Gemeente Leeuwarden

MEMO

Aan:	Directeur Bedrijfsvoering 5.1.2e
Van:	Functionaris Gegevensbescherming 5.1.2e
Datum:	13 januari 2026
Onderwerp:	Advies op nieuwe dashboard met data voor Meldingen openbare ruimte (MOR)
Registratienummer:	2026-007772

Inleiding
Jaarlijks ontvangt en verwerkt gemeente Leeuwarden ruim 30.000 meldingen van inwoners over de openbare ruimte. Deze worden binnen de volgende afdelingen verwerkt: Inrichting en Beheer Buitenruimte (IBB), Vergunningverlening, Toezicht en Handhaving (VTH), Project Management Bureau (PMB), Handhaving en team Service en Informatie (S&I).

Sinds juni 2023 gebeurt dit via het systeem Signalen, waarmee Melddesk is vervangen. Deze overstap volgde op een rekenkameronderzoek naar onze dienstverlening, met als doel de ervaren ontevredenheid van burgers aan te pakken.

Ontwikkeling Dasboards
De dashboards zijn ontwikkeld om de dienstverlening aantoonbaar te verbeteren en op peil te houden. Ze bieden inzicht in het meldingenproces en ondersteunen leidinggevenden bij het voeren van het goede gesprek over prestaties.

Belangrijkste kenmerken:
- Visualisatie van reeds bekende gegevens
- Toegang uitsluitend voor functionarissen met een rol in het MOR-proces
- Rolgebonden toegang via Cognos:
    - Management: directie en sectormanagers
    - Teamleiders: inzicht per team en medewerker
    - Operationeel: kwaliteitsmedewerkers voor procesanalyse
    - Keten: proceseigenaar en procesregisseur voor analyse op hoofdlijnen

Risico-aspecten
Onderstaande aspecten zijn in het gesprek met de FG besproken en behandeld:

- Rollen en autorisaties;
  Afhankelijk van de functie is de toegang tot Signalen en daarmee tot de informatie vanuit het dashboard ingeregeld. In het ketendashboard en het operationeel dashboard is het mogelijk om door te klikken naar een specifieke melding, maar dit gebeurt uitsluitend via de applicatie Signalen, waar de bestaande autorisaties en blokkades gelden. Hierdoor blijft de toegang tot persoonsgegevens strikt rolgebonden.

- Controle op rollen en autorisaties;
  Elke maand ontvangt de functioneel beheerder een lijst vanuit Mens & Organisatie (M&O) met een overzicht van verplaatste of vertrokken medewerkers. De rollen en autorisaties worden indien nodig aangepast.

- Inzage in persoonsgegevens van melders;
  In het ketendashboard en het operationeel dashboard is het mogelijk om door te klikken naar een specifieke melding, maar dit gebeurt uitsluitend via de applicatie Signalen, waar de bestaande autorisaties en blokkades gelden. Hierdoor blijft de toegang tot persoonsgegevens strikt rolgebonden.

- Risico bij delen van de Cognos-link naar het dashboard;
  Er is alleen toegang tot het dashboard als de ontvanger van de link een autorisatie heeft voor Cognos én voor Signalen. Is dat het geval, dan is er alleen toegang tot de gegevens vanuit Signalen, welke passen bij de rol van de ontvanger.

- Mate van inzage van teamleiders bij andere (behandel)teams;
  Teamleiders hebben inzage in de prestatiegegevens van het eigen team of een ander team, dat in dezelfde behandelgroep zit. Doorklikken naar persoonsgegevens van melders is beperkt. Kwaliteitsmedewerkers hebben die optie wel; dit is vanuit hun rol en functie ook noodzakelijk.

- OR instemmingsrecht in verband met prestatiegegevens;
  Informeren van de OR is voldoende; in november 2021 is de Regeling gebruik prestatiegegevens vastgesteld door het College. Hierin zijn regels opgesteld rondom het gebruiken en bewaren van prestatiegegevens.

- Technische aspecten bij inzetten van de app;
  In april 2025 is de toepassing van de app besproken met de Information Security Officers (ISO) van gemeente Leeuwarden. Die heeft geen bezwaren opgemerkt op het gebied van techniek of informatiebeveiliging.

Conclusie en aandachtspunt
Door de aard van de persoonsgegevens van de melders (NAW en contactgegevens), is een DEPIA niet noodzakelijk. Er is evengoed advies ingewonnen op het gebied van informatiebeveiliging en privacy in verband met de inzet van een app en de ontwikkeling van het dashboard.

Door de toegang tot persoonsgegevens van melders te beperken en in te richten per rol, is privacy by design toegepast, waarmee de risico's voor melders zo klein mogelijk zijn gemaakt.
De controle op autorisaties is goed ingericht en zorgt voor minimalisatie van het risico op ongeautoriseerde toegang.

De risico's die van toepassing kunnen zijn met betrekking tot ongeoorloofde of uitgebreide toegang tot persoonsgegevens van melders, zijn goed overdacht en geminimaliseerd.

Aandachtspunt:
Wat overblijft is de bewaartermijn rondom de prestatiegegevens. Pas het "Reglement gebruik prestatiegegevens" toe met betrekking tot het bewaren van de prestatiegegevens en informeer de eigen medewerkers over het gebruik van prestatiegegevens.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1

Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 14058

Gemeente Leeuwarden

MEMO

Aan:	Sectormanager SDF
Van:	Functionaris Gegevensbescherming
Datum:	2 okober 2025
Onderwerp:	Advies gebruik Teams binnen SDF
Registratienummer:	2025-258045

Inleiding

Tijdens gesprekken eind augustus en september tussen de privacy officers en de sectormanager is de wens uitgesproken om een advies te krijgen rondom het gebruik van Teams binnen het SDF. Dit naar aanleiding van de zoektocht naar een nieuw systeem en de uitlatingen daarover vanuit Informatiemanagement. Hieronder mijn advies, gevolgd door de uitleg daarover.

Advies

Mijn advies is om een applicatie in te richten/in gebruik te nemen, waarmee samenwerken in dossiers voldoet aan geldende wet- en regelgeving (waaronder, maar niet uitsluitend: AVG, UAVG, Archiefwet en sectorale wetgeving). Dat betekent dat deze applicatie moet voldoen aan voorwaarden rondom oa logging, autorisatiebeheer, bewaar- en vernietigingstermijnen.

Richt daarnaast Teams in als een kanaal voor samenwerking, waarbij uitdrukkelijk persoonsgegevens géén onderdeel zijn van die samenwerking.
Maak afspraken waarvoor Teams wel wordt gebruikt.

Uitleg advies

Teams is een applicatie waarmee kan worden samengewerkt en worden vergaderd/overlegd. Teams heeft behoorlijke beperkingen, als het gebruikt wordt voor de (tijdelijke) opslag van (bijzondere of gevoelige) persoonsgegevens.

Beperkingen Teams

- **Logging** is niet aanwezig. Daardoor is dus niet te achterhalen wie wanneer inzage heeft gehad in de persoonsgegevens of wat er met de persoonsgegevens is gebeurd (delen/kopiëren/verwijderen kan zonder dat dit te achterhalen is etc.);
- **Bewaartermijnen** worden niet automatisch in acht gehouden, waardoor persoonsgegevens mogelijk te kort of te lang worden bewaard;
- **Autorisaties** kunnen niet periodiek automatisch gecontroleerd worden en zijn niet gekoppeld aan een rol of functie;
- **Vernietigen** van dossiers worden niet via de archivaris uitgevoerd. Daardoor is er geen zicht is op vernietigingstermijnen of worden er überhaupt geen vernietigingsdocumenten opgesteld.

Microsoft Amerikaans

Al in 2022 worden de Rijksoverheid en universiteiten afgeraden Microsoft Teams te gebruiken voor uitwisselen van gevoelige informatie. Dat schrijft Privacy Company in een rapport dat is opgesteld in opdracht van onder meer het Nederlandse ministerie van Justitie en Veiligheid (zie artikel van IB-P).

Dit advies heeft voornamelijk te maken met het feit dat Microsoft een Amerikaans bedrijf is. In het *Data protection impact assessment (DPIA)* ofwel de risico-inventarisatie voor privacy, informatiebeveiliging en record management, wordt onder andere gesproken over een **hoog** risico voor de bescherming van gevoelige gegevens dat bestaat bij het gebruik van Microsoft Teams. Dat risico is gerelateerd aan mogelijk opvragen van die gegevens door Amerikaanse wetshandhavings- en inlichtingendiensten. Het risico blijft gelijk als Microsoft gegevens op Europees grondgebied opslaat, omdat de VS dergelijke gegevens alsnog kan opvragen via wetten als de US Clouds Act.

Privacy Company schrijft in een samenvatting dat Microsoft gedwongen kan worden om gegevens te ontsleutelen, zolang het bedrijf toegang heeft tot de encryptiesleutel. Microsoft heeft verklaard dat het nog nooit gegevens van werknemers van publieke sectorinstellingen heeft verstrekt aan enige overheid, dus ook niet aan de Amerikaanse overheid. Microsoft schrijft zelf: Microsoft verstrekt geen persoonsgegevens van EU-burgers aan regeringen en heeft dat ook nooit gedaan.

1. Conclusie

De conclusie is dan ook dat Teams als samenwerkingsapplicatie prima gebruikt kan worden. Als daarbij dossiers worden gemaakt en in samengewerkt, waarin persoonsgegevens staan, dan loopt gemeente Leeuwarden (en alle partijen die binnen het SDF samenwerken) diverse risico's op het gebied van het toegang en beheer van deze dossiers. Datalekken zijn niet uit te sluiten, laat staan te achterhalen. Toegang en gebruik valt niet te controleren, evenals het aanhouden van bewaar- en vernietigingstermijnen.

Met andere woorden; archiefwet en privacywetgeving worden niet gevolgd en dat is geen wenselijke situatie.

Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 14058

Gemeente Leeuwarden

MEMO

Aan:	Wethouder Gijs Jacobse
Van:	5.1.2e
Datum:	21 oktober 2025
Onderwerp:	Update Wpg audit
Bijlagen:	1

Inleiding

In 2025 is een externe audit uitgevoerd in het kader van de registratie van politiegegevens vanuit de Wpg. Deze audit is uitgevoerd door BKBO en heeft zich gericht op het beoordelen van de opzet, bestaan en werking van processen en procedures gericht op de verwerkingen vanuit de Wpg voor de periode 2021-2024.

De resultaten waren minder goed dan verwacht. Zeker omdat er de afgelopen jaren is ingezet op het verbeteren van de opzet en het bestaan van de diverse procedures, was de verwachting dat het resultaat positiever zou zijn. De uitkomsten van de audit zijn als bijlage toegevoegd.

De uitkomst van de audit, verplicht gemeente Leeuwarden tot het opstellen van een verbeterplan. Dit plan moet binnen 3 maanden na het definitieve rapport worden opgesteld en de verplichte heraudit op dat verbeterplan moet binnen 1 jaar worden uitgevoerd.

Externe ondersteuning

De afgelopen jaren is gebleken dat het de 3 domeinen (Handhaving OOV, Leerplicht en Sociale recherche) niet lukt om te komen tot het volledig oplossen van de bevindingen. De verantwoordelijke sectormanagers hebben toegezegd externe ondersteuning in te zetten op de uitvoering daarvan. Er is een offerte opgesteld door Implére, een kleine organisatie met veel kennis van de Wpg en het verbeteren van de processen en procedures.

Daarnaast worden de kwaliteitsmedewerkers die met de bevindingen aan de slag gaan, intern begeleid vanuit projectmanagement.

Heraudit medio 2026

Met de ondersteuning van Implére, die niet alleen bij opzet en bestaan gaat helpen, maar ook de werking gaat borgen door instructies te geven aan de boa’s, wordt het verbeterplan op de juiste wijze uitgevoerd. De verwachting is dan, dat heraudit die medio 2026 wordt uitgevoerd, een resultaat weergeeft dat past bij de geleverde inspanningen.

Zodra er nieuwe informatie gegeven kan worden over de status van de verbeteringen, zal ik dit via het Portefeuilleoverleg laten weten.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1

M2511 4186 LDA-experiment - (nog) minder typen, (nog) meer luisteren

5.1.2e (Gemeente Leeuwarden)

Aanmelder

Naam	5.1.2e
Locatie	Gemeente Leeuwarden
Inlognaam netwerk	5.1.2e
Aanspreekvorm aanmelder	[Naam]
Telefoonnummer	5.1.2e
E-mail	5.1.2e @leeuwarden.nl
Kostenplaats	AO-CS-Mid - CS-Middelen
Organisatie	Gemeente Leeuwarden

Details

Korte omschrijving	LDA-experiment - (nog) minder typen, (nog) meer luisteren
Soort 'Melding'	Service verzoek SC
Categorie	LWD - Privacy
Subcategorie	DEPIA

Object

Object ID	Shared Service Centrum
Soort	Domeinen
Locatie	Gemeente Leeuwarden

Planning

Impact	Normaal
Urgentie	Normaal
Prioriteit	Prio 3
Streefdatum	28 mei 2026 17:00
Doorlooptijd	3 dagen
On hold	Nee

Afhandeling

Behandelaar	5.1.2e
Behandelaarsgroep	LWD Privacy
Status	Opgelost/Hersteld
Afgemeld	Ja
Datum afgemeld	1 april 2026 9:18
Geregistreerde tijd	00:00

Verzoek

5.1.2e 19 november 2025 7:47

Het experiment (nog) minder typen, (nog) meer luisteren heeft een doorstart gevonden in ronde 10 van de LDA. Er is een subsidie van 50K uitgegeven vanuit de VNG die 2025 opgemaakt moet worden. Een externe partij (5.1.2i) gaat een DEPIAMA doen 17-12.

Met concerncontroller afgesproken hier zelf bij aan te haken. Vandaar nu melding gemaakt in 5.1.2i. Even op eigen naam.

Actie

van 5.1.2e 1 april 2026 9:19

Advies gegeven aan Harm, experiment is uitgevoerd op basis van dat besluit. Is in mails opgenomen, welke opgenomen worden in zaak in 5.1.2i: 2026-088150.
Omdat het experiment is uitgevoerd, kan deze melding afgesloten worden. Mocht er sprake zijn van gewenste inzet in de uitvoering, zal dit als normaal proces moeten worden opgepakt. Dus via PPM-proces etc.

5.1.2e 4 december 2025 11:24

17-12 sessie met 5.1.2i voor IAMA/DPIA

5.1.2e Mailimport 24 november 2025 7:54

Ha 5.1.2e !

Dank je wel voor je uitgebreide reactie en je enthousiasme!
Fijn dat jullie ook zo enthousiast worden. 5.1.2e en ik hebben gisteren gesproken met 5.1.2i en hebben de 17e vastgezet.

Aan ons om voor dit tijd het DEPIA-Format en onze ethische waarden te delen. Zodra ik deze laatste van 5.1.2e heb ontvangen zal ik alles in een keer doorzetten.
Ook de use cases moeten we nog iets verder uitwerken, dat doen we op het moment dat de collega's vanuit Sociaal bekend zijn. 5.1.2e heeft er net een mail uitgedaan naar de teamleiders daar om weer collega's te werven.

5.1.2e is bezig wat achtergrondonderzoek naar de tools nav jullie gesprek. Ik hoop ook de tool voor de 17e helder

te hebben. Op zich niet erg als die nog niet bekend is, geeft wel beter inzicht als die er al wel is.

Tot slot; 5.1.2i heeft 2 weken de tijd nodig om tot een rapportage te komen, die verwacht ik dus de eerste week van januari ergens. Kunnen jullie daarmee rekening houden in jullie agenda's? Ik ben naast het advies natuurlijk ook heel benieuwd naar jullie feedback op het rapport en de werkwijze zelf.

Fijn weekend alvast!

Groet,

5.1.2e

Van: 5.1.2e <5.1.2e @leeuwarden.nl>
Verzonden: Woensdag, 19 November, 2025 10:53
Aan: 5.1.2e <5.1.2e @leeuwarden.nl>; 5.1.2e <5.1.2e @leeuwarden.nl>
CC: 5.1.2e <5.1.2e @leeuwarden.nl>; 5.1.2e <5.1.2e @leeuwarden.nl>; 5.1.2e 5.1.2e <5.1.2e @leeuwarden.nl>; 5.1.2e <5.1.2e @leeuwarden.nl>; 5.1.2e <5.1.2e @leeuwarden.nl>
Onderwerp: DPIAMA - 5.1.2i + verkenning Tools M2511 4186

Hi 5.1.2e,

N.a.v. ons overleg vorige week maandag, heb je ons wat stukken toegestuurd. 5.1.2e 5.1.2e en ik hebben even naar de stukken gekeken van 5.1.2i en daar werden we eigenlijk wel enthousiast van!
Je stuurde ons ook een rapportage van de DPIA bij WerkSaam en de vragen die de FG van WerkSaam nog had gesteld. Ook dit zag er goed uit.
Volgens mij een erg bekwame partij die dit samen met ons kan gaan doen.

Kortom, veel mooie dingen gelezen. Ik heb het projectvoorstel met onze opmerkingen/suggesties ook even in de bijlage gevoegd. Je gaf aan tijdens dit overleg dat als deze sessie gaat plaatsvinden, het dan niet zo moet zijn dat we daarna nog onze eigen DEPIA-format en/of data-ethiek-vragen moeten beantwoorden. Terecht ook, want er gaat veel tijd en moeite (én geld) in zitten. Omdat de bijlagen alleen een rapportage van de DPIA bij WerkSaam bevatte én aanvullende vragen van de FG van WerkSaam, konden we niet zien welke vragen ze stellen om tot deze rapportage te komen. We konden dit dan ook niet afzetten tegen onze eigen format/data-ethische waarden en beoordelen of alles op deze manier geraakt wordt. Om te voorkomen dat we na deze sessie nog ‘eigen’ hoepels door moeten op dit vlak, is ons voorstel wel om onze data-ethische waarden en eigen format mee te nemen in die sessie van de 17e (en dus ook in de rapportage). Zo hebben we gewoon een compleet beeld én voorkomen we dat we na de sessie nog vragen/risico’s moeten aftikken. Ik heb ons DEPIA-format bijgevoegd. @5.1.2e ik kon de stukken voor data-ethiek niet 123 vinden, kan jij die ook alvast delen? Dat scheelt in de voorbereiding weer. Misschien is het mogelijk dat 5.1.2i nog hun format ook met ons wil delen.

Gister heb ik samen met 5.1.2e en 5.1.2e een overleg gehad om verschillende tools te verkennen. Er waren als het ware 4 opties. We hebben gezamenlijk een afweging gemaakt en zijn uiteindelijk gekomen tot 2 tools die zich, volgens ons, goed voor dit experiment zouden kunnen lenen:

1. Veilignotuleren 5.1.2e
1. Nederlands bedrijf, gegevens worden binnen de EER opgeslagen.
2. Gegevens worden niet gedeeld met externe partijen en/of cloudproviders.
3. Geven aan volgens de BIO en ISO-27001-certificering te werken. Al lijkt het niet heel duidelijk of ze ook gecertificeerd zijn. Dit gaat 5.1.2e nog even uitvragen.

- 5.1.2i (5.1.2i)

1. De tool die WerkSaam ook gebruikt (en waar dus die DPIA van 5.1.2i op toeziet).
2. Wordt veel in de zorgsector gebruikt (waar dus ook bijzondere/gevoelige persoonsgegevens veelvuldig verwerkt wordt, waardoor dit mogelijk weer beter toepasbaar is op de ‘gevoeligere’ processen bij ons).
3. Zie ook dat deze toegepast wordt bij het sociaal domein van gemeente Westerkwartier, Tilburg en Amersfoort (nog wel de moeite waard om contact met hen op te nemen? Ik heb nog wel contactgegevens van de privacy-mensen van Amersfoort, dus ik kan wel even bij hen horen)
4. Niet helemaal duidelijk waar de gegevens opgeslagen zijn? 5.1.2e vond in ieder geval al een pagina dat ze veel geregeld hebben op gebied van Informatiebeveiliging (certificering, SOC2, etc). Dat is voor privacy uiteraard ook van belang!

Andere opties waren Plaud AI en Transcriptonline. Deze zien we liever niet. Plaud slaat alles in de US op en Transcript online is niet heel transparant in hoe ze werken, wat ze met de gegevens doen, waar ze opgeslagen worden, etc. Dat maakt dus dat we in gezamenlijkheid deze afweging hebben gemaakt. Mooiste zou zijn dat we voor de 17e al een tool voor ogen hebben, zodat we die ook mee kunnen nemen in de risico-afwegingen die

gemaakt moeten worden bij de DPIAMA.

Nog een laatste puntje voor ik deze, ietwat lange, mail afsluit: Ik zie dat er voor de 17e nog geen mensen uit de business aangesloten zijn, het zou juist mooi zijn als we ook een aantal collega's weten te vinden die hier mogelijk mee gaan experimenteren. Zo kunnen we hun invalshoeken ook meenemen in de DPIAMA.

Als er nog vragen zijn, dan hoor ik het graag! En anders tot de 17e!

P.S. ik heb iedereen waar ik mee gesproken heb over dit experiment in de CC meegenomen (ter info). Dat scheelt me weer mailtjes.

Met vriendelijk groet,

5.1.2e

5.1.2e | Privacy Officer
Concern
E 5.1.2e @leeuwarden.nl
T 5.1.2e | **M** 5.1.2e

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000, 8900 JA LEEUWARDEN
5.1.2e

5.1.2e

Werkdagen: maandag, dinsdag, woensdag en donderdag

5.1.2e Mailimport 19 november 2025 10:53

Hi 5.1.2e,

N.a.v. ons overleg vorige week maandag, heb je ons wat stukken toegestuurd. 5.1.2e 5.1.2e en ik hebben even naar de stukken gekeken van 5.1.2i en daar werden we eigenlijk wel enthousiast van!
Je stuurde ons ook een rapportage van de DPIA bij WerkSaam en de vragen die de FG van WerkSaam nog had gesteld. Ook dit zag er goed uit.
Volgens mij een erg bekwame partij die dit samen met ons kan gaan doen.

Kortom, veel mooie dingen gelezen. Ik heb het projectvoorstel met onze opmerkingen/suggesties ook even in de bijlage gevoegd. Je gaf aan tijdens dit overleg dat als deze sessie gaat plaatsvinden, het dan niet zo moet zijn dat we daarna nog onze eigen DEPIA-format en/of data-ethiek-vragen moeten beantwoorden. Terecht ook, want er gaat veel tijd en moeite (én geld) in zitten. Omdat de bijlagen alleen een rapportage van de DPIA bij WerkSaam bevatte én aanvullende vragen van de FG van WerkSaam, konden we niet zien welke vragen ze stellen om tot deze rapportage te komen. We konden dit dan ook niet afzetten tegen onze eigen format/data-ethische waarden en beoordelen of alles op deze manier geraakt wordt. Om te voorkomen dat we na deze sessie nog 'eigen' hoepels door moeten op dit vlak, is ons voorstel wel om onze data-ethische waarden en eigen format mee te nemen in die sessie van de 17e (en dus ook in de rapportage). Zo hebben we gewoon een compleet beeld én voorkomen we dat we na de sessie nog vragen/risico's moeten aftikken. Ik heb ons DEPIA-format bijgevoegd. @5.1.2e ik kon de stukken voor data-ethiek niet 123 vinden, kan jij die ook alvast delen? Dat scheelt in de voorbereiding weer. Misschien is het mogelijk dat 5.1.2i nog hun format ook met ons wil delen.

Gister heb ik samen met 5.1.2e en 5.1.2e een overleg gehad om verschillende tools te verkennen. Er waren als het ware 4 opties. We hebben gezamenlijk een afweging gemaakt en zijn uiteindelijk gekomen tot 2 tools die zich, volgens ons, goed voor dit experiment zouden kunnen lenen:

1. Veilignotuleren 5.1.2e
1. Nederlands bedrijf, gegevens worden binnen de EER opgeslagen.
2. Gegevens worden niet gedeeld met externe partijen en/of cloudproviders.
3. Geven aan volgens de BIO en ISO-27001-certificering te werken. Al lijkt het niet heel duidelijk of ze ook gecertificeerd zijn. Dit gaat 5.1.2e nog even uitvragen.

- 5.1.2i (5.1.2i)

1. De tool die WerkSaam ook gebruikt (en waar dus die DPIA van 5.1.2i op toeziet).

2. Wordt veel in de zorgsector gebruikt (waar dus ook bijzondere/gevoelige persoonsgegevens veelvuldig verwerkt wordt, waardoor dit mogelijk weer beter toepasbaar is op de ‘gevoeligere’ processen bij ons).
3. Zie ook dat deze toegepast wordt bij het sociaal domein van gemeente Westerkwartier, Tilburg en Amersfoort (nog wel de moeite waard om contact met hen op te nemen? Ik heb nog wel contactgegevens van de privacy-mensen van Amersfoort, dus ik kan wel even bij hen horen)
4. Niet helemaal duidelijk waar de gegevens opgeslagen zijn? 5.1.2e vond in ieder geval al een pagina dat ze veel geregeld hebben op gebied van Informatiebeveiliging (certificering, SOC2, etc). Dat is voor privacy uiteraard ook van belang!

Andere opties waren Plaud AI en Transcriptonline. Deze zien we liever niet. Plaud slaat alles in de US op en Transcript online is niet heel transparant in hoe ze werken, wat ze met de gegevens doen, waar ze opgeslagen worden, etc. Dat maakt dus dat we in gezamenlijkheid deze afweging hebben gemaakt. Mooiste zou zijn dat we voor de 17e al een tool voor ogen hebben, zodat we die ook mee kunnen nemen in de risico-afwegingen die gemaakt moeten worden bij de DPIAMA.

Nog een laatste puntje voor ik deze, ietwat lange, mail afsluit: Ik zie dat er voor de 17e nog geen mensen uit de business aangesloten zijn, het zou juist mooi zijn als we ook een aantal collega’s weten te vinden die hier mogelijk mee gaan experimenteren. Zo kunnen we hun invalshoeken ook meenemen in de DPIAMA.

Als er nog vragen zijn, dan hoor ik het graag! En anders tot de 17e!

P.S. ik heb iedereen waar ik mee gesproken heb over dit experiment in de CC meegenomen (ter info). Dat scheelt me weer mailtjes.

Met vriendelijk groet,

5.1.2e

5.1.2e | Privacy Officer
Concern
E 5.1.2e @leeuwarden.nl
T 5.1.2e | **M** 5.1.2e

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000 8900 JA LEEUWARDEN
5.1.2e

5.1.2e

Werkdagen: maandag, dinsdag, woensdag en donderdag

Informatie

Aanmelddatum	19 november 2025 7:45	Standaardoplossing	Er is geen standaardoplossing gekoppeld
Gerealiseerde doorlooptijd	820:18		
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	820:18		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	820:18		
Geregistreerde tijd	00:00		

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2, 3, 4
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2, 3

From: "5.1.2e" <5.1.2e@leeuwarden.nl>
Sent: 5/17/2024 1:42:55 PM +00:00
To: "5.1.2e" <5.1.2e@leeuwarden.nl>
Cc:
Subject: RE: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen

Graag gedaan, dank en jij ook prettig weekend 5.1.2e!

Van: 5.1.2e <5.1.2e@leeuwarden.nl>
Verzonden: vrijdag 17 mei 2024 15:37
Aan: 5.1.2e <5.1.2e@leeuwarden.nl>
CC: 5.1.2e <5.1.2e@leeuwarden.nl>
Onderwerp: RE: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen

Hoi 5.1.2e,
Dank voor de terugkoppeling! Ik had toch wat haast en heb toch maar alvast de melding gedaan richting de AP, daarbij wat "dichterlijke" vrijheid genomen met betrekking tot het voorkomen van dergelijke fouten in de toekomst. Wat ik zo lees, zijn prima oplossingen voor de toekomst. En vooral de aanvragers aangeven, wat wel en niet hoeft doorgegeven te worden. Dat scheelt jullie alweer heel veel controlewerk!
Jouw laatste opmerking snap ik; daarbij is toch altijd de afweging wat het risico is als we wel publiceren. Maar 5.1.2e en 5.1.2e kunnen jullie daar zeker bij helpen.

Goed weekend, ik sluit nu echt af!
Hartelijke groeten,
5.1.2e

Van: 5.1.2e <5.1.2e@leeuwarden.nl>
Verzonden: vrijdag 17 mei 2024 15:31
Aan: 5.1.2e <5.1.2e@leeuwarden.nl>
CC: 5.1.2e <5.1.2e@leeuwarden.nl>
Onderwerp: RE: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen

Goedemiddag 5.1.2e,
We hebben het gesprek naar vanmiddag verplaatst vanwege een last-minute ingelast sollicitatiegesprek welke vanochtend plaats vond.

<u>Uit de analyse zijn een aantal aspecten naar voren gekomen:</u>

- In de periode 3 t/m 10 mei werden de inboekwerkzaamheden tijdelijk overgenomen door een andere collega vanwege meivakantie afwezigheid van de vaste inboekster;
- Diegene die het tijdelijk heeft overgenomen ervaarde diverse problemen met het anonimiseren door DigiEplan. Het anonimiseren wordt niet consequent uitgevoerd door DigiEplan, controle wordt vereist en vervolgens wordt er nog manueel gecontroleerd en geanonimiseerd;
- Het opslaan in de juiste extensie is een belangrijke stap in dit proces (als PDF-bestand).

<u>Welke actie nemen we hierop:</u>

- We zijn met betroffen collega's om tafel gaan zitten om van elkaar te horen op welke manier iedereen het anonimiseren uitvoert. Dit gebeurt op verschillende manieren. Men gaat bij elkaar meekijken om te begrijpen waar e.e.a. mis kan gaan om daarvan te leren;
- Nogmaals de WEP-checklist die destijds gedeeld en gepresenteerd is doorheen te gaan;
- In overleg met de Privacy Officer willen we bespreken of we aan de voorkant afspraken kunnen maken waarbij de aanvrager de suggestie krijgt aangeleverde data door de aanvrager al te anonimiseren (zodat wij dat niet meer hoeven te doen);
- Waar onduidelijkheid over bestaat is het nut in het voorbeeld "Schildersbedrijf 5.1.2e waarbij de eigenaar 5.1.2e is" en die zou geanonimiseerd moeten worden. Dit vragen we na bij de Privacy Officer

Heb je hier voldoende input mee?
Gr.

5.1.2e

Senior Team vergunningen & leefomgeving
E 5.1.2e@leeuwarden.nl
T 5.1.2e

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000, 8900 JA LEEUWARDEN
T 14 058 | www.leeuwarden.nl | Twitter | Facebook

GLOBAL GOALS GEMEENTE

Van: 5.1.2e <5.1.2e@leeuwarden.nl>
Verzonden: vrijdag 17 mei 2024 13:34

Aan: [redacted] <[redacted]@leeuwarden.nl>
CC: [redacted] <[redacted]@leeuwarden.nl>
Onderwerp: RE: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen
Hoi [redacted],
Kun je me bijpraten over het gesprek met [redacted] en dan vooral over de borging van het proces van publicatie van vergunningen?
Hartelijke groeten,
[redacted]

Van: [redacted] <[redacted]@leeuwarden.nl>
Verzonden: woensdag 15 mei 2024 15:18
Aan: [redacted] <[redacted]@leeuwarden.nl>; [redacted] <[redacted]@leeuwarden.nl>
Onderwerp: Re: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen
Spreken we het zo af en dank voor de extra toelichting [redacted].
Verzonden vanaf Outlook voor Android

From: [redacted] <[redacted]@leeuwarden.nl>
Sent: Wednesday, May 15, 2024 3:08:45 PM
To: [redacted] <[redacted]@leeuwarden.nl>; [redacted] <[redacted]@leeuwarden.nl>
Subject: RE: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen
Wat mij betreft ook hoor. Ik wil daarbij wel benadrukken dat het me niet gaat om de “schuldvraag”, maar eerder op voorkomen richting de toekomst. En dan het laatste vooral procedureel voorkomen. Dat er fouten gemaakt worden, is heel logisch en niet meer dan normaal.
Hartelijke groeten,
[redacted]

Van: [redacted] <[redacted]@leeuwarden.nl>
Verzonden: woensdag 15 mei 2024 15:07
Aan: [redacted] <[redacted]@leeuwarden.nl>
CC: [redacted] <[redacted]@leeuwarden.nl>
Onderwerp: Re: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen
Wat mij betreft prima.
[redacted], wat jou betreft ook?
Verzonden vanaf Outlook voor Android

Van: [redacted] <[redacted]@leeuwarden.nl>
Verstuurd: woensdag, mei 15, 2024 3:02:00 p.m.
Aan: [redacted] <[redacted]@leeuwarden.nl>
CC: [redacted] <[redacted]@leeuwarden.nl>
Onderwerp: RE: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen
Hoi [redacted],
Ik heb vrijdagochtend a.s. een overleg met [redacted] gepland staan en bespreken we deze beide voorvallen. De uitkomst van dat gesprek koppel direct daarna terug naar [redacted].
Morgen is mijn verlofdag en lukt het niet om af te stemmen (ik verwacht hier samen met [redacted] wel uit te komen).
Gr.
[redacted]

Van: [redacted] <[redacted]@leeuwarden.nl>
Verzonden: woensdag 15 mei 2024 14:39
Aan: [redacted] <[redacted]@leeuwarden.nl>
CC: [redacted] <[redacted]@leeuwarden.nl>
Onderwerp: Fwd: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen
Hoi [redacted],
Wil jij dit afstemmen / oppakken met [redacted]?
Waar nodig ben ik er morgen om met je af te stemmen hierover. Vrijdag vrije dag namelijk.
Alvast bedankt,
[redacted]
Verzonden vanaf Outlook voor Android

Van: Functionaris Gegevensbescherming <fg@leeuwarden.nl>
Verstuurd: woensdag, mei 15, 2024 2:36:10 p.m.
Aan: [redacted] <[redacted]@leeuwarden.nl>
Onderwerp: contact via mail over 2 nieuwe datalekken bij publicatie vergunningsaanvragen
Hoi [redacted],
Vandaag zijn er twee nieuwe datalekken gemeld vanwege het niet juist/niet anonimiseren van vergunningsaanvragen. Ik maak nog een afweging om deze wel of niet te melden bij de AP, afhankelijk van de verdere uitkomsten van ons onderzoek.
Voor het geval ik wel ga melden, heb ik wel een goede verklaring nodig richting de Autoriteit Persoonsgegevens. Natuurlijk zijn dergelijke taken en fouten altijd mensenwerk, maar aanvragers mogen ook van ons verwachten dat

wij de publicaties zo goed mogelijk uitvoeren.
Dat betekent dus, dat ik graag hoor wat er wordt ingezet om dergelijke fouten zoveel als mogelijk te voorkomen.
Hoe zit het bijvoorbeeld met het toepassen van DigiEplan, werkt dat nog steeds zodanig vertragend, dat de anonimisering vooral handmatig wordt uitgevoerd? Omdat onze beide agenda's erg vol zijn, toch maar even via de mail mijn vragen gesteld, want ik moet uiterlijk zaterdag een melding doen naar de AP. Je snapt dat ik dat toch vooral bij voorkeur vrijdag afhandel 😉.
Hartelijke groeten,

5.1.2e | Functionaris Gegevensbescherming
Concern

E fg@leeuwarden.nl
T 5.1.2e | **M** 5.1.2e

1.

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000, 8900 JA LEEUWARDEN
T 14 058 | www.leeuwarden.nl | Twitter | Facebook

GLOBAL GOALS GEMEENTE

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2, 3

From: "5.1.2e " <5.1.2e @leeuwarden.nl>
Sent: 2/24/2026 8:53:30 AM +00:00
To: "5.1.2e " <5.1.2e @leeuwarden.nl>
Cc:
Subject: Re: DPIAMA transcribeertool Gemeente Leeuwarden 1.0

Hoi 5.1.2e ,

Scherp van je, dat klopt inderdaad. Ik heb beide aangepast/aangescherpt.
Dan rest ons niets anders dan aan Harm vragen of hij akkoord kan gaan met de procedure zoals hieronder is opgeschreven ;)

Ik stuur Harm zo een mail met jou en 5.1.2e in de cc.

Groet,

5.1.2e

Van: 5.1.2e
Verzonden: Dinsdag, 24 Februari, 2026 08:43
Aan: 5.1.2e
Onderwerp: RE: DPIAMA transcribeertool Gemeente Leeuwarden 1.0

Hoi 5.1.2e
Ik heb nog een vraag over de vergelijking tussen beide verslagen; dat kan volgens mij niet direct na het gesprek. Ik neem nl aan dat de consulent betrokken bij het dossier, dit nog moet uitwerken?
Verder misschien goed om bij het vragen van de client duidelijk aan te geven dat het AI-rapport wordt vernietigd na bespreking en dus niet onderdeel is van het dossier.
Verder is het zoals we hebben afgesproken.
Hartelijke groeten,

5.1.2e |Functionaris Gegevensbescherming
gemeente Leeuwarden, Vlieland, Terschelling, Ameland, Schiermonnikoog

E fg@leeuwarden.nl
T 5.1.2e | **M** 5.1.2e

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000, 8900 JA LEEUWARDEN
5.1.2e

GLOBAL GOALS GEMEENTE

Van: 5.1.2e
Verzonden: maandag 23 februari 2026 17:26
Aan: 5.1.2e
Onderwerp: Re: DPIAMA transcribeertool Gemeente Leeuwarden 1.0
Hoi 5.1.2e
ZOals vanmiddag besproken:

Voorstel werkwijze bij experiment 'Meer luisteren, minder typen'

Voorafgaand aan het gesprek

- Collega-consulent die niet betrokken is op het dossier belt de inwoner vooraf (3 dagen om voldoende bedenktijd) of hij/zij wil deelnemen aan een test waarbij het gesprek ook wordt getranscribeerd met behulp van 5.1.2i . De Collega-consulent die niet betrokken is op het dossier geeft hierbij duidelijk aan dat weigering geen gevolgen heeft voor hun

gesprek en geen gevolgen heeft voor de inspanningen die de gemeente verricht om de inwoner aan het werk te krijgen. Er zijn dus geen nadelige gevolgen van weigeren.

- Bij dit gesprek wordt uitgelegd dat:
  - het gesprek gewoon doorloopt zoals altijd,
  - er een extra verslag wordt gemaakt via automatische transcriptie,
  - dit verslag aan het einde samen wordt doorgenomen.
  - Dit verslag niet opgenomen wordt in het dossier, maar verwijderd.

Tijdens het gesprek

- Betrokken consulent op dit dossier voert het gesprek met de inwoner.
- Betrokken consulent op dit dossier maakt notities op de gebruikelijke, handmatige manier.
- Collega-consulent die niet betrokken is op het dossier zit bij het gesprek, maar heeft geen actieve rol in het gesprek zelf.
- Collega-consulent die niet betrokken is op het dossier start en beheert de transcriptie in 5.1.2i.

Na afloop van het gesprek

- Collega-consulent die niet betrokken is op het dossier toont het automatisch gegenereerde verslag aan de inwoner.
- Samen wordt besproken:
  - of het verslag een realistische en volledige weergave is van het gesprek,
  - of er onnauwkeurigheden of omissies zijn.
  - Vragenlijst over hoe het gesprek is ervaren (enquêtevragen via 5.1.2e).
- Het gespreksverslag wordt niet opgeslagen of gebruikt in het dossier. Het handmatige opgestelde verslag (de gebruikelijke manier) zal worden opgeslagen
- Vergelijking tussen het gemaakte verslag door AI en door de consulent. Eventuele verschillen in de 2 verslagen worden genoteerd ter lering.
- Na de vergelijking wordt het gespreksverslag verwijderd.

Groeten

5.1.2e

Van: 5.1.2e <5.1.2e@leeuwarden.nl>
Verzonden: Maandag, 2 Februari, 2026 19:43
Aan: 5.1.2e <5.1.2e@leeuwarden.nl>
CC: 5.1.2e <5.1.2e@leeuwarden.nl>; 5.1.2e <5.1.2e@leeuwarden.nl>
Onderwerp: FW: DPIAMA transcribeertool Gemeente Leeuwarden 1.0

Hoi 5.1.2e

Zie in de bijlage de definitieve versie van de DPIAMA en het advies van de FG.

Ik heb haar advies hieronder integraal overgenomen, dan hoef je het document niet door helemaal door te lezen.

4.2 Beoordeling en advies FG

In deze DEPIA gaat het om transcriberen van gesprekken als middel. Wat is het doel dat hoort bij dit middel? Het gekozen middel wordt gebruikt in twee verschillende processen: uitvoeren van de participatiewet en voeren werkoverleggen. Het doel lijkt te zijn: meer efficiency bij de uitvoering van deze twee processen. Deze twee processen hebben elk een andere rechtsgrond. Daardoor is het DPIA-rapport lastig te beoordelen. Punten van aandacht: De doelomschrijving is niet helemaal helder omdat het hier eigenlijk gaat om de inzet van een middel.

Het doel van de participatiewet is kort gezegd het uitvoeren daarvan (art. 6 lid 1 onder e AVG). Het doel van de werkoverleggen is bedrijfsvoering waarbij wordt verwezen naar 160 gemeentewet (art. 6 lid 1 onder f AVG). Deze twee grondslagen en doelen verschillen erg van elkaar. De twee processen kunnen niet samen worden beoordeeld. Voor beide grondslagen moet worden voldaan aan voorwaarden uit de AVG.

Mijn advies: voor de inzet van een transcribeertool voor beide soorten processen uitgaan van de grondslag gerechtvaardigd belang. Daar hoort vervolgens bij:

1. Aantonen rechtsgrond voor het verwerken van bijzondere en strafrechtelijke persoonsgegevens.

2. Aantonen van de noodzaak van het gebruiken van deze oplossing voor deze grondslag.

3. Belangenafweging uitvoeren (belang afwegen tegen privacy-impact betrokkenen)

4. Derdenverwerking buiten de EER laten toetsen door de CISO (Nis2/ BIO(2). (als dat niet al gedaan is; maakte ik niet op uit document).

5. Toon aan dat de AI-verordening wordt nageleefd. Zie website AP: https://www.autoriteitpersoonsgegevens.nl/themas/algoritmes-ai/ai-verordening/risicogroepen-ai-verordening

De inzet van deze tool bij een kwetsbare groep blijft een risico voor het niet naleven van de AVG. Mijn advies is om een andere vorm van testen in te zetten, waarbij er geen sprake is van de verwerking van bijzondere of strafrechtelijke gegevens van betrokkenen.

Datum: **02-01-2026**	**Voorafgaande raadpleging AP nodig**: nee

Het is volgens ons nu aan de proceseigenaar ([5.1.2e] en/of [5.1.2e]?) om een besluit te nemen. Zal ik dit aan hen voorleggen of wil jij dit liever doen?

Besluit is op meerdere onderdelen:

- Kan deze, ondanks de genoemde risico's, akkoord gaan met de inzet van [5.1.2i] in het proces van team Werk tbv het experiment 'Minder typen, meer luisteren'?
- Kan deze, ondanks de genoemde risico's, akkoord gaan met de inzet van [5.1.2i] in overleggen van team A&A en team I&I tbv het experiment 'Minder typen, meer luisteren'?

En tot slot;

- Vanuit de secretariële ondersteuning is er vergaande interesse in ons experiment, vanuit zowel de Diva's als het sociaal domein. Omdat ons DPIAMA zich uitsluitend op bovenstaande processes heeft gericht, valt deze doelgroep buiten de boot. Aan de andere kant is het doel van de ondersteuning in beide interne processen gelijk. Kan deze, ondanks de genoemde risico's, akkoord gaan met de inzet van [5.1.2i] voor 1 á 2 secretaresses tbv het experiment?

Voor de duidelijkheid; het experiment loopt tot en met maart en we hebben licenties van [5.1.2i] tot juli 2026. Het besluit ziet alleen toe voor deze periode. Als transcriberen echt in productie wordt genomen volgt het reguliere PPM-proces.

We gebruiken het experiment ook om een voorzet te doen de businesscase voor in productiename van deze tool o[5.1.2e] als deze zover is. Hierover volgt nog bericht.

Let me know!

Groet,

[5.1.2e]

Van: 5.1.2e <5.1.2e @leeuwarden.nl>
Verzonden: Maandag, 2 Februari, 2026 14:49
Aan: 5.1.2e <5.1.2e @leeuwarden.nl>; 5.1.2e <5.1.2e @leeuwarden.nl>
Onderwerp: DPIAMA transcribeertool Gemeente Leeuwarden 1.0

Hoi 5.1.2e 5.1.2e

Ik blijf worstelen met deze DPIAMA. Ik wil heel graag meedenken, maar merk dat ik toch steeds terugkom op dezelfde punten van aandacht.

Ik heb een aantal opmerkingen toegevoegd en mijn advies definitief gemaakt.

Het is wat mij betreft nu aan de proceseigenaar om hier een besluit op te nemen.

Hartelijke groeten,

5.1.2e |Functionaris Gegevensbescherming

gemeente Leeuwarden, Vlieland, Terschelling, Ameland, Schiermonnikoog

E fg@leeuwarden.nl
T 5.1.2e | **M** 5.1.2e

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000, 8900 JA LEEUWARDEN
5.1.2e

GLOBAL GOALS GEMEENTE

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2, 3, 4
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1, 2, 3

From: "Jong de, Eelke" <5.1.2e @leeuwarden.nl>
Sent: 10/15/2025 3:28:33 PM +00:00
To: "5.1.2e " <5.1.2e @leeuwarden.nl>
Cc:
Subject: RE: input rondom publicatietermijn vergunningen

Beste 5.1.2e ,
Ter informatie: Het onderstaande besproken met Homme. Hij snapt het en gaat in gesprek! Andere mail ook met de nieuwe griffier besproken!
Groet,
Eelke

Van: 5.1.2e
Verzonden: dinsdag 14 oktober 2025 11:04
Aan: Jong de, Eelke
Onderwerp: input rondom publicatietermijn vergunningen
Hallo 5.1.2e
Zoals afgesproken, hierbij een overzicht van de wettelijke verplichtingen rondom publicatie van vergunningsaanvragen en de privacyrisico's die ontstaan door maximale transparantie.

Wettelijke bepalingen:

- Gemeenten **moeten** vergunningsaanvragen publiceren zodat belanghebbenden bezwaar kunnen maken.
- De **bezwaartermijn is 6 weken**, gerekend vanaf de **bekendmaking aan de aanvrager** (niet per se vanaf publicatie in het gemeenteblad).
- De **publicatie in het gemeenteblad (Huis aan Huis) of op overheid.nl** is formeel een "mededeling", niet de juridische bekendmaking. Dit is vaak wel de bron voor inwoners
- Daarna moet een vergunningsaanvraag op verzoek beschikbaar blijven.

Wanneer verwijderen

- Omdat de wettelijke verplichting tot **actieve** bekendmaking direct na afloop van de bezwaartermijn vervalt, kan de publicatie in principe worden verwijderd.
- Gebruikelijk is wel om de publicatie langer te laten staan, bijvoorbeeld:
  - Tot het besluit definitief is (geen bezwaar ingediend).
  - Tot de vergunning is uitgevoerd.
  - Of archiveren het besluit in een Woo-portaal of raadsinformatiesysteem.
- Er is geen landelijke standaard voor hoe lang deze publicaties online moeten blijven. Dit wordt lokaal bepaald, vaak in overleg met de afdeling juridische zaken en informatiebeheer.

Hieronder een overzicht van de verschillende vergunningsaanvragen, bewaartermijnen en publicatietermijnen:

Vergunningssoort	Publicatievorm	Publicatietermijn	Bewaartermijn	Duur actieve publicatie
Omgevingsvergunning	Volledige beschikking + bijlagen	Minimaal 6 weken	10 jaar (of langer bij bezwaar)	Minimaal 6 weken
Evenementenvergunning	Volledige beschikking + voorwaarden	Minimaal 6 weken	5 jaar	Minimaal 6 weken
Drank- en horecavergunning	Volledige beschikking	Minimaal 6 weken	10 jaar	Minimaal 6 weken
Exploitatievergunning	Volledige beschikking	Minimaal 6 weken	10 jaar	Minimaal 6 weken
Standplaatsvergunning	Volledige beschikking	Minimaal 6 weken	5 jaar	Minimaal 6 weken
Reclamevergunning	Volledige beschikking	Minimaal 6 weken	5 jaar	Minimaal 6 weken
Kapvergunning	Volledige beschikking + motivatie	Minimaal 6 weken	10 jaar	Minimaal 6 weken

Privacy risico's bij langdurige publicatie:

- Door onjuiste anonimisering (of gebruik van verouderde anonimiseringstechnieken) blijven persoonsgegevens van betrokkenen (aanvragers of bezwaarmakers) online vindbaar.
- Door onbekendheid rondom metadata (informatie over de informatie, zoals auteur, datum van aanmaken etc), zijn deze gegevens niet altijd geanonimiseerd vóór publicatie

Door veranderingen in technische mogelijkheden op internet kan dit steeds grotere risico's voor de betrokkenen veroorzaken. De mogelijkheden om gegevens te combineren en daar misbruik van te maken nemen steeds meer toe.
Door dergelijke aanvragen langer dan wettelijk verplicht te publiceren, kunnen door menselijke fouten risico's voor betrokkenen toenemen.
Dit is een punt van aandacht, welke een bewuste keuze vraagt rondom publicaties.
Kiezen voor maximale transparantie vraagt om actieve beperking van risico's voor betrokkenen. Daar horen dan ook de juiste tools bij voor de medewerkers die dergelijke stukken moeten publiceren. Dit geldt overigens ook voor een minder maximale transparantie ��.
Het voordeel van een kortere actieve publicatieperiode is, dat gemeente Leeuwarden met de kennis van nu, bewust rekening houdt met de risico's van publicatie en daarmee betrokkenen nog meer beschermd dan voorheen.
Hartelijke groeten,

5.1.2e |Functionaris Gegevensbescherming
gemeente Leeuwarden, Vlieland, Terschelling, Ameland, Schiermonnikoog

E fg@leeuwarden.nl
T 5.1.2e | **M** 5.1.2e

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000, 8900 JA LEEUWARDEN
T 14 058 | www.leeuwarden.nl | Twitter | Facebook

GLOBAL GOALS GEMEENTE

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1

From: 5.1.2e ' <5.1.2e @leeuwarden.nl>
Sent: 8/15/2024 1:22:08 PM +00:00
To: 5.1.2e <5.1.2e @leeuwarden.nl>, 5.1.2e ' <5.1.2e @leeuwarden.nl>, "Functionaris Gegevensbescherming" <fg@leeuwarden.nl>
Cc: 5.1.2e " <5.1.2e @leeuwarden.nl>, " 5.1.2e <5.1.2e @leeuwarden.nl>
Subject: RE: Memo datalekken bij online publicaties

Allen,
Aanvullend op onderstaande monitoringsoverzicht, heb ik deze week met de Leeuwarder Courant, 5.1.2e contact gehad om de eerste periode te evalueren zoals afgesproken. De nieuwe manier van werken waarbij de LC de verzoeken voor inzage in specifieke dossiers per mail kenbaar maakt, verloopt naar grote tevredenheid! De verzoeken worden vlot uitgevoerd zodat de opgevraagde stukken ook snel beschikbaar zijn voor de LC. Doel is om ieder verzoek binnen 2-3 werkdagen te beantwoorden afhankelijk van de grote van het dossier. Bij grotere projecten/dossiers laat de LC vooraf weten welke stukken van dat dossiers hun interesse hebben.
We hebben afgesproken over drie maanden opnieuw contact te hebben voor een volgende evaluatie.
Gr.
5.1.2e

Van: 5.1.2e
Verzonden: maandag 5 augustus 2024 15:10
Aan: 5.1.2e ; 5.1.2e ; Functionaris Gegevensbescherming
CC: 5.1.2e ; 5.1.2e
Onderwerp: RE: Memo datalekken bij online publicaties
Hoi 5.1.2e 5.1.2e,
Sinds we op 10 juni jl. gestopt zijn met het publiceren van de stukken als onderdeel van de verleende en geweigerde vergunningen (zgn. reguliere procedure), hebben we bijgehouden hoeveel verzoeken voor dossierinzage we hebben ontvangen van particulieren, bedrijven, organisatoren en separaat vermelden we de LC. Dit betreft alle vergunningen die bij V&L als bij P&V behandeld zijn en daar gepubliceerd worden; deze verzoeken ontvangen we via REX en per mail. In bijgaand overzicht zijn deze uitgesplitst en vinden jullie daarvan een eerste indruk.

Verzoek tot dossierinzage

REX						
	Inzage bouwtekeningen	OV voor 1/1/24 (Key2)	OV na 1/1/24 (CLO)	APV /Evenementen vergunning	Overig	Totaal
week 24	15	0	0	0	0	15
week 25	4	0	0	0	1	5
week 26	15	1	0	0	1	17
week 27	8	2	0	0	0	10
week 28	7	0	0	0	0	7
week 29	12	1	0	0	0	13
week 30	3	0	1	0	0	4
week 31	7	2	0	0	0	9
week 32						
	71	6	1	0	2	80

Mailbox								
	Inzage bouwtekeningen	OV voor 1/1/24 (Key2)	OV na 1/1/24 (CLO)	APV /Evenementen vergunning	Overig	Totaal	LC	
week 24	11	1	0	1	2	15		
week 25	10	0	3	1	0	14	1	1 dossier inzage
week 26	9	1	1	0	0	11		
week 27	0	1	0	0	0	1		
week 28	0	0	1	0	0	1		
week 29	4	0	1	0	0	5		
week 30	1	1	3	0	0	5	2	6 dossier inzages
week 31	4	0	2	0	0	6		
week 32								
	39	4	11	2	2	58		

Context bij het overzicht:
- OV voor 1/1/24 (Key2) – inzage in omgevingsvergunning opgestart voor 1/1/2024 (verleend)
- OV na 1/1/24 (CLO) – inzage in omgevingsvergunning opgestart na 1/1/2024 (verleend c.q. in behandeling)
- APV/Evenementenvergunning – inzage in draaiboek, afgegeven vergunning o.i.d.
- Overig: alles wat niet onder de andere vier categorieën valt (inzage ruimtelijk plan/bestemmingsplan, tekening van riolering)

Bij een volgende update wil ik ook het aantal gepubliceerde vergunningen per week meenemen in het overzicht voor een totaalbeeld.
Gr.
5.1.2e

Van: 5.1.2e <5.1.2e @leeuwarden.nl>
Verzonden: vrijdag 24 mei 2024 12:17
Aan: 5.1.2e <5.1.2e @leeuwarden.nl>; Functionaris Gegevensbescherming <fg@leeuwarden.nl>
CC: 5.1.2e <5.1.2e @leeuwarden.nl>; 5.1.2e <5.1.2e @leeuwarden.nl>
Onderwerp: RE: Memo datalekken bij online publicaties
Hoi 5.1.2e,
Ja natuurlijk, geen probleem!
Hartelijke groeten,
5.1.2e

Van: 5.1.2e <5.1.2e @leeuwarden.nl>
Verzonden: vrijdag 24 mei 2024 12:12
Aan: 5.1.2e <5.1.2e @leeuwarden.nl>; Functionaris Gegevensbescherming <fg@leeuwarden.nl>
CC: 5.1.2e <5.1.2e @leeuwarden.nl>; 5.1.2e <5.1.2e @leeuwarden.nl>
Onderwerp: FW: Memo datalekken bij online publicaties
Hoi,
Dankjewel. We spreken hier maandag over met elkaar, waarbij ik het van belang vind om 5.1.2e even zelf voor te informeren als we het eens zijn over de inhoud van de memo (hoewel hij natuurlijk al deels bekend is met de problematiek).
Bovendien zou het fijn zijn als 5.1.2e al direct kan deelnemen aan onze afstemming, mede omdat hij er inderdaad op inhoud mee verder zal gaan (samen met 5.1.2e overigens).
Wil je 5.1.2e daarom ook uitnodigen voor ons overleg van aanstaande maandag?
Alvast bedankt,
5.1.2e

Van: Functionaris Gegevensbescherming <fg@leeuwarden.nl>
Verzonden: vrijdag 24 mei 2024 09:30
Aan: 5.1.2e <5.1.2e @leeuwarden.nl>
Onderwerp: Memo datalekken bij online publicaties
Hoi 5.1.2e,
Excuses dat ik gister de memo niet heb kunnen toesturen. Teveel calamiteiten op een dag. Hierbij de memo, waarbij ik uiteraard het laatste, geel gearceerde deel met je wil bespreken.
Inhoudelijk denk ik dat dit vooral door 5.1.2e opgepakt gaat worden, maar ik wilde toch vooral jou hierin meenemen.
Groeten,
5.1.2e

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1

From: "Brink, Harm" <5.1.2e @leeuwarden.nl>
Sent: 3/2/2026 1:13:17 PM +00:00
To: "5.1.2e" <5.1.2e @leeuwarden.nl>
Cc: "5.1.2e" <5.1.2e @leeuwarden.nl>, "5.1.2e" <5.1.2e @leeuwarden.nl>
Subject: RE: Werkwijze bij het testen van 'Meer luisteren, minder typen'

Beste 5.1.2e en 5.1.2e,

Dank voor jullie inzet om te komen tot deze werkmethodiek!
Ik ben akkoord!
Met vriendelijke groet,

Harm Brink | Directeur
Portefeuille Bedrijfsvoering,Dienstverlening en Digitalisering
M 5.1.2e @leeuwarden.nl
T 5.1.2e

Gemeente Leeuwarden
Oldehoofsterkerkhof 2
Postbus 21000, 8900 JA LEEUWARDEN
5.1.2e

GLOBAL GOALS GEMEENTE

Aanwezig: maandag t/m vrijdag

Van: 5.1.2e
Verzonden: dinsdag 24 februari 2026 09:58
Aan: Brink, Harm
CC: 5.1.2e ; 5.1.2e
Onderwerp: Werkwijze bij het testen van 'Meer luisteren, minder typen'
Hoi 5.1.2e
Naar aanleiding van ons gesprek afgelopen donderdag hebben 5.1.2e en ik een werkwijze voor het experiment 'Minder typen, meer luisteren' uitgewerkt. Zie onder deze mail de uitwerking.
Deze werkwijze is akkoord bevonden door 5.1.2e Met alles wat we de afgelopen dagen hebben besproken, denk ik dat hier een mooi compromis ligt die recht doet aan de zorgen van 5.1.2e en tegelijkertijd ook het experimenteren met deze tool mogelijk maakt.
Kan jij hier ook mee akkoord gaan?
Met vriendelijke groet,
5.1.2e

Voorstel werkwijze bij experiment 'Meer luisteren, minder typen'

Voorafgaand aan het gesprek

- Collega-consulent die niet betrokken is op het dossier belt de inwoner vooraf (3 dagen om voldoende bedenktijd) of hij/zij wil deelnemen aan een test waarbij het gesprek ook wordt getranscribeerd met behulp van 5.1.2i. De Collega-consulent die niet betrokken is op het dossier geeft hierbij duidelijk aan dat weigering geen gevolgen heeft voor hun gesprek en geen gevolgen heeft voor de inspanningen die de gemeente verricht om de inwoner aan het werk te krijgen. Er zijn dus geen nadelige gevolgen van weigeren.
- Bij dit gesprek wordt uitgelegd dat:
  - het gesprek gewoon doorloopt zoals altijd,
  - er een extra verslag wordt gemaakt via automatische transcriptie,
  - dit verslag aan het einde samen wordt doorgenomen.
  - Dit verslag niet opgenomen wordt in het dossier, maar verwijderd.

Tijdens het gesprek

- Betrokken consulent op dit dossier voert het gesprek met de inwoner.
- Betrokken consulent op dit dossier maakt notities op de gebruikelijke, handmatige manier.
- Collega-consulent die niet betrokken is op het dossier zit bij het gesprek, maar heeft geen actieve rol in het gesprek zelf.
- Collega-consulent die niet betrokken is op het dossier start en beheert de transcriptie in 5.1.2i.

Na afloop van het gesprek

- Collega-consulent die niet betrokken is op het dossier toont het automatisch gegenereerde verslag aan de inwoner.
- Samen wordt besproken:
    - of het verslag een realistische en volledige weergave is van het gesprek,
    - of er onnauwkeurigheden of omissies zijn.
    - Vragenlijst over hoe het gesprek is ervaren (enquêtevragen via 5.1.2e.
- Het gespreksverslag wordt niet opgeslagen of gebruikt in het dossier. Het handmatige opgestelde verslag (de gebruikelijke manier) zal worden opgeslagen
- Vergelijking tussen het gemaakte verslag door AI en door de consulent. Eventuele verschillen in de 2 verslagen worden genoteerd ter lering.
- Na de vergelijking wordt het gespreksverslag verwijderd.

Legenda toegepaste uitzonderingsgrondslagen

In dit document zijn gegevens definitief geanonimiseerd op grond van:

Wet	Artikel	Omschrijving	Pagina's
Wet open overheid	Art. 5.1 lid 2 sub e	De eerbiediging van de persoonlijke levenssfeer	1, 2
Wet open overheid	Art. 5.1 lid 2 sub i	Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen	1

Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 14058

Gemeente Leeuwarden

MEMO

Aan:	Gemeentesecretaris Eelke de Jong
Van:	Functionaris Gegevensbescherming
Datum:	27 november 2024
Onderwerp:	Vervolg op datalek in raads- en informatiesystemen door niet anonimiseren metadata
Registratienummer:	2024-192096

Inleiding

24 september 2024 heb ik via een eerdere memo je aandacht gevraagd voor het aanwezige risico op misbruik door niet-geanonimiseerde metadata in gepubliceerde documenten. Via een brief aan IBabs, verzonden op 24 oktober 2024, hebben we gevraagd om de optie tot downloaden te reactiveren, waardoor het datalek zou worden stopgezet.

IBabs heeft op 11 november 2024 gereageerd op ons verzoek en daarbij aangegeven dat het stopzetten van de download-optie niet mogelijk is. Dit heeft ten eerste te maken met de SaaS-optie die wij hebben. Dat betekent dat er een applicatie wordt geleverd, die voor alle afnemers identiek is. Een aanpassing voor één afnemer betekent een aanpassing voor alle afnemers.

Verder geeft IBabs aan, dat de applicatie op mobile devices anders werkt dan via de website, waardoor het stopzetten van de download-optie niet zou werken op de mobile devices.

Via deze memo vraag ik je besluit op het voorstel om:

1. Vanaf uiterlijk 1 januari 2025 alle documenten die gepubliceerd worden, in Rex op te nemen met geanonimiseerde metadata.
2. Vanaf de start van een nieuw college (mei 2026) alle documenten vóór mei 2025 te verwijderen uit IBabs en te vervangen door een documenten-catalogus. Deze documenten zijn dan op te vragen via een Woo-verzoek en hoeven dus dan pas te worden geanonimiseerd.
3. Een project op te laten starten om het verwijderen van de documenten en het maken van een documentencatalogus.
4. Optie 1: Het huidige risico op misbruik van (persoons)gegevens vanuit IBabs te accepteren totdat de documenten opgenomen zijn in de documentencatalogus danwel geanonimiseerd zijn.
   Optie 2: De meest recente documenten (vanaf 1-1-2024) toch te anonimiseren, totdat deze worden opgenomen in de documentencatalogus.

Uiteenzetting voorstel

Naar aanleiding van de reactie van IBabs is er overleg geweest met de sectormanager van IM, om de vervolgstappen te bespreken.

1. Er wordt zo snel mogelijk intern gecommuniceerd dat alle stukken, die ter publicatie worden opgenomen in Rex (en daarna naar IBabs gaan), geanonimiseerde metadata moeten bevatten. Deze communicatie wordt door de privacy officers en de FG afgestemd met de collega's die veel met Rex en IBabs werken. Vervolgens wordt dit met de rest van de organisatie gedeeld via mail en Leo.

   Dit betekent dus ook, dat er mogelijk bespreekdocumenten vertraging oplopen, omdat de opstellers van de documenten alsnog hun stukken moeten anonimiseren, voordat deze op route gaan.

2. Een IM-adviseur gaat in kaart brengen wat het project gaat worden om de huidige documenten in IBabs (en dus Rex) te anonimiseren.

   Daarbij is dus de verwachting, dat het aantal te anonimiseren documenten minimaal tot nihil is. De verplichting tot persoonsgegevensvrije metadata gaat in per 1 januari 2025 en documenten tot mei 2025 zullen worden opgenomen in een documentencatalogus.

3. De enige zorg die overblijft, is het risico op misbruik van (persoons)gegevens via de beschikbaarheid daarvan in de metadata. Dat risico is uiteraard al aanwezig sinds het in gebruik nemen van IBabs, medio 2018.

   Online criminaliteit neemt echter toe, dus het is een risico dat nu groter is, dan voorheen. De enige mogelijkheid om dat risico zo klein mogelijk te houden, is om de meest actuele stukken (vanaf 1 januari 2024 tot heden) alsnog en versneld te anonimiseren, totdat deze worden opgenomen in de datacatalogus.