Beleidsnotitie Gegevensbescherming

Vastgesteld door het college van B&W op 24 maart 2020

Gemeente Leeuwarden

Samenvatting

Sinds 2018 is de Algemene Verordening Gegevensbescherming van kracht, die van grote invloed is op de verwerking van persoonsgegevens binnen de Gemeente Leeuwarden. Daarnaast heeft de Gemeente te maken met sectorale wetgeving, die tegelijkertijd ook invulling en aanknopingspunten biedt op het gebied van persoonsgegevens.

Er zijn echter nog veel open normen te vinden in de privacywetgeving. Wanneer is er sprake van een 'hoog' risico? Wanneer 'twijfelt' de gemeente aan de identiteit of wanneer vindt de gemeente een verzoek 'kennelijk buitensporig'? Dit is slechts een greep uit de vragen die zich dagelijks voordoen. Met de beleidsnotitie gegevensbescherming wordt invulling gegeven aan deze termen door middel van juridisch onderbouwde kaders en criteria met als doel één gedragslijn te hanteren binnen de Gemeente Leeuwarden.

In de beleidsnotitie worden kaders en criteria gegeven die op onderdelen nadere uitwerking behoeven op domein- of afdelingsniveau, bijvoorbeeld in concrete werkinstructies. Ter verduidelijking: dit beleid is niet bedoeld om de burgers of medewerkers te informeren over de omgang met wier persoonsgegevens. Voor de burgers is die hier gepubliceerd. Tevens wordt er nog een privacyverklaring opgesteld speciaal voor de medewerkers, waarin wordt beschreven hoe er met hun persoonsgegevens wordt omgegaan.

Dit document bevat geen herhaling van de reeds bekende wetgeving, maar een invulling van de open normen en antwoorden op de vraag hoe de Gemeente om wenst te gaan met persoonsgegevens. De bevoegdheid hieromtrent beleid te schrijven ontleent de Gemeente aan art. 24 lid 2 AVG.

Veelgebruikte afkortingen:

Art.	Artikel
AVG	Algemene Verordening Gegevensbescherming
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
AP	Autoriteit Persoonsgegevens
PIA	Privacy Impact Assessment
BRP	Basisregistratie Personen
FG	Functionaris voor Gegevensbescherming
WBP	Wet Bescherming Persoonsgegevens
BSN	Burgerservicenummer
MvT	Memorie van Toelichting
EDPR	European Data Protection Board (Voorheen Working Party 29, afgekort WP29) een orgaan bestaande uit alle voorzitters van de privacytoezichthouders van de EU welke belast is met het uitbrengen van richtlijnen om een uniforme toepassing van de AVG principes in alle lidstaten te bevorderen.
Wmo	Wet Maatschappelijke Ondersteuning 2015
Wgs	Wet Gemeentelijke Schuldhulpverlening

Inhoud

In deze beleidsnotitie komen diverse onderwerpen aan de orde die te maken hebben met gegevensbescherming.

Privacy Impact Assessment

Een Privacy Impact Assessment, kortweg PIA (ook wel DPIA of Gegevensbeschermingseffectbeoordeling genoemd) is een instrument om vooraf na te denken over de privacy risico's die een bepaalde gegevensverwerking met zich meebrengt.

De AVG zegt over de noodzaak van de uitvoering van een PIA het volgende: *"Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden."*[1]

De AVG schetst in ieder geval drie situaties waarin een PIA verplicht is[2]:

- *een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;*
- *grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of*
- *stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten*".

Er is lijst met criteria gepubliceerd door het huidige European Data Protection Board (Hierna: EDPR)[3]. Wanneer aan meerdere criteria wordt voldaan, des te groter de kans is dat de verwerking een groot risico inhoudt. Uitgangspunt is dat in geval er twee of meer criteria aanwezig zijn, een PIA dient te worden uitgevoerd omdat dan de kans op een hoog risico groot is.

Criteria

Criteria voor de inschatting van een 'waarschijnlijk hoog risico':

1. Evaluatie of scoretoekenning met inbegrip van profielbepaling en voorspelling, met name van *"kenmerken betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene"*[4]
2. Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg: verwerking die gericht is op het nemen van beslissingen met betrekking tot betrokkenen "*waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden*" of die "*de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen*".[5]
3. Stelselmatige monitoring: verwerking die wordt gebruikt voor het observeren, monitoren of controleren van betrokkenen, inclusief via netwerken verzamelde gegevens of "*stelselmatige [...] monitoring van openbaar toegankelijke ruimten*. [6]

[1] Art. 35 lid 1 AVG.
[2] Art. 35 lid 3 AVG.
[3] Voorheen de WP29, een orgaan bestaande uit alle voorzitters van de privacytoezichthouders van de EU welke belast is met het uitbrengen van richtlijnen om een uniforme toepassing van de AVG principes in alle lidstaten te bevorderen.
[4] Overweging 71 en 91 AVG.
[5] Art. 35 lid 3 onder A AVG.
[6] Art. 35 lid 3 onder C AVG.

4. Gevoelige gegevens of gegevens van zeer persoonlijke aard: dit omvat speciale categorieën persoonsgegevens zoals omschreven in artikel 9 AVG (bijvoorbeeld informatie over iemands gezondheid), evenals persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten zoals omschreven in artikel 10 AVG.
5. Op grote schaal verwerkte gegevens: in de AVG wordt niet gedefinieerd wat grootschalig is, al worden in overweging 91 enkele richtsnoeren gegeven. De EDPR raadt aan om met name de volgende factoren in aanmerking te nemen bij het bepalen of een verwerking op grote schaal wordt uitgevoerd[7]:
    a. het aantal betrokkenen, hetzij als een specifiek aantal hetzij als een deel van de relevante populatie;
    b. het volume van gegevens en/of het bereik van verschillende gegevensitems die worden verwerkt;
    c. de duur, of het permanente karakter, van de gegevensverwerkingsactiviteit;
    d. de geografische omvang van de verwerkingsactiviteit.
6. Matching of samenvoeging van datasets, bijvoorbeeld datasets die voortkomen uit twee of meer gegevensverwerkingen die voor verschillende doeleinden zijn uitgevoerd en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd op een wijze die de redelijke verwachtingen van de betrokkene zouden overschrijden.
7. Gegevens met betrekking tot kwetsbare betrokkenen[8]: de verwerking van dit soort gegevens is een criterium vanwege de toegenomen machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke, wat betekent dat de natuurlijke personen mogelijk niet in staat zijn om gemakkelijk te kunnen instemmen met of bezwaar te kunnen maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen. Cliënten in het Sociaal Domein worden standaard aangemerkt als een kwetsbare groep. Ook burgers die in aanraking komen met het Veiligheidsdomein worden aangemerkt als kwetsbare groep.
8. Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen, zoals het combineren van het gebruik van vingerafdrukken en gezichtsherkenning voor een betere fysieke toegangscontrole enz. Het gebruik van dergelijke technologie kan nieuwe vormen van gegevensverzameling en -gebruik inhouden, mogelijk met een hoog risico voor de rechten en vrijheden van natuurlijke personen.
9. Wanneer als gevolg van de verwerking zelf *"betrokkenen [...] een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst".* [9] Dit omvat verwerkingen die erop gericht zijn de toegang van betrokkenen tot een dienst of de mogelijkheid van betrokkenen om een overeenkomst aan te gaan toe te staan, te wijzigen of te weigeren.

Lijst verplichte PIA's

De Autoriteit Persoonsgegevens (AP) heeft van zijn wettelijke bevoegdheid[10] gebruik gemaakt om een lijst op te stellen van het soort verwerkingen waarvoor een PIA verplicht is. Het gaat om de volgende grootschalige en/of stelselmatige verwerkingen[11]:

1. Heimelijk onderzoek
2. Zwarte lijsten
3. Fraudebestrijding
4. Creditscores
5. Financiële situatie
6. Genetische persoonsgegevens
7. Gezondheidsgegevens
8. Samenwerkingsverbanden
9. (Flexibel) cameratoezicht
10. Controle werknemers
11. Locatiegegevens

[7] Zie de WP29-richtlijnen voor functionarissen voor gegevensbescherming 16/EN WP 243.
[8] Overweging 75 AVG.
[9] Overweging 91 en art. 22 AVG.
[10] Art. 35 lid 4 AVG.
[11] Zie hier een uitgebreidere toelichting op deze lijst door de AP

12. Communicatiegegevens
13. Internet of Things
14. Profilering
15. Monitoring en beïnvloeding van gedrag

Daarnaast heeft de AP ook een mogelijkheid een lijst samen te stellen waarin situaties worden geschetst waarbij géén PIA vereist is. Van die mogelijkheid heeft de toezichthouder nog geen gebruik gemaakt.[12]

Grootschalige en/of stelselmatige verwerkingen

Volgens de richtlijn van de EDPR kan "stelselmatig" een of meer van de volgende betekenissen hebben[13]:

- plaatsvindend volgens een systeem;
- vooraf geregeld, georganiseerd of methodisch;
- plaatsvindend in het kader van een algemeen plan voor gegevensverzameling;
- uitgevoerd als onderdeel van een strategie.

Voor wat betreft “grootschaligheid” raadt de EDPR aan om met name de volgende factoren in aanmerking te nemen bij het bepalen of een verwerking op grote schaal wordt uitgevoerd[14]:

- het aantal betrokkenen, hetzij als een specifiek aantal hetzij als een deel van de relevante populatie;
- het volume van gegevens en/of het bereik van verschillende gegevensitems die worden verwerkt;
- de duur, of het permanente karakter, van de gegevensverwerkingsactiviteit
- de geografische omvang van de verwerkingsactiviteit

Prioritering

Uit bovenstaande criteria zou geconcludeerd kunnen worden dat bijna elke verwerking binnen de gemeente een PIA behoeft; het betreffen immers veelal bijzondere persoonsgegevens, op grote schaal en ook nog eens van kwetsbare betrokkenen. Echter er hoeft geen PIA te worden uitgevoerd als een verwerking gebaseerd is op de uitvoering van een publieke taak of een wettelijke verplichting; een rechtsgrond heeft in het Unierecht of het recht van een lidstaat; de specifieke verwerking door de wet wordt geregeld en er al een PIA is uitgevoerd in het kader van de vaststelling van die rechtsgrond.[15]

Tegelijkertijd met de inwerkingtreding van de AVG is de sectorale wetgeving aangepast[16]. Daarbij is rekening gehouden met de risico’s voor betrokkenen. Sinds 1 september 2013 is het uitvoeren van een PIA bij ontwikkeling van nieuwe wetgeving en systemen, die zien op de verwerking van persoonsgegevens, verplicht voor de rijksoverheid.[17] Dit beperkt de risico’s die de wettelijk geregelde verwerkingen met zich meebrengen aanzienlijk.

PIA’s die zien op verwerkingen, uitwisselingen en samenwerkingen die niet expliciet in de wet zijn beschreven, zullen prioritair worden uitgevoerd waarbij aangesloten wordt bij de door de AP gepubliceerde lijst met verplichte PIA’s.

[12] Art. 35 lid 5 AVG.
[13] WP29 richtlijn 16/EN WP 243, blz. 8.
[14] WP29 richtlijn 16/EN WP 243, blz. 7.
[15] Zie art. 35 lid 10 AVG en de WP29 richtlijn 17/NL WP 248, p. 15.
[16] Zie de Aanpassingswet Algemene Verordening Gegevensbescherming.
[17] *Kamerstukken II* 2017-18, 34 851, 3, p. 57.

Datalek

Beveiligingsincident of datalek?

Een datalek is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.[18] Onrechtmatig houdt in dat er geen grondslag aanwezig is als bedoeld in art. 6 AVG, het wettelijk niet is toegestaan of er geen gegronde reden aanwezig is. Ongeoorloofd is de inzage door of verstrekking aan iemand, die daartoe niet gemachtigd of geautoriseerd is.

Een beveiligingsincident is een tekortkoming in de beveiliging (zoals verouderde software of een onbeveiligd verzonden mail). Niet ieder beveiligingsincident leidt echter tot een daadwerkelijk lek van data, het verloren gaan van data of een onrechtmatige verwerking.
Een beveiligingsincident zonder lek van data blijft een beveiligingsincident. Wanneer er in geval van een beveiligingsincident ook data verloren zijn gegaan, gelekt of anderszins onrechtmatig zijn verwerkt, is er sprake van een datalek.

Datalek melden bij de Autoriteit Persoonsgegevens

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de AP, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.[19]

Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen wier gegevens het voorwerp van de inbreuk zijn. Voorbeelden van dergelijke schade zijn discriminatie, identiteitsdiefstal of -fraude, financieel verlies en reputatieschade. Wanneer de inbreuk betrekking heeft op persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, of op persoonsgegevens die genetische gegevens of gegevens met betrekking tot de gezondheid of het seksleven, of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen omvatten, moet dergelijke schade als waarschijnlijk worden beschouwd.[20] Indien bovengenoemd risico aanwezig is, dient het datalek in beginsel te worden gemeld bij de AP.

De AP heeft advies uitgebracht hoe dit risico te beoordelen.[21] Als de persoonsgegevens verzonden zijn naar een verkeerde, maar betrouwbare ontvanger, betekent dit mogelijk dat het datalek niet langer een risico oplevert. ‘Betrouwbaar’ houdt volgens de AP in dat met redelijke zekerheid kan worden gezegd dat de onjuiste ontvanger geen kwaad in de zin heeft. Bijvoorbeeld dat de ontvanger niets doet met de per ongeluk ontvangen gegevens en zich houdt aan de eventuele instructies, zoals het vernietigen of terugsturen. De AP geeft op zijn website aan dat de volgende ontvangers als betrouwbaar kunnen worden aangemerkt:

- Partijen met wie wij een zakelijke relatie hebben, zoals een vaste leverancier
- Partijen die een wettelijk beroepsgeheim hebben, zoals een huisarts of zorgverlener, bewindvoerder, schuldhulpverleners of deurwaarders.

Bij de beoordeling van een risico vanwege een datalek wordt het advies van de AP gevolg.

De Functionaris Gegevensbescherming (FG) beslist op grond van bovengenoemde criteria of een beveiligingsincident is aan te merken als een datalek en of deze vervolgens gemeld dient te worden

[18] Art. 4 onder 12 AVG.
[19] Art. 33 lid 1 AVG.
[20] WP29 richtlijn 18/NL WP250, blz. 26.
[21] Zie website Autoriteit Persoonsgegevens (hier).

aan de AP. Vermoedelijke inbreuken worden onverwijld gemeld aan de FG. Daarnaast worden inbreuken die niet aan de AP en betrokkene worden gemeld, wel geregistreerd.[22]

Datalek melden bij betrokkene

Niet alle datalekken die gemeld zijn bij de AP moeten tevens worden gemeld aan de betrokkene(n); alleen als de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkene(n) moet het datalek aan de betrokkene worden gemeld.[23]

Een datalek hoeft niet aan betrokkene te worden gemeld als [24]:

- Er onverwijld doch uiterlijk binnen 24 uur passende technische en organisatorische maatregelen zijn genomen die de risico's beperken;
- Er onverwijld doch uiterlijk binnen 24 uur maatregelen zijn getroffen om het hoge risico voor de rechten en vrijheden van betrokkenen te minimaliseren;
- De mededeling doen een onevenredige inspanning zou vergen. In plaats daarvan wordt volstaan met een openbare mededeling of soortgelijke maatregel om betrokkenen te informeren.

Verzoeken van betrokkenen

Burgers kunnen verzoeken om inzage, verwijdering, correctie, beperking en bezwaar maken op de verwerking van de eigen persoonsgegevens.[25] Er dient derhalve onderscheid te worden gemaakt tussen een verzoek en een algemene vraag over persoonsgegevens. Voor laatste categorie is geen identificatie vereist is. ("Wat vermeldt de Gemeente in een dossier vs. wat staat er in mijn dossier"). Dergelijke verzoeken worden in beginsel gehonoreerd.

Wanneer wordt voldaan aan een verzoek worden namen van derden (zoals van melders of klagers) geanonimiseerd of niet verstrekt teneinde diens rechten en vrijheden te beschermen. Bovendien dient voor het goed functioneren van bepaalde meldingssystemen vertrouwelijkheid te worden gegarandeerd en moet dat belang zwaarder wegen dan het belang van kennisname van de complete melding inclusief naam van de melder c.q. klager.[26]

De FG besluit over verzoeken, na consultatie van de teamleider onder wiens verantwoordelijkheid de persoonsgegevens worden verwerkt.

Weigering te voldoen aan verzoek

Een verzoek wordt geweigerd indien:

1. Vanwege het belang van de nationale veiligheid, de openbare veiligheid, de voorkoming, opsporing en vervolging van strafbare feiten en ter bescherming van betrokkene of rechten en vrijheden van anderen of andere in art. 23 AVG genoemde beperkingen.[27]
   Bijvoorbeeld een verzoek om inzage in het dossier van een kind kan worden geweigerd, wanneer er een redelijk vermoeden bestaat dat deze informatie misbruikt kan worden bij een scheiding. Ook kan een inzageverzoek worden geweigerd als er een fraudeonderzoek loopt en het verzoek betrekking heeft op de gegevens waar fraudeonderzoek betrekking op heeft.
2. De verzoeker vraagt om een kopie van de documenten.
   In de AVG is geen bepaling opgenomen waarin staat dat de betrokkene recht heeft op een kopie van de bescheiden waarin de persoonsgegevens zijn verwerkt. Wel bestaat een recht op een volledig overzicht, in begrijpelijke vorm, van alle persoonsgegevens. Afhankelijk

[22] Art. 33 lid 5 AVG.
[23] Art. 34 lid 1 AVG.
[24] Art. 34 lid 3 AVG.
[25] Zie voor alle rechten van betrokkenen de art. 12 t/m 21 AVG.
[26] Hiervoor wordt aangesloten bij ECLI:RBUTR:2010:BO5227, r.o 4.8.
[27] Art. 23 lid 1 AVG, zie daar meer weigeringsgronden.

van de omstandigheden van het geval, kan worden volstaan met een andere vorm van verstrekking. Sommige gegevens lenen zich niet goed voor opname in een dergelijk overzicht. In dat geval heeft betrokkene in beginsel het recht op een (eventueel deels zwartgemaakte) kopie van de documenten.[28]

3. Het verzoek betrekking heeft op een lopende bezwaar- of beroepsprocedure.
   Omwille van de eerlijkheid van het proces kan een verzoek in een lopende bezwaar- of beroepsprocedure worden geweigerd.[29] *Omdat betrokkene in de procedure op enig moment op andere gronden al in bezit wordt gesteld van enkele stukken, kan het delen van bijvoorbeeld verweerschriften, motivaties en andere communicatie omtrent de zaak, vooruitlopend op de procedures, worden geweigerd.*
4. Het verzoek kennelijk buitensporig is.[30]
   Meer dan twee verzoeken die betrekking hebben op dezelfde voorziening, zaak of dossier per kalenderjaar worden aangemerkt als buitensporig[31]*, omdat een enkel verzoek reeds een maximale behandelingstermijn kent van drie maanden en de meeste voorzieningen binnen de gemeente voor de duur van een jaar verstrekt worden, waardoor de kans dat er tussentijds iets wijzigt klein is.*
5. Het verzoek niet gespecifieerd is tot een enkele voorziening, zaak of dossier.
   De bijbehorende hoeveelheid gegevens zijn anders te omvangrijk waardoor het onevenredig veel inspanning kost om aan een algemeen verzoek te kunnen voldoen. Derhalve wordt altijd om specificering van de verzoeken gevraagd.[32]
6. Niet is voldaan aan de randvoorwaarden.
7. Er vermoedelijk sprake is van misbruik van recht
   Misbruik van recht doet zich voor indien een dergelijke bevoegdheid wordt aangewend voor een ander doel dan waarvoor zij is gegeven, waardoor het doel van het verzoek relevant kan zijn om te beoordelen of misbruik van recht plaatsvindt.[33] *Indien er twijfel bestaat zal om toelichting van het doel gevraagd worden. Voorbeelden van misbruik van recht zijn verzoeken die tot doel hebben een ontslag van een medewerker of een afwijzing van een voorziening aan te vechten.*

Kosten

Het verstrekken van de informatie geschiedt kosteloos, tenzij het verzoek kennelijk buitensporig is (met name vanwege het repetitieve karakter).[34] Op grond van politieke of bestuurlijke overwegingen kan desondanks overgegaan worden tot het verstrekken van of inzage geven in de gegevens. Dan wordt een redelijke vergoeding in rekening gebracht waarbij wordt aangesloten bij de Legesverordening hoofdstuk ‘algemene kopieën’.

Identificatie

De AVG stelt dat wanneer er twijfel is over de identiteit van burgers die een verzoek indienen, er om aanvullende informatie gevraagd kan worden om de identiteit van de betrokkene te bevestigen.[35]

Gelet op de gevoeligheid van de gegevens waarover de gemeente beschikt, zal er standaard om identificatie van de verzoeker gevraagd worden. Identificatie kan plaatsvinden op de volgende manieren:

---

[28] Rb Den Haag 10 oktober 2019, ECLI:NL:RBDHA:2019:13029, r.o. 4.5 en 4.6.
[29] Art. 23 lid 1 onder F en I AVG.
[30] Art. 12 lid 5 AVG.
[31] Art. 12 lid 3 AVG.
[32] Overweging 63 laatste zin AVG.
[33] Omdat er nog weinig tot geen jurisprudentie omtrent misbruik van bevoegdheid bestaat onder de AVG, zoekt de Gemeente vooralsnog aansluiting bij bestaande jurisprudentie over WOB-verzoeken, zoals RvS 6 november 2019, ECLI:NL:RVS:2019:3750, r.o 5.
[34] Art. 12 lid 5 AVG.
[35] Art. 12 lid 6 AVG.

- Elektronisch door middel van Digid, omdat dit een algemeen erkend middel is die de overheid gebruikt om gebruikers te identificeren.
- Lijfelijk door middel van het tonen van een geldig legitimatiebewijs.

Het meezenden van een kopie van het legitimatiebewijs bij een verzoek is geen identificatiemethode.

Iemand kan namens een ander een verzoek indienen. De meest eenvoudige manier is om via DigiD een verzoek in te dienen. In dat geval kan gemachtigde samen met volmachtgever het contactformulier invullen.
Indien het verzoek door de gemachtigde in persoon wordt gedaan (e-mail, balie of telefonisch), is er een schriftelijke machtiging vereist.[36] Bij twijfel kan er om identificatie van zowel gemachtigde als van volmachtgever worden gevraagd. In dit geval kan voor de identificatie van de volmachtgever worden wel worden volstaan met het verstrekken van een kopie van het identiteitsbewijs omdat tevens een schriftelijke machtiging met handtekening aanwezig moet zijn.

Uitzondering

Bij BRP-aangelegenheden kan bij uitzondering worden volstaan met identificatie door middel van het stellen van identificerende vragen aan betrokkene. Dit omdat de BRP geen gevoelige gegevens omvat en vanwege de snelle afhandeling van eenvoudige verzoeken.

Samenwerkingen

De gemeente werkt samen met diverse partijen en in verschillende hoedanigheden. Denk aan zorgaanbieders, leveranciers of regionale samenwerkingsverbanden etc. Alle relaties en partners van de gemeente worden geschaard onder de term ‘samenwerking’.

De AVG schrijft voor dat de gemeente alleen een beroep hoort te doen op verwerkers als die afdoende garanties kunnen geven over het bieden van passende technische en organisatorische maatregelen zodanig dat de verwerking aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.[37] Om te kunnen inschatten of hiervan sprake is, dient een potentiele verwerker desgevraagd het volgende aan de gemeente te overleggen of aan te tonen, alvorens wordt besloten met deze partij te gaan werken:

- De aanwezigheid van een FG, indien dit wettelijk vereist is.
- De aanwezigheid van protocollen over datalekken en de omgang met verzoeken van betrokkenen.
- De aanwezigheid van een up-to-date privacy statement.
- De aanwezigheid van een verwerkingsregister.
- Certificering ten behoeve van beveiligingsmaatregelen zoals ISO of NEN. Indien de organisatie daarover niet beschikt zal op andere wijze aantoonbaar moeten maken of het voldoende maatregelen heeft getroffen ter beveiliging. Dit is ter beoordeling van de Security Officer.

Een partij is een verwerker wanneer de verwerking van persoonsgegevens namens een verwerkingsverantwoordelijke wordt verricht en het verwerken van persoonsgegevens de primaire opdracht is (en niet iets wat daaruit voortvloeit)[38]. In dat geval wordt een verwerkersovereenkomst met de betreffende partij afgesloten.

De meeste vormen van samenwerking van de gemeente typeren zich door zelfstandige verantwoordelijkheid of gezamenlijke verantwoordelijkheid. Alleen in geval van gezamenlijke verantwoordelijkheid dienen er tussen partijen afspraken over de gegevensuitwisseling gemaakt te

[36] Art. 2:1 lid 2 Awb.
[37] Art. 28 lid 1 AVG.
[38] Art. 28 lid 1 AVG.

worden.[39] Hoewel de AVG, de AP en de EDPR hierover enkele criteria geven, zijn deze in de praktijk vooralsnog vaak onvoldoende specifiek om de partners waarmee de gemeente samenwerkt te categoriseren. Dit vanwege de complexiteit en aard van de samenwerkingen. In alle gevallen waarin wordt samengewerkt met een andere partij worden er afspraken gemaakt over de gegevensuitwisseling, behoudens wanneer deze samenwerking en bijbehorende gegevensuitwisseling is gebaseerd op een wettelijk verplichte gegevensuitwisseling.

Bij de samenwerking wordt vastgelegd welke gegevens vereist zijn en welke partij verantwoordelijk is voor welk proces of verwerking binnen de samenwerking. Indien een wettelijke of publieke taak wordt uitgevoerd door of in samenwerking met een andere partij, dient deze partij een minimale set van gegevens uit te wisselen dat noodzakelijk is voor de gemeente om zijn taak naar behoren te kunnen uitvoeren.

In geval de samenwerking uit gaat van een verantwoordelijkheid van beide partijen (zoals bij zorgaanbieders) kan de gemeente besluiten om, alvorens tot samenwerking over te gaan, te verifiëren of de betreffende partij voldoende garanties kan afgeven dat met het toepassen van passende technische en organisatorische maatregelen de verwerking van persoonsgegevens aan de vereisten van de AVG voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd. Dit kan met name wenselijk zijn indien de gegevensuitwisseling niet specifiek wettelijk geregeld is.

Monitoring, analyse & rapportering

Monitoring, analyse en rapportering hebben tot doel de maatschappelijke impact van het gemeentelijk beleid te toetsen opdat desgewenst bijgestuurd kan worden. Dit is niet gericht op gegevens van een individu en heeft bovendien geen directe gevolgen voor betrokkenen.

Intern

Het delen en combineren van data om de maatschappelijke impact van het gemeentelijk beleid te toetsen binnen de organisatie is toegestaan binnen de kaders van de AVG. De gemeente heeft de wettelijke bevoegdheid om beleid te ontwikkelen[40], en daaruit vloeit voort de plicht om de kwaliteit van dit beleid te bewaken en te bevorderen. Het combineren van deze data geschiedt vaak door het BSN als koppeling te gebruiken, omdat dit het enige gegeven is dat diverse voorzieningen aan een unieke burger koppelt en om dubbelingen in gelijke namen en geboortedata te voorkomen.

Teneinde de veiligheidsrisico's te beperken, worden maatregelen genomen, zoals versleuteling. Die maatregelen dienen een passend niveau van beveiliging en vertrouwelijkheid te waarborgen. Daarbij worden de risico's en de aard van de te beschermen persoonsgegevens afgezet tegen de stand van de techniek en de uitvoeringskosten.[41]

Hashen is het vervormen van de BSN zodat niet meer bekend is welk persoonsnummer het betreft. Het blijft wel een uniek nummer, maar deze is niet naar persoonsgegevens te herleiden, zolang de sleutel niet beschikbaar is. De sleutel mag dan ook alleen toegankelijk zijn voor een geautoriseerde medewerker. Alle BSN's van de verschillende bronnen worden met dezelfde sleutel gehashed, omdat anders niet kan worden gekoppeld.

Met de huidige stand van de techniek is het op voorhand versleutelen (hashen) van het BSN vooralsnog niet in alle gevallen mogelijk. Dit is gerechtvaardigd gelet op het doel en de, qua waarschijnlijkheid en ernst, uiteenlopende risico's voor de rechten en vrijheden van personen[42]. Uitgangspunt is dat de uitkomsten van de betreffende analyses worden geanonimiseerd. Zo kan bijvoorbeeld de leerplichtadministratie worden geraadpleegd om te analyseren of nieuw beleid op

[39] Art. 26 lid 1 AVG.
[40] Zie bijvoorbeeld art. 2.1 en 2.2 Wmo.
[41] Artikel 32 AVG.
[42] Artikel 32 lid 1 AVG.

het gebied van integrale jeugdhulp op een bepaalde school doel treft. De koppeling geschiedt op BSN niveau, de uitkomsten worden daarentegen volledig geanonimiseerd gebruikt om het beleid te evalueren.

Het kan echter voorkomen dat het bij uitzondering gewenst is dat de uitkomsten wel herleidbaar zijn naar de individuele burger. Hiervoor worden twee categorieën analyses onderscheiden:

- Op individueel niveau voor intern- of dossieronderzoek (ten behoeve van beleidsanalyse) zonder dat betrokkene naar aanleiding hiervan wordt benaderd en/of er geen directe rechtsgevolgen aanzijn verbonden, zoals het wijzigen van een beschikking. Hiervoor lopen de verzoeker (veelal beleidsmedewerker), de betrokken data-analist en de privacy officer gezamenlijk een checklist door, waar onder meer doelbinding, subsidiariteit en dataminimalisatie worden besproken en vastgelegd.
- Op individueel niveau waarbij het doel is om, naar aanleiding van de analyse, de burger wel te benaderen en/of rechtsgevolgen voor betrokkene er aan te verbinden. In dit geval dient een PIA te worden verricht en is akkoord van de betreffende sectormanager(s) vereist.

Extern

De gemeente maakt deel uit van diverse samenwerkingen met als doel om van elkaar te kunnen leren, zoals het project 'Samen Digitaal'. Het delen van data met deze partijen is mogelijk op voorwaarde dat dit anoniem geschiedt. Omdat op geanonimiseerde data de AVG niet meer van toepassing is[43], is er geen overeenkomst over de gegevensuitwisseling vereist.

Integraliteit/Maatwerk

De gemeente is verantwoordelijk voor een brede waaier aan taken, op de terreinen van onder andere jeugd, veiligheid, passend onderwijs, leerplicht, aanpak kindermishandeling en huiselijk geweld, publieke gezondheid, welzijn, zorg en begeleiding, schuldhulpverlening en werk en inkomen. Om de burger integraal van dienst te kunnen zijn, wordt de volgende onderbouwing gehanteerd.[44]

De Jeugdwet stelt in art. 2.1 onder f dat het gemeentelijk beleid gericht moet zijn op integrale hulp aan de jeugdige en zijn ouders, indien sprake is van multiproblematiek. Uit de Jeugdwet blijkt overigens dat het belangrijk is dat de eventuele individuele maatwerkvoorziening wordt afgestemd op andere voorzieningen op het gebied van zorg, onderwijs, maatschappelijke ondersteuning en werk en inkomen.
In art. 2.3.5 lid 5 Wet Maatschappelijke Ondersteuning 2015 (hierna: Wmo) staat dat de maatwerkvoorziening, zover daartoe aanleiding bestaat, is afgestemd op onder meer de omstandigheden en mogelijkheden van de cliënt, de jeugdhulp als bedoeld in de Jeugdwet die de cliënt ontvangt of kan ontvangen, betaalde werkzaamheden, ondersteuning in gevolge de Participatiewet en scholing die de cliënt volgt of kan volgen.
In de Participatiewet staat in art. 18 lid 1 dat de bijstand en de daaraan verbonden verplichtingen afgestemd moeten worden op de omstandigheden, mogelijkheden en middelen van de belanghebbende. Daarnaast dient er een beroep op voorliggende voorzieningen gedaan te worden alvorens er een recht op bijstand bestaat.
In de Verordening Jeugdhulp 2019 Gemeente Leeuwarden wordt in art. 2 en 8 de mogelijkheid gegeven de maatwerkvoorziening af te stemmen op onderwijs en andere voorzieningen.

In de Memorie van Toelichting (MvT) bij de Wijziging van onder meer de Wet educatie en beroepsonderwijs inzake regionale samenwerking voortijd schoolverlaten en jongeren in een kwetsbare positie wordt gesteld dat er voor vroegtijdige schoolverlaters (Leerplichtwet) een betere

[43] Overweging 26 AVG.
[44] Hoewel hier landelijk overigens diverse opvattingen over bestaan, stelt de Gemeente niet alleen de privacy van de burgers bovenop, maar tevens het recht van burgers op een goed samenhangend sociaal zekerheidsstelsel.

afstemming moet zijn met het Arbeidsdomein (via een tijdelijke uitkering naar werk begeleiden) en met het Zorgdomein.[45]

In de Wet Gemeentelijke Schuldhulpverlening (Wgs) staat in art. 2 dat de Gemeente 'integrale schuldhulpverlening' tot taak heeft. Integrale schuldhulpverlening is volgens de MvT een samenhangend hulpaanbod van preventie tot en met zorg gericht op zowel de financiële- als psychosociale en andere oorzaken van schulden. Het kan daarbij bijvoorbeeld gaan om relatieproblemen, de woonsituatie, de gezondheid, de verslaving en de gezinssituatie.[46]
Hoewel de Wgs, Leerplichtwet en de Participatiewet, anders dan de Jeugdwet en de Wmo, niet expliciet afstemming tussen de andere wettelijke taken verplicht, lijkt dit wel impliciet uit de wettelijke taak voort te vloeien.

Uit de MvT van de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) blijkt bovendien dat de wettelijke verplichting niet noodzakelijkerwijs hoeft te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken, maar bijvoorbeeld ook uit een ruimer geformuleerde zorgplicht of een wettelijke verplichting kan bestaan.[47] Bovendien is de publieke taak naar zijn aard dynamisch en veranderlijk door de tijd heen. De grenzen van de publieke taak zijn niet altijd op voorhand scherp te trekken.[48] Er is overigens een algemenere zorgplicht ten aanzien van de sociale zekerheid neergelegd in de Grondwet.[49] Er is daarmee een algemene impliciete wettelijke grondslag voor integrale dienstverlening binnen het Sociaal Domein.

In geval een expliciete verplichting ontbreekt, is de verantwoordelijkheid om de noodzaak van de verwerking van gegevens te beoordelen, om te voldoen aan de wettelijke verplichting, wel groter. Dan moet een verwerking van gegevens noodzakelijk zijn om te kunnen voldoen aan een wettelijke verplichting.[50] De ervaring leert namelijk dat er in de praktijk niet integraal kan worden gewerkt zonder binnen de kaders van de diverse wettelijke taken gegevens uit te wisselen.

Hoewel de mogelijkheid tot integraliteit in sommige gevallen slechts impliciet uit de betreffende wetgeving blijkt, heeft het Rijk zich hier wel expliciet over geuit. Sterker nog; de integrale dienstverlening is een voorwaarde voor de decentralisatie, zoals blijkt uit onder meer de Decentralisatiebrief.[51] De minister heeft de beleidsvisie 'Gegevensverwerking en Privacy in een gedecentraliseerd Sociaal Domein' op gesteld.[52] In de bijbehorende brief van de minister valt te lezen dat de visie voldoende ruimte biedt voor gemeenten om hun dienstverlening vorm te geven op een manier die past bij hun eigen specifieke omstandigheden.[53]

Gezien bovenstaande (soms impliciete) wettelijke bevoegdheid en de expliciete wens van het kabinet tot integrale dienstverlening, kan worden betoogd dat er een grondslag ligt in de uitvoering van de publiek taak van de Gemeente[54].

---

[45] *Kamerstukken II*, 2017-2018, 34 812, nr. 3, p. 7
[46] *Kamerstukken II*, 2009/10, 32 291, nr. 3, p.21.
[47] *Kamertukken II* 2017/18, 34851, nr. 3, p.35.
[48] *Kamertukken II* 2017/18, 34851, nr. 3, p.35.
[49] Art. 20 Grondwet.
[50] *Kamertukken II* 2017-18, 34851, nr. 3, p.35.
[51] Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 19 februari 2013, 2013-0000108917 (Decentralisatiebrief).
[52] *Zorgvuldig en bewust: Gegevensverwerking en Privacy in een gedecentraliseerd Sociaal Domein* (Beleidsvisie van de Minister van Binnenlandse Zaken en Koninkrijksrelaties), bijlage bij *Kamerstukken II*, 2013/14, 32761, 62.
[53] *Kamerstukken II*, 2013/14, 32761, 62, p.3.
[54] Anders dan de AP stelt in haar Rapport uit 2016 over toestemming in het Sociaal Domein, blz. 12, waarin wordt betoogd dat de opdracht tot integraliteit alleen gericht is op het opstellen van beleid. De Gemeente Leeuwarden is van mening dat het opstellen van een beleid gericht op integraliteit logischerwijs als gevolg heeft dat er integraal wordt gewerkt. Opmerking verdient allereerst het feit dat dit rapport dateert uit 2016. Daarnaast is dit rapport openbaar gemaakt vóór publicatie van de MvT van de UAVG waarin wordt gesproken over dat de wettelijke verplichting niet noodzakelijkerwijs hoeft te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken, maar bijvoorbeeld ook uit een ruimer geformuleerde zorgplicht of wettelijke verplichting kan bestaan. Dat bijvoorbeeld een maatwerkvoorziening ingevolge art. 2.3.5 lid 5 Wmo afgestemd

Noodzaak

Bovenstaande laat onverlet dat er alleen een noodzaak tot integraliteit bestaat indien hier een sterke aanleiding toe is. Daarvan is in ieder geval, doch niet uitsluitend, sprake in geval van multiproblematiek; acuut levensgevaar voor betrokkene dreigt; aanzienlijk risico voor een ander op levensgevaar; ernstig lichamelijk letsel; ernstige psychische, materiële, immateriële of financiële schade; ernstige verwaarlozing of maatschappelijke teloorgang of om ernstig in zijn ontwikkeling te worden geschaad, dan wel dat de algemene veiligheid van personen of goederen in gevaar is. Het is aan de ter zake deskundige (in casu consulenten of hulpverleners) om dergelijke signalen te herkennen.

De proportionaliteit, subsidiariteit en doelmatigheid van de betreffende uitwisseling laat zich per situatie toetsen aan de hand van de volgende vragen, op basis waarvan een afweging kan worden gemaakt:

- Wat is het belang van de betrokkene?
- Wat gebeurt er als ik die gegevens niet uitwissel, als ik zwijg?
- Wat gebeurt er als ik die gegevens wel uitwissel, als ik spreek?
- Staat mijn actie in verhouding tot mijn doel, is mijn actie in proportie?
- Is mijn actie echt nodig, is er een andere (minder ingrijpende actie) mogelijk om mijn doel te bereiken?
- Bereik ik met deze actie mijn beoogde doel?
- Weegt het belang van de burger om deze van adequate, integrale benadering c.q. hulp te voorzien in casu zwaarder dan de vergaande inmenging in persoonlijke levenssfeer van de betreffende burger?

Antwoorden op bovenstaande vragen en bijbehorende afwegingen dienen schriftelijk te worden gemotiveerd en worden gedocumenteerd in het dossier van betrokkene.

Het kan ook voorkomen dat signalen van multiproblematiek (nog) niet geconstateerd zijn door een professional, maar achteraf bekend worden. Dat kan bijvoorbeeld geconstateerd worden als er naar aanleiding van een analyse blijkt dat een burger of gezin van meerdere voorzieningen en hulpverleners gebruik maakt. De proportionaliteit, doelbinding en subsidiariteit zullen aan de hand van bovengenoemde vragen vervolgens nog moeten worden afgewogen, gemotiveerd en gerapporteerd.

Uitgangspunt is dat integraliteit in samenspraak gaat met betrokkene en deze actief op de hoogte wordt gesteld. Deze samenspraak moet niet worden verward met toestemming. Dit uitgangspunt kan alleen worden genegeerd indien er zwaarwegende redenen zijn, bijvoorbeeld in verband met de veiligheid van betrokkene en/of zijn omgeving. Ook deze afweging wordt gemotiveerd en gerapporteerd.

Profilering

Het nemen van geautomatiseerde besluiten zonder menselijke tussenkomst op basis van risicoprofilering is niet toegestaan, tenzij er een (expliciete) wettelijke basis voor bestaat.[55] Een voorbeeld van profilering is het automatisch genereren van een weigering van een aangevraagde lening omdat de aanvrager een ‘risicovolle’ postcode woonachtig is. Profilering met menselijke tussenkomst wordt alleen gebruikt indien daarmee een aantoonbaar belang is gediend. Dit is ter beslissing van de FG en betreffende sectormanager.

---

moet zijn op onder andere omstandigheden als ondersteuning uit Participatiewet en Jeugdwet, houdt logischerwijs het gevolg in dat er wetsoverstijgende persoonsgegevens worden verwerkt.

[55] Art. 22 AVG.

Journalistiek

De gemeente is zeer actief op Social Media, maar doet tevens veel aan marketing. Dit soort journalistieke activiteiten zijn toegestaan indien zij tot doel hebben om het publiek te informeren ongeacht het overdrachtsmedium. Deze activiteiten zijn niet voorbehouden aan mediaondernemingen en kunnen zelfs een winstoogmerk hebben.[56]

Het plaatsen van nieuwsberichten met foto's is geen publieke taak, maar dient het gerechtvaardigd belang van de gemeente[57] dat in toenemende mate van de overheid wordt verwacht die zorgt voor actieve nieuwsverspreiding met gebruik van Social Media.

De uitzondering dat de overheid zich niet op de grondslag van gerechtvaardigd belang mag baseren in het kader van de uitvoering van haar publieke taken gaat niet op. [58] De verspreiding van nieuwsberichten is immers niet te kwalificeren als een publieke taak van de overheid maar kan worden gezien als reguliere bedrijfsvoering zoals bij ieder ander bedrijf. Door de aanwezigheid van deze grondslag is het vragen van toestemming op grond van de AVG niet vereist.

Wanneer beeldmateriaal op portretniveau wordt vervaardigd, vraagt de gemeente waar mogelijk of betrokkene bezwaar heeft tegen het gebruik van dit beeldmateriaal voor journalistieke doeleinden. Indien betrokkene bezwaar heeft dan wordt dit gerespecteerd. Deze vraag moet niet verward worden met de toestemming als bedoeld in de AVG.

Burgerservicenummer (BSN)

Het BSN is geen bijzonder persoonsgegeven. De UAVG zegt over het BSN het volgende: "Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald."[59] Aan dat laatste is gehoor gegeven in de Wet Algemene Bepalingen Burgerservicenummer (WABB) in art. 10 op te nemen dat overheidsorganen, bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak, gebruik kunnen maken van het BSN.

De MvT op laatstgenoemde wet stelt over de noodzaak tot het gebruik van het BSN nog het volgende: "Persoonsnummers moeten alleen gebruikt worden wanneer dat nodig is. Als een overheidsorgaan een dienst kan leveren zonder dat het nodig is om gegevens van de persoon vast te leggen of te raadplegen, dan is het niet nodig om een persoonsnummer bij deze transactie te betrekken (…) Door deze situaties duidelijk te onderscheiden van de situaties waarbij de rechten en/of plichten van een persoon ten opzichte van de overheid in het geding zijn, wordt vermeden dat er situaties ontstaan waarbij de persoon om zijn nummer wordt gevraagd maar waarbij er geen (directe) aanleiding is om de relatie tussen nummer en persoon te verifiëren".[60] Daarmee kan er van worden uitgegaan dat bij de invoering van de WABB het huidige en hedendaagse beschermingsniveau van persoonsgegevens reeds als uitgangspunt is meegenomen.

Het kan dus voorkomen dat het gebruik van het BSN expliciet wordt voorgeschreven zoals bijvoorbeeld in de Wmo of Jeugdwet, maar in de WABB is tevens bepaald dat het in zijn algemeenheid voor de uitvoering van de publieke taak van de Gemeente kan worden gebruikt.

Uitgangspunt is dat de Gemeente Leeuwarden voor de uitvoering van haar taken gebruik zal maken van het BSN en wel om de volgende redenen:

- het in sommige gevallen expliciet wordt voorgeschreven;
- het BSN is het enige unieke gegeven dat diverse beschikkingen, voorzieningen, dossiers etc. aan een persoon kan koppelen. Hierdoor worden fouten of dubbelingen voorkomen;
- om te bepalen of het de juiste persoon betreft.

[56] HvJEU 16 december 2008, ECLI:EU:C:2008:727, r.o. 61 *(Satakunnan en Satamedia)*.
[57] Art. 6 lid 1 onder F AVG.
[58] Art. 6 lid 1 onder F laatste zin.
[59] Art. 46 UAVG.
[60] *Kamerstukken II* 2005,06, 30 312, 3, p. 10.

Richtlijn is hierbij dat het BSN alleen wordt gebruikt als identificatie van persoon vereist is of als het betrekking heeft op een zaak, dossier of vergunning dat toebehoort aan een burger. Zo is voor het maken van een afspraak, de aanvraag van een brochure, een terugbelverzoek, het melden van een loszittende stoeptegel, het stellen van een algemene vraag, (op dat moment in het proces) geen identificatie of vastlegging van een grote hoeveel gegevens vereist, anders dan de gegevens die nodig zijn om contact met betrokkene te kunnen leggen.

Toestemming

Voor een beter begrip van deze paragraaf dient onderscheid te worden gemaakt tussen toestemming als bedoeld in de AVG of toestemming anderzijds, bijvoorbeeld toestemming voor het aannemen van hulp en de doorbreking van de (medische) geheimhoudingsplicht van een hulpverlener. Toestemming, anders dan bedoeld in de AVG, ziet bijvoorbeeld op de vrijwillig- en vrijblijvendheid van zorg en hulp.[61] Een burger kan toestemming geven om (integraal) hulp te krijgen. De wet schrijft vaak voor wanneer deze toestemming vereist is, zoals bijvoorbeeld in art. 7.3.4 lid 1 Jeugdwet.

Toestemming is een van de zes grondslagen om gegevens te mogen verwerken op grond van de AVG.[62] De grondslag voor het grootste deel van de verwerkingen ligt in het voldoen aan een wettelijke plicht of de uitvoering van een publieke taak.[63] Daarmee is toestemming, als andere grondslag, niet meer vereist.

Het geven van toestemming zoals bedoeld in de AVG, vormt in beginsel geen grondslag voor de gemeente omdat toestemming verlenen vrijelijk dient te geschieden.[64] Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.[65] Wanneer er sprake is van een overheidsinstantie is het onwaarschijnlijk dat de toestemming vrijelijk is verleend, omdat betrokkene in veel situaties afhankelijk is van de gemeente.[66]

Veelal is toestemming niet nodig omdat het verwerken van persoonsgegeven zijn rondslag in andere regelgeving vindt. Er bestaan situaties waarin sectorale wetgeving wel specifiek om toestemming vraagt, voor gegevensuitwisseling met derden, waaraan vanzelfsprekend voldaan moet worden. Dit gaat veelal om situaties waarin derde partijen betrokken zijn, zoals toezichthouders, vertrouwenspersonen of ouders.[67]

[61] Grensgebied is hierbij de het spectrum van zorgmijders en Wet verplichte GGZ, dat blijft hierbij buiten beschouwing en kent een eigen regime.
[62] Art. 6 AVG.
[63] Art. 6 lid 1 onder C en E AVG.
[64] Art. 7 lid 4 AVG.
[65] Overweging 42, laatste zin AVG.
[66] Overweging 43 AVG.
[67] Zie bijvoorbeeld art. 7.3.11 Jeugdwet.