PBLQ

Handreiking AVG voor Wegbeheerders

Handreiking
Talking Traffic
15 oktober 2019

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

Binnen het partnership Talking Traffic werken wegbeheerders samen met een groot aantal publieke en private partijen om de kansen van intelligente verkeersregelinstallaties (iVRI's) ten volle te benutten. In de keten van wegbeheerders, iVRI leveranciers, cloud providers, service providers en weggebruikers worden gegevens uitgewisseld waarvan sommige zijn te herleiden tot persoonsgegevens. Om de privacy van betrokkenen te waarborgen is het belangrijk dat wegbeheerders zicht krijgen op hoe zij met persoonsgegevens om moeten gaan. Onder meer de Functionarissen Gegevensbescherming (FG'en) en de Chief Information Security Officers (CISO's) van sommige wegbeheerders kunnen een ruggesteun gebruiken bij het AVG-compliant krijgen en houden van hun organisaties. Wegbeheerders zijn gebaat bij een toegankelijk document over de AVG-vereisten die relevant voor hen zijn. Deze handreiking beoogt te voorzien in deze behoefte.

1.2 Verantwoordings- en documentatieplicht

Het is belangrijk dat de lezer zich realiseert dat de AVG voortborduurt op zijn voorganger, de Wet bescherming persoonsgegevens (Wbp). Een belangrijk verschil tussen de twee is de nieuw ingevoerde verantwoordingsplicht: een organisatie moet kunnen aantonen dat aan de eisen van de AVG voldaan wordt. De gedachte is dat gegevensbescherming aantoonbaar geborgd moet zijn in de organisatie (de verantwoordingsplicht). Dit resulteert erin dat door te documenteren als vanzelf meer weloverwogen keuzes gemaakt zullen worden en dat het voor toezichthouders makkelijker wordt om bij overtredingen op te treden. Het register van gegevensverwerkingen, het privacybeleid en het inrichten van de processen en het uitdragen van de bewustwording rondom het effectueren van de rechten van betrokkenen (inzage, correctie, verwijdering en opschorting van de verwerking) moeten allen gedocumenteerd moeten worden.

1.3 Leeswijzer

Deze handreiking behandelt een aantal onderwerpen uit de AVG die bij wegbeheerders bekend moeten zijn. Daarnaast bevat de handreiking *best practices,* gebaseerd op opinies en richtlijnen van de Europese toezichthouders, maar ook op basis van praktijkervaringen van de auteurs. Voorbeelden worden in de tekst altijd cursief weergegeven.

- Het register van gegevensverwerkingen;
- Het formuleren van beleid op het gebied van gegevensbescherming en informatiebeveiliging (het privacybeleid);
- Het inrichten van de processen en het uitdragen van de bewustwording rondom het effectueren van de rechten van betrokkenen (inzage, correctie, verwijdering en opschorting van de verwerking);
- Het inrichten van het vermogen op incidenten te acteren alsmede de meldplicht datalekken in te vullen;
- Een meetlat voor PIA's;
- Tips voor de verwerkingsovereenkomsten.

De gedachtegang achter bovenstaande opsomming is dat een wegbeheerder geacht wordt gepaste beveiligingsmaatregelen te nemen ten aanzien van de persoonsgegevens die aan haar toevertrouwd zijn. En dat betrokkenen in staat moeten zijn hun rechten uit te oefenen. Dit vraagt om beleid ten aanzien van de verwerking van persoonsgegevens. Want wanneer je niet goed op de hoogte bent van wat je aan persoonsgegevens in huis hebt, kun je geen concreet beleid maken en uitvoeren.

2. Het verwerkingenregister

2.1 Doel en uitleg

Het verwerkingenregister, zie bijlage A voor een voorbeeld van een register, moet de spil van het privacybeleid van een organisatie zijn. Want als je niet weet wat je “in huis” hebt, weet je ook niet of en hoe je het kunt beschermen. Het begrip “verwerking” is wel gedefinieerd in de AVG, maar niet in een verwoording die behulpzaam is bij de afbakening van wat een individuele verwerking precies is. Verwerkingsverantwoordelijken zijn vrij om te kiezen hoe ze die afbakening kiezen, sommige organisaties gaan daarbij fijnmaziger te werk dan andere. In de praktijk zijn dit soort afbakeningen makkelijker aan de eigen organisatie uit te leggen als ze aansluiten bij organisatieprocessen of deelprocessen daarvan.

Voorbeelden van afbakeningen die als logisch worden ervaren zijn:

- Primaire processen
    - Parkeerbeheer
    - Handhaving milieuzone (ANPR-camera’s)
    - Verkeerscentrale
    - Verkeersmanagementnetwerk
- Bedrijfsvoeringsprocessen
    - Personeelszaken
        - Werving en selectie
        - Salarisverwerking
        - Ontwikkeling en opleiding
        - Beoordeling
        - Ziekteverzuim en re-integratie
        - Beëindigen arbeidsrelatie
    - Communicatie
        - Website
    - Facilitaire zaken
        - Toegangsbeheer
        - Camerabewaking

2.2 Kernelementen

Op basis van artikel 30 van de AVG moeten de volgende kernelementen in het verwerkingenregister staan:

Element	Toelichting
Contactgegevens van de verwerkingsverantwoorde-lijke(n) en de functionaris gegevensbescherming	Artikel 30 laat in het midden of dit eenmalig of voor alle verwerkingen apart wordt vastgelegd. Er zijn organisaties die afwisselend verwerker en verwerkingsverantwoordelijke zijn. Voor hen is het nodig te registreren wanneer welke rol wordt vervuld.
Doeleinden van de verwerking	Hier moet vooral aan organisatiedoeleinden gedacht worden. Denk bijvoorbeeld aan “het verbeteren van de verkeersveiligheid” of “het onderhouden van de wegen”.
Categorieën van betrokkenen	Dit is bedoeld om een beeld te hebben van de kwetsbaarheid van de betrokkenen. Zo leveren “locatiegegevens over ambulante vervoerders” een ander beeld op dan “NAW-gegevens”. Het kan zo zijn dat voor wegbeheerders dit niet altijd te segmenteren valt.
Categorieën van gegevens	De AVG maakt onderscheid tussen gewone persoonsgegevens, bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens. Bij gewone persoonsgegevens gaat het om NAW-gegevens. Bij bijzondere persoonsgegevens gaat het om gegevens over bijvoorbeeld etnische afkomst of gezondheidsgegevens. Bij strafrechtelijke persoonsgegevens gaat het bijvoorbeeld om strafrechtelijke feiten waarvan een persoon wordt verdacht. Wegbeheerders zullen met name te maken hebben met ‘locatie- en verplaatsingsgegevens’.
Categorieën van ontvangers	Denk aan organisaties binnen het Partnership, zowel TLEX en het NDW, als partijen uit cluster 2 en 3.
Derde landen en waarborgen (Alleen van toepassing bij doorgifte naar landen buiten de EER)	Een eventuele doorlevering aan partijen buiten de Europese Economische Ruimte (EER) dient nadrukkelijk opgenomen te worden in het verwerkingenregister.
Bewaartermijnen	Het is belangrijk bewaartermijnen te definiëren. Deze moeten zo kort mogelijk zijn in het kader van dataminimalisatie. Als het niet mogelijk is een harde bewaartermijn te geven, kan volstaan worden met een beslisregel als “één jaar na einde langlopend verkeersonderzoek”
Genomen beveiligingsmaatregelen	Het gaat hier om aanvullende beveiligingsmaatregelen of andere afwijkingen van het algemene beveiligingsbeleid.

2.3 Aanvullende elementen

Het verwerkingenregister wordt gemakkelijker toepasbaar door het toevoegen van een aantal niet-verplichte gegevenselementen.

Element	Toelichting
Hoofdproces	Door het hoofdproces weer te geven, wordt het eenvoudiger ook de interne managementverantwoordelijkheid voor verwerkingen te identificeren en vast te leggen én het wordt gemakkelijker om de organisatiedoelen te identificeren.
Deelproces	Door ook deelprocessen weer te geven, wordt het eenvoudiger vast te stellen wat de verwerkingsgrondslag(en) is/zijn. Bij deelprocessen kan gedacht worden aan voorbeelden als genereren van data en de communicatie en data-stromen tussen afdelingen.
Grondslagen	Door grondslagen in het verwerkingenregister op te nemen, wordt aan de algemene documentatieplicht van de AVG voldaan. Hiermee worden de grondslagen bedoeld zoals genoemd in AVG artikel 6. Dit zijn: a) Toestemming b) Aangaan en/of uitvoeren overeenkomst met betrokkene c) Wettelijke plicht d) Vitaal belang betrokkene of een derde e) Publieke taak f) Gerechtvaardigd belang Voor wegbeheerders is grondslag e), uitvoering van een publieke taak, doorgaans van toepassing voor de primaire processen. Wegbeheerders kunnen zich vrijwel nooit beroepen op f).
Handmatige of geautomatiseerde verwerking	De beveiligingsaspecten van papieren verwerkingsprocessen kunnen afwijken van een digitale situatie. Het is nuttig zowel de beveiliging van de papieren als digitale processen in kaart te brengen.
Ondersteunende applicaties of online diensten	Denk bijvoorbeeld aan het gebruik van externe voorzieningen (TLEX, bijvoorbeeld), maar ook meer technische informatie over de gebruikte applicaties.
Contractnummers	Dit is om de relatie met de verplichtingenadministratie inzichtelijk te maken.
Verwerkersovereenkomst	Hier is een ja/nee over de aanwezigheid voldoende.
(D)PIA uitgevoerd	Hier is een ja/nee over de uitvoering, eventueel aangevuld met een uitvoeringsdatum, voldoende.
Herkomst van de persoonsgegevens	Dit is nodig om de transparantieverplichtingen van AVG artikel 12, 13 en 14 te kunnen vervullen.

Een voorbeeld van een verwerkingsregister is te vinden in Bijlage A.

3. Het algemene privacybeleid

Het privacybeleid is een spil in de verantwoordingsplichten van de AVG - de AVG stelt expliciet dat een organisatie niet alleen moet handelen naar de AVG, maar daar ook formeel beleid over moet hebben[1]. Met name wanneer het gaat om organisaties met grotere en/of riskantere gegevensverwerkingen is het hebben van privacybeleid verplicht. Art. 24 AVG beschrijft voor deze organisaties een aanvullende documentatieplicht. In dit hoofdstuk wordt dieper ingegaan op een aantal aspecten van het privacybeleid.

3.1 Functionaris gegevensbescherming en mandatering

Een van de eerste te beantwoorden vragen is wie verantwoordelijk is voor de uitwerking en verdere operationalisering van het privacybeleid. Het is verstandig dit te beleggen bij functionarissen met managementverantwoordelijkheden voor de aan de verwerkingen gerelateerde organisatieprocessen, omdat dergelijke “datahouders” vaak beter in staat zijn de meer inhoudelijke afwegingen te maken. Zo is het ook eenvoudiger om het beleid wendbaar te houden.

Voorbeelden hiervan zijn:

- Personeelsdossiers: manager verantwoordelijk voor het personeelsbeleid;
- Verkeersinformatie: directeur verantwoordelijk voor het wegbeheer;
- Toegangsbewaking van de kantoorlocaties: directeur bedrijfsvoering;
- Algemene ICT-middelen: directeur bedrijfsvoering.

Een andere goede praktijk is om in het beleid duidelijk te maken wat de rol van de functionaris gegevensbescherming is, dit is namelijk primair een adviserende. Ook moet voor de medewerkers duidelijk zijn hoe ze met de functionaris gegevensbescherming in contact kunnen komen.

3.2 Privacybeleid opstellen

Privacybeleid heeft als doel de organisatie effectieve aanknopingspunten te bieden voor het beantwoorden van de vragen die in de uitvoeringspraktijk rijzen. Onderwerpen die daarbij horen zijn:

- Eindigheid van gegevens en de daaruit voortvloeiende bewaartermijnen;
- Omgang met bedrijfsmiddelen;
- Interne regeling voor de omgang met datalekken;
- Positionering Functionaris gegevensbescherming.

De Autoriteit Persoonsgegevens (AP) heeft een zestal tips[2] voor het privacybeleid gepubliceerd.

- Beoordeel of de organisatie verplicht is om een privacybeleid in te richten. De uitkomst van deze beoordeling zal in het geval van structurele verwerking van persoonsgegevens vrijwel altijd “ja” zijn;

[1] Zie artikel 24 AVG
[2] https://autoriteitpersoonsgegevens.nl/nl/nieuws/zes-aanbevelingen-voor-een-privacybeleid

- Gebruik interne en/of externe expertise. Aanboren van externe kennis is natuurlijk niet verkeerd, maar men moet het zich uiteindelijk wel toe-eigenen en internaliseren: het uiteindelijke beleid moet door de eigen mensen begrepen en gedragen worden;
- Leg het beleid vast in één document. Splits dat ene document wel op in onderdelen die door verschillende functionarissen bijgehouden kunnen worden of gebruik bijlagen, bijvoorbeeld voor het beveiligings- en continuïteitsbeleid;
- Wees concreet;
- Maak het beleid bekend. Ga daarin verder dan alleen initiële communicatie in bijvoorbeeld het kennismakingsproces van nieuwe medewerkers in de organisatie;
- Wanneer het niet verplicht is, kan het toch verstandig zijn privacybeleid op te stellen. Dit kan ook samenwerkingspartners helpen inzicht te krijgen in de verwerkingen die plaats vinden binnen de keten van clusters.

Een nuttig element van privacybeleid is dat het de organisatie uitgangspunten biedt voor de uitvoering van werkprocessen. Enige overlap van die uitgangspunten met de AVG zal onontkoombaar zijn, maar het is toch nuttig om een aantal beginselen uit te schrijven in ´spelregels´. Veel organisaties hebben kernwaarden geformuleerd, die vaak ook toepasbaar zijn op de omgang met persoonsgegevens en privacy. Door spelregels aan te laten sluiten op deze kernwaarden worden ze passender voor de organisatie. Voorbeelden van uitgangspunten in bewoordingen die herkenbaar zijn voor de medewerkers op de werkvloer, zijn:

- Gegevens van de organisatie worden uitsluitend verwerkt met middelen van de organisatie (we gebruiken dus geen privé e-mailaccount, privé-computers et cetera voor het werken met locatiegegevens);
- We verwerken nooit gegevens zonder dat we daar een reden voor hebben, dus niet omdat het misschien “handig voor later” is;
- Gegevens hebben altijd een eindige levensduur in onze organisatie. Ooit worden ze vernietigd of gearchiveerd;
- Als je merkt dat er iets fout gaat met gegevens neem je je verantwoordelijkheid om dat te melden bij je leidinggevende of de afdeling ICT;
- Iedereen weet en begrijpt dat we gegevens vertrouwelijk moeten houden en begrijpt ook dat dit betekent dat er niet alleen instructies over de omgang met gegevens zijn, maar dat dit ook met zich meebrengt dat het gebruik van gegevens achteraf gecontroleerd kan worden;
- Afwijkingen van het privacybeleid worden alleen in overleg met desbetreffende manager toegestaan. Deze afwijkingen zullen gedocumenteerd worden en met de functionaris gegevensbescherming gedeeld worden;
- Vragen over gegevensbescherming stellen we aan de functionaris gegevensbescherming. Graag de contactgegevens van de functionaris gegevensbescherming vermelden.

3.3 Gegevenscategorieën en -classificatie

Privacybeleid werkt in de praktijk vaak beter als er met een aantal categorieën van persoonsgegevens wordt gewerkt, zodat deze ook herkenbaar zijn voor de medewerkers. Een voorbeeld van een dergelijke classificatie zou zijn:

- Verplaatsingsgegevens;
- Gezondheidsgegevens
- Personeelsgegevens;
- Bezoekersgegevens;
- Leveranciersgegevens (gegevens over contactpersonen bij leveranciers).

Daarnaast is het goed om een interne risicoclassificatie te hebben die ook operationeel hanteerbaar is en mandaat geeft aan de datahouders om gegevens in die risicoclassificatie te classificeren.

3.3.1 Voorbeeld van een interne risicoclassificatie

Ten aanzien van de gevoeligheid van de gegevensverwerking zijn de volgende drie soorten te onderscheiden: hoog, midden en laag. Voor zover niet is vastgesteld wat de gevoeligheidsclassificatie van persoonsgegevens is, wordt dit door de procesverantwoordelijke manager gedaan en schriftelijk vastgelegd. Criteria hiervoor zijn:

- In het geval van locatie- en verplaatsingsgegevens, gezondheidsgegevens, politieke voorkeuren, seksuele voorkeuren/activiteit, etniciteit, gegevens over religie en strafrechtelijke gegevens, dan geldt de classificatie hoog;
- Voor persoonsgegevens die niet uit een publieke bron betrokken kunnen worden geldt de classificatie midden;
- Voor overige persoonsgegevens geldt de classificatie laag;
- Als het grote volumes[3] betreft, dan geldt dat de classificatie een rang hoger is dan op basis van de aard van de gegevens gegeven zou worden vastgesteld.

3.4 Bewaartermijnen en verwerkingsspecifieke elementen

Bewaartermijnen zijn in de praktijk sterk verweven met de doelen van een verwerking en daarom is het vaak lastig om op dit punt een categorisch beleid op te stellen. Er is dan ook niets mis mee om dit per verwerking te doen, en dat samen te nemen met andere verwerkingsspecifieke elementen. Het is wel mogelijk om rekening te houden met een aantal uitgangspunten:

- Het is de bedoeling dat persoonsgegevens altijd voor een bepaald doel worden verwerkt. Het doel zal richting geven in hoe lang het nodig is deze gegevens te bewaren. Vaak wordt er onterecht gedacht dat het goed is om persoonsgegevens te bewaren voor het geval deze in de toekomst nog nuttig kunnen zijn. Dit is expliciet *niet* de bedoeling. Als er geen concreet doel (meer) is voor het bewaren van gegevens, moeten deze worden verwijderd.
- Daarnaast is het de bedoeling zo min mogelijk data te verzamelen als nodig is voor het gestelde doel.

[3] De verwerking van persoonsgegevens door wegbeheerder is vaak grootschalig. Dit kan er ook toe leiden dat de gegevens niet meer herleidbaar zijn tot personen.

3.5 Samenhang met inkoopbeleid

Omdat in veel organisaties de verwerkingen deels of geheel worden gedaan met middelen die bestaan uit diensten van externe partijen geeft het privacybeleid kader voor het inkoopbeleid. Voorbeelden van leveranciersrelaties waar het privacybeleid in mee moeten worden genomen, zijn:

- De verkeerscentrale wordt gedeeld met andere wegbeheerders in een gemeenschappelijke regeling;
- De (i)VRI's worden ondersteund en beheerd door de fabrikant;
- De ANPR-camera's voor de handhaving van de milieuzone worden beheerd door een dienstverlener;
- De werkplekken worden beheerd en ondersteund door een dienstverlener.

Bovenstaande roept vragen op als:

- Met welke dienstenleveranciers doen we zaken?
- Welke criteria passen we toe?

Hoofdregel zou moeten zijn dat externe inkoop niet tot een ander beschermingsniveau zou mogen leiden dan het geval zou zijn bij interne verwerking.

3.5.1 Voorbeeld uit een organisatie zonder centrale inkoopfunctie

Binnen een organisatie kan bijvoorbeeld gelden dat proceseigenaren een hoge mate van vrijheid hebben om zelfstandig ICT-middelen in te kopen. Aan dit principe doet privacybeleid geen afbreuk. Wel stellen wij de volgende randvoorwaarden aan deze zelfstandige inkoop:

- Daar waar mogelijk persoonsgegevens worden verwerkt door leveranciers worden de functionaris gegevensbescherming en de CISO geconsulteerd voor de informatiebeveiliging en continuïteitsmaatregelen die van de leverancier gevergd gaan worden. Uitgangspunt daarbij is dat externe verwerking niet tot een lager niveau van beveiliging mag leiden dan het geval zou zijn bij interne verwerking. Een dergelijke consultatie vindt plaats vóór het aangaan van verplichtingen;
- Onderdeel van de verplichtingen van de leverancier is het aangaan van een verwerkersovereenkomst die voldoet aan de AVG;
- Externe verwerkingen worden opgenomen in het verwerkingenregister, het is een verantwoordelijkheid van de proceseigenaar dat dit ook daadwerkelijk gebeurt;
- Een externe verwerking moet altijd gegarandeerd plaatsvinden binnen het grondgebied van de Europese Economische Ruimte (EER) of Zwitserland. Bij gegevens met een lage risicoclassificatie kan hiervan afgeweken worden, maar dit moet schriftelijk vastgelegd worden en overlegd worden met de functionaris gegevensbescherming.

3.6 Beveiligingsbeleid

In een privacybeleidsdocument is het vaak beter om ten aanzien van informatiebeveiliging de inhoud te beperken tot een mandateringsparagraaf. Het informatiebeveiligingsbeleid zelf wordt dan opgenomen in een bijlage. De ontwikkelingen op het gebied van ICT gaan vaak dusdanig snel, dat men regelmatig bijstellingen van het beveiligingsbeleid zal willen doorvoeren. In de mandateringsparagraaf ten aanzien van informatiebeveiliging is het vaak goed om bijvoorbeeld de CISO het mandaat te geven om beveiligingsconsequenties te verbinden aan de classificatiekeuzes van de “datahouder”.

3.7 Transparantie

Een goed en compleet privacybeleidsdocument kan helpen bij het invullen van de transparantieverplichtingen onder de AVG. Voor de betrokkene moet duidelijk zijn:

- Welke partij verwerkingsverantwoordelijk is, hoe hij of zij ermee in contact kan komen;
- Hoe hij of zij in contact kan komen met de functionaris gegevensbescherming;
- Wat de doelen en grondslagen van de verwerkingen zijn;
- Met welke partijen zijn of haar gegevens gedeeld worden;
- Wat de bewaartermijnen zijn;
- Wat zijn of haar rechten zijn, inclusief klachtrechten;
- Of de te verstrekken gegevens verplicht zijn en waarom;
- Of er sprake is van geautomatiseerde besluitvorming.

Dit is niet genoeg als de gegevens niet van de betrokkene afkomstig zijn, maar van een andere partij - bijvoorbeeld afkomstig van het NDW of een andere externe partij. Het is raadzaam om in het privacybeleid vast te stellen hoe met derden wordt omgegaan dient te worden.

3.8 Datalekken

Voor datalekken geldt dat het privacybeleid een goede plek is om te regelen wie waartoe bevoegd is als er een incident wordt geconstateerd. Een voorbeeld uit een middelgrote organisatie:

Ten aanzien van de besluitvorming om een incident te melden bij de Autoriteit Persoonsgegevens en/of de betrokkenen gelden de volgende uitgangspunten:

- *Tijd is essentieel, deze besluitvorming dient binnen 72 uur nadat een incident geconstateerd is (bijvoorbeeld door een medewerker), afgerond te zijn;*
- *De bestuursjurist, het hoofd wegbeheer en het hoofd ICT zijn gezamenlijk bevoegd om een besluit om een datalek bij de Autoriteit Persoonsgegevens te melden al dan niet te nemen - wanneer deze groep van functionarissen niet compleet is, worden de besluiten genomen door degenen die wel bereikbaar zijn. Voor dit besluit wordt de Functionaris Gegevensbescherming, indien bereikbaar, geconsulteerd en deze zal de melding doen waar mogelijk, maar is niet de functionaris die hier over besluit;*
- *Zij zijn ook bevoegd om tot 2.000 EUR uit te geven om eventueel forensisch onderzoek uit te laten voeren als zij dit noodzakelijk achten;*
- *Zij zullen van bovenstaande besluitvorming altijd het management team en de directie verwittigen.*

3.9 Rol ondernemingsraad

Bij het vaststellen van het privacybeleid moet niet over het hoofd gezien worden dat er sprake kan zijn van inspraakrechten van de medezeggenschapsraad en ondernemingsraad. Zeker ten aanzien van personeelsgegevens geldt dat de ondernemingsraad een instemmingsrecht heeft. Het is dan ook zaak om deze te betrekken bij de totstandkoming van het beleid.

4. Rechten van betrokkenen

In dit hoofdstuk wordt het effectueren van de rechten van betrokkenen behandeld. Deze zijn niet nieuw in de AVG en bestonden al in de Wbp. Wel is nieuw in de AVG dat een organisatie moet documenteren hoe zij dit denkt in te vullen. Achtereenvolgens behandelen we het inzagerecht, correctierecht, verwijderingsrecht en opschortingsrecht.

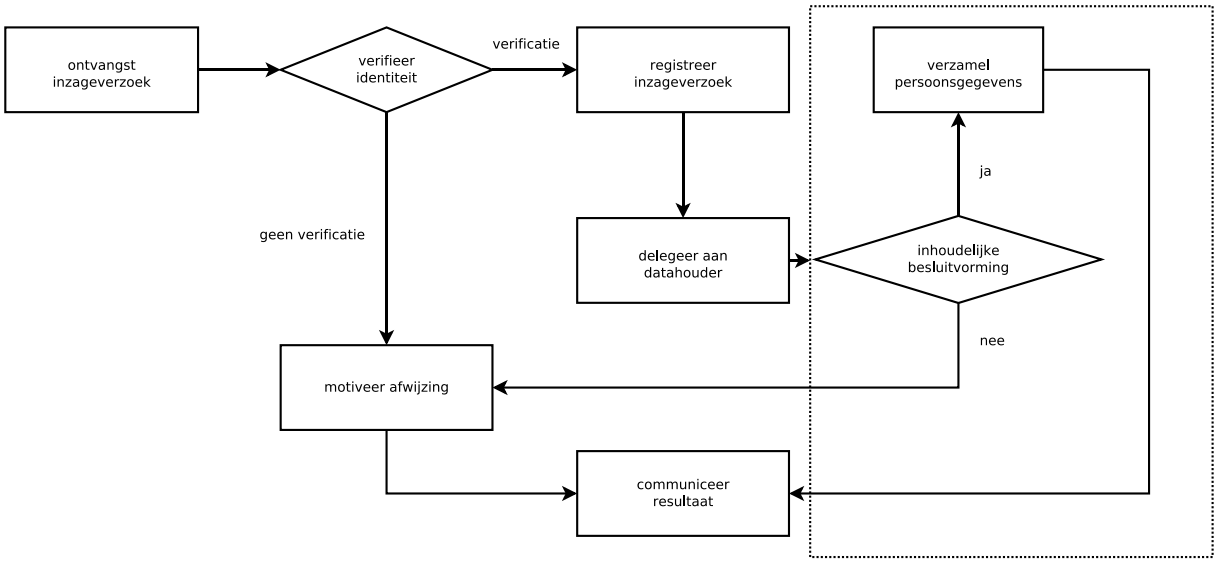
4.1 Inzagerecht

Het inzagerecht is een breedstrekkend recht van betrokkenen: eigenlijk zijn er maar twee situaties waarin een inzageverzoek geweigerd kan worden, namelijk:

- als het rechten van derden (dus andere burgers dan de verzoeker) te zeer raakt en als het redigeren van informatie over die derden niet mogelijk is;
- wanneer de persoonsgegevens dusdanig gepseudonimiseerd zijn dat het voor de verwerkingsverantwoordelijke aantoonbaar niet mogelijk is de betrokkene direct te identificeren.

De tweede uitzondering zal in de Talking Traffic context eerder regel dan uitzondering zijn, met name als het om V-LOG-data gaat. Denk bijvoorbeeld aan een verzoek van (of, in de praktijk vaker, namens, bij bijvoorbeeld subrogatie naar een autoschadeverzekeraar) een weggebruiker om de V-LOG- en SPaT-data in het kader van een ongevallenreconstructie.

Ter illustratie een voorbeeld van hoe het proces van inzageverstrekking beschreven kan worden:

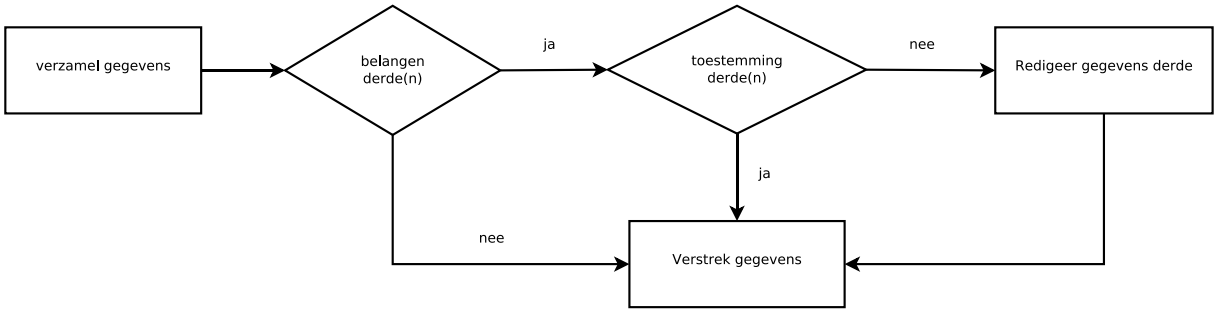


De eerste stap na de ontvangst van het inzageverzoek is de verificatie van de identiteit van de verzoeker. De AVG vermeldt niet hoe dit moet, maar in het verleden heeft de Autoriteit Persoonsgegevens aangegeven dat de zwaarte van de verificatie samenhangt met de aard van de gegevens. Het mag dus niet zo zijn dat een betrokkene veel meer persoonsgegevens moet opsturen

voor de verificatie in verhouding met de aard van de gegevens dat de betrokkene wil inzien. Ook is het aanbevelingswaardig om de verificatie in persoon plaats te kunnen laten vinden.

De volgende stap is de registratie van het inzageverzoek. Dit is geen AVG-vereiste, maar het is in de praktijk wel belangrijk omdat er niet langer dan vier weken gedaan mag worden over het afhandelen van inzageverzoeken (idem voor correctie, verwijdering en opschorting).

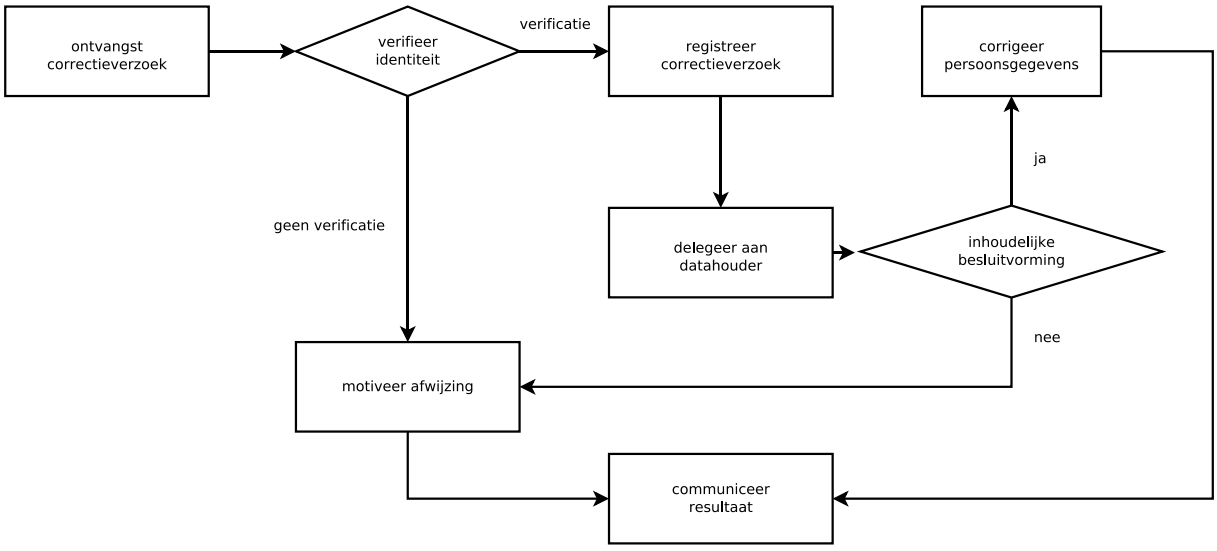
In het voorbeeld is ervoor gekozen om de uiteindelijke afweging over het honoreren van een inzageverzoek aan een “datahouder” over te laten. Er zijn uiteraard ook organisaties waarin een meer gecentraliseerde aanpak wordt gekozen. Los van die organisatorische keuze zal er een inhoudelijke toetsing plaats moeten vinden van het inzageverzoek, grafisch weer te geven als:



Een voorbeeld van een situatie waarin de rechten van derden geraakt kunnen worden door een inzageverzoek, betreft een gegeven, bijvoorbeeld een locatiegegeven, dat gaat over meerdere personen.

4.2 Correctierecht

Het correctierecht (officieel het recht op rectificatie, artikel 16 AVG) is het meest verstrekkende recht van een betrokkene: gegevens die objectief onjuist zijn moeten altijd gecorrigeerd kunnen worden. Ook hiervoor geldt een verificatie van de identiteit van de betrokkene. Omdat hier geen afweging van de belangen van derden speelt, is het proces relatief eenvoudiger en kan het er als volgt uitzien:



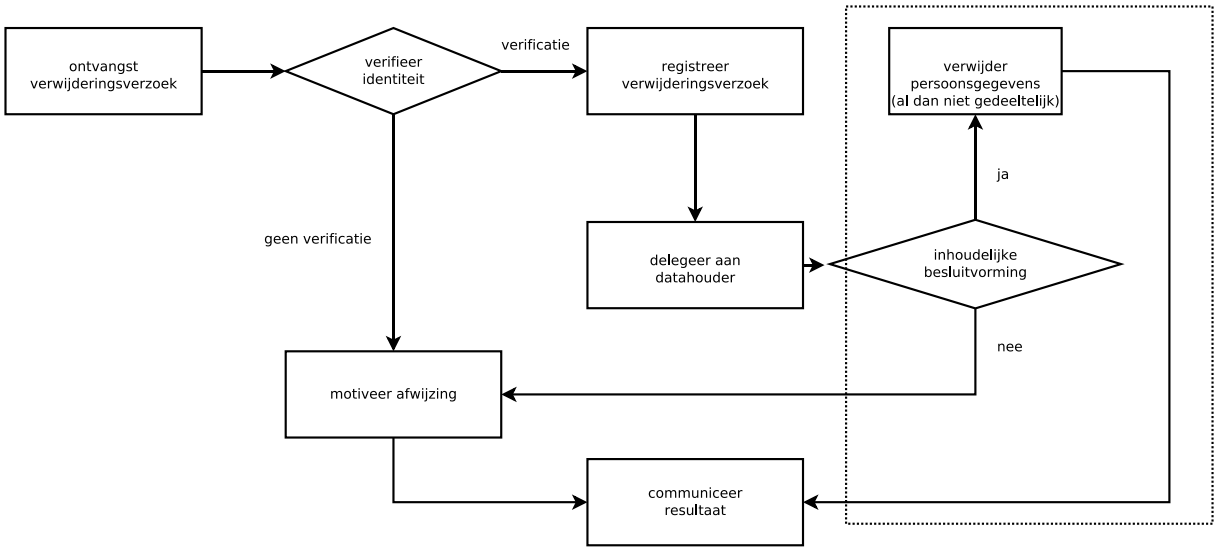
Onder correctie kan overigens ook verstaan worden dat een aantekening van de correctie wordt toegevoegd aan het dossier, met een uitleg waarom de eerdere gegevens onjuist waren.

Opgemerkt moet worden dat als de te corrigeren gegevens gedeeld zijn met een wegbeheerder, de wegbeheerder hierover geïnformeerd moet worden, voor zover dat redelijkerwijze mogelijk is.

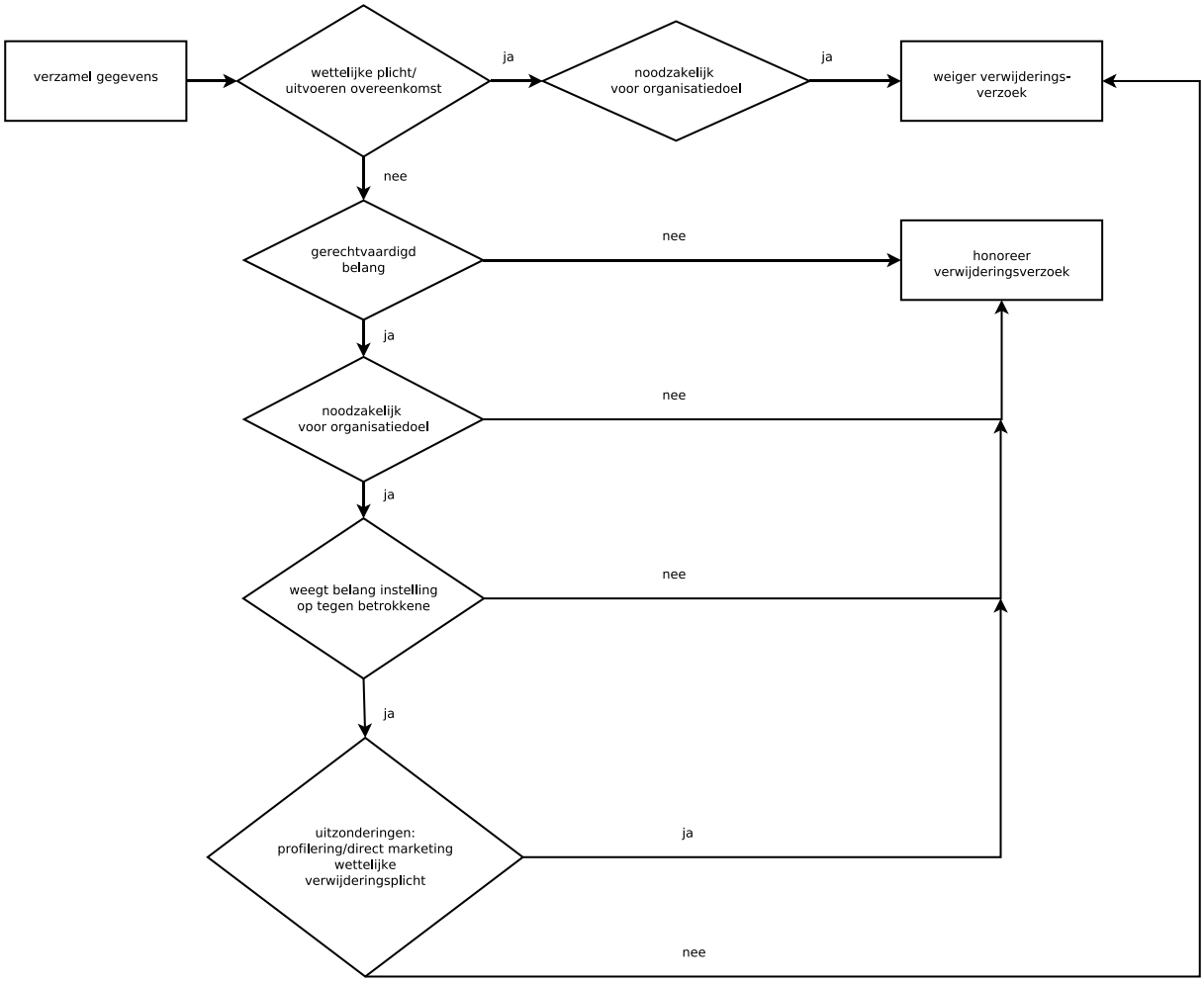
4.3 Verwijderingsrecht

Het recht op verwijdering (officieel het recht op vergetelheid, artikel 17 AVG) is het meest gecompliceerde recht van de betrokkene. Gecompliceerd omdat de beslisboom een ander karakter krijgt naar aanleiding van de grondslag van de verwerking. Bij de wegbeheerders zal het vrijwel altijd gaan om de uitvoering van de publieke taak.

Het hoofdproces ziet er nog steeds vergelijkbaar uit met een inzageverzoek:



Maar de inhoudelijke besluitvorming is anders:



Opgemerkt moet worden dat als de te verwijderen gegevens gedeeld zijn met een wegbeheerder, de wegbeheerder hierover geïnformeerd moet worden, voor zover dat redelijkerwijze mogelijk is.

4.4 Opschortingsrecht

Het opschortingsrecht komt in het spel als de betrokkene het oneens is met een weigering van een correctie- of een verwijderingsverzoek. In dat geval kan de betrokkene vragen de verwerking te beperken. Artikel 18 AVG beschrijft hoe deze beperkingen eruit zien. Voor de toegankelijkheid van deze handreiking is ervoor gekozen om deze relatief uitzonderlijke situatie niet verder uit te werken.

5. Datalekken en andere incidenten

5.1 Wat is een datalek?

De AVG omschrijft niet duidelijk wat een datalek is, maar er moet vooral gedacht worden aan:

- Een gebeurtenis of reeks van gebeurtenissen die de verwerking van persoonsgegevens betreft;
- Een gebeurtenis of reeks van gebeurtenissen waardoor de rechtmatigheid van de verwerking is aangetast. Denk daarbij aan:
  - Er ontstaat een disproportionele verwerking;
  - Er wordt gedeeld met (onbevoegde) derden zonder dat hier een grondslag voor bestaat;
  - Er ontstaat een verwerking zonder grondslag;
  - Er ontstaat een verwerking voor heel andere doeleinden dan waar de gegevens voor zijn verkregen;
  - Gegevens gaan verloren of worden ontoegankelijk.

Voor de duidelijkheid: de AVG spreekt over een datalek als een doorbreking van de beveiliging, maar door de beschrijving van de risico's waartegen die beveiligingsmaatregelen zouden moeten beschermen is de conclusie onontkoombaar dat niet zozeer de beveiliging het spilpunt van de analyse is, maar de onrechtmatigheid van de verwerking. De Europese toezichthouders onderkennen drie verschillende datalekken[4]:

- Inbreuk op de betrouwbaarheid: als er een ongeautoriseerde of ongewilde toegang tot of openbaarmaking van de persoonsgegevens heeft plaatsgevonden;
- Inbreuk op de integriteit: als er een ongeautoriseerde of ongewilde aanpassing van de persoonsgegevens heeft plaatsgevonden;
- Inbreuk op de beschikbaarheid: als de persoonsgegevens verloren zijn gegaan of tijdelijk niet beschikbaar zijn geweest.

Van alle dergelijke gebeurtenissen moet een registratie bijgehouden worden (artikel 33 lid 5 AVG). In sommige gevallen moet er een melding gedaan worden bij de toezichthouder, de Autoriteit Persoonsgegevens (artikel 33 lid 1 AVG), en in sommige gevallen ook aan de betrokkenen (artikel 34 AVG). Hierover meer in de volgende paragrafen.

5.2 Doel meldingsplicht datalekken

Het doel van de regels rond (meldingsplichtige) datalekken is:

- Zorgen dat de organisatie leert van fouten, ook als deze niet tot grote gevolgen hebben geleid;
- Toezichthouders een beeld geven van hoe vaak het fout gaat;
- Betrokkenen in staat stellen hun (mogelijke) schade te beperken.

[4] Zie 693/14/EN, WP 213, Opinion 03/2014 on Personal Data Breach Notification, adopted on 25 March 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

5.3 Wanneer is het melden van een datalek aan de Autoriteit Persoonsgegevens verplicht?

De korte versie is: “altijd, tenzij het voorzienbaar is dat het datalek geen risico voor de betrokkenen oplevert”. Het criterium van de AVG zelf is een waarschijnlijk risico voor de “rechten en vrijheden” van de betrokkenen. Voorbeelden van dit soort risico’s zijn te vinden in overweging 74 AVG:

- Ernstige lichamelijke, materiële of immateriële schade:
    - discriminatie, identiteitsdiefstal of -fraude;
    - financiële verliezen;
    - reputatieschade;
    - verlies van vertrouwelijkheid van door beroepsgeheim beschermde persoonsgegevens;
    - ongeoorloofde ongedaanmaking van pseudonimisering;
    - of enig ander aanzienlijk economisch of maatschappelijk nadeel;
- Wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen;
- Wanneer persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt;
- Bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen;
- Wanneer persoonlijke aspecten worden geëvalueerd, om met name:
    - beroepsprestaties;
    - economische situatie;
    - gezondheid;
    - persoonlijke voorkeuren of interesses;
    - betrouwbaarheid of gedrag;
    - locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- Wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt;
- Of wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

5.4 Wanneer is het melden van een datalek aan betrokkenen verplicht?

De meldingsplicht naar betrokkenen ontstaat als er sprake is van een voorzienbaar verhoogd risico voor de betrokkenen. Bovendien kunnen de betrokkenen redelijkerwijze nog niet van het verhoogd risico weten. Dit kan bijvoorbeeld gebeuren wanneer de anonimisering van de data uit cluster 1 niet correct of volledig blijkt te zijn, waardoor deze persoonsgegevens ongeoorloofd zijn uitgewisseld met cluster 2 en/of 3.

6. PIA

De AVG stelt een PIA (Privacy Impact Assessment), ook wel DPIA's (Data Protection Impact Assessment) of formeel gegevenseffectbeoordelingen (GEB) genoemd, verplicht bij gegevensverwerkingen waarbij vooraf al het vermoeden bestaat dat ze een verhoogd risico voor de betrokkenen met zich meebrengen. Dit risico kan zowel om de schaal als om de aard van de verwerkte gegevens gaan. Voorbeelden zijn de grootschalige verwerking van zogenaamde bijzondere categorieën van persoonsgegevens zoals gezondheidsgegevens en strafrechtelijke gegevens, maar ook grootschalige surveillance van de publieke ruimte zoals cameratoezicht of rekeningrijden.

Door deze verplichting worden er voor veel van de grotere overheids-ICT-projecten PIA's uitgevoerd. Ook alle wegbeheerders moeten in het kader van hun deelname aan Talking Traffic een PIA uitvoeren. Voor organisaties met relatief weinig ervaring in het uitvoeren van PIA's kan dit een uitdaging zijn.

6.1 AVG-vereisten voor een PIA

Een PIA moet aan de volgende voorwaarden voldoen: de (beoogde) gegevensverwerking en de (organisatie)doelen daarvan zijn duidelijk omschreven; de grondslagen voor de verwerking en de evenredigheid daarvan zijn getoetst; de risico´s voor de betrokkenen zijn geanalyseerd en er zijn maatregelen omschreven om geconstateerde risico's te beheersen.

De risicoanalyse richt zich op het risico dat bestaat zonder dat er enige maatregelen zijn genomen, ook wel het basisrisico of het inherent risico genoemd. Daarnaast is het aan te raden om ook het restrisico, dit is het risico dat overblijft na het nemen van maatregelen, te analyseren. Mocht dit als hoog worden gezien, dan kan er een consultatie met de toezichthouder, de AP (Autoriteit Persoonsgegevens), plaatsvinden. In het geval van een consultatie is een motivatie, waarin uiteengezet wordt waarom de gegevensverwerking ondanks een verhoogd restrisico voor de betrokkenen door moet gaan, een vereiste. De AP kan opdragen dat een gegevensverwerking niet mag worden uitgevoerd of zelfs stopgezet moet worden. Voor de risicoanalyse geldt dat er een voldoende objectieve, gangbare methodologie gebruikt moet worden.

6.2 Uitvoerend team

Om te voorkomen dat de PIA niet aan de eisen van de AVG voldoet, wordt een PIA het best uitgevoerd door een team van ten minste drie personen met de juiste mix van vaardigheden en kennis. Wanneer bijvoorbeeld alleen juristen worden betrokken, krijgt de rechtmatigheids- en evenredigheidstoetsing verreweg de meeste aandacht, terwijl deze toets eigenlijk pas goed uitvoerbaar is als de proces- en systeembeschrijvingen van voldoende kwaliteit zijn.

Daarnaast is aan te raden een PIA door interne, ervaren medewerkers uit te laten voeren die de organisatie en de processen goed kennen. Dit in tegenstelling tot de relatief onervaren medewerkers of externen die vaak worden ingezet. De beschrijving van de verwerking is bij uitstek een taak voor een systeem- of business analist, terwijl de toetsing van rechtmatigheid en proportionaliteit beter bij een juridisch medewerker kan worden belegd. Voor de risicoanalyse geldt dat kennis en ervaring op het gebied van ICT-risicobeheersing, inclusief informatiebeveiliging en -continuïteit, wenselijk is.

6.3 Grondslagenanalyse en evenredigheidstoets

Bij de grondslagenanalyse wordt per doel van de verwerking gekeken of deze aansluit bij een verwerkingsgrondslag (artikel 6 AVG) én of de beoogde verwerking evenredig is voor het doel. Dit is een relatief juridische activiteit waarbij de Europese toezichthouders nog betrekkelijk weinig houvast hebben geboden in de vorm van richtlijnen en opinies.

In situaties waarin de verwerkingsgrond niet evident te vinden is in een publieke taak, wordt soms gekozen voor de ´oplossing´ van “toestemming van de betrokkenen”. Maar niet iedere relatie tussen verwerker en betrokkene is er een waarin die toestemming vrijwillig gegeven kan worden. Situaties zoals deze zijn natuurlijke momenten om te overwegen of een verwerking echt rechtmatig is. Een tijdige realisatie dat een verwerking onrechtmatig is, kan een organisatie veel onrust en geld besparen.

Wanneer het ondanks het ontbreken van een verwerkingsgrond broodnodig is dat een verwerking plaatsvindt, dan kan de consultatie met de toezichthouder mogelijkheden bieden om de benodigde helderheid te krijgen.

6.4 Risicoanalyse: bekende methodes

Voor de risicoanalyse is het belangrijk dat deze een inventarisatie bevat van gebeurtenissen met een mogelijke negatieve impact op het leven van de betrokkenen (bijvoorbeeld weggebruikers) en een inschatting van de kans dat een dergelijke gebeurtenis plaatsvindt. Bedenk daarbij dat er meer risico’s moeten worden meegenomen dan alleen de privacyrisico’s. Zo is een risico op verkeerde medicatie ook een risico dat binnen de reikwijdte van de risicoanalyse van een PIA valt. Hierbij is het aanbevelenswaardig om dit zo concreet mogelijk te maken, ook met de gedachte dat het dan vaak ook relatief eenvoudig is om maatregelen te formuleren die de impact dan wel de kans reduceren.

Risicoanalysemodellen afkomstig uit de ISO27001 en NEN7510-werelden leiden relatief snel tot een kwaliteitssprong. Een voorbeeld van zo’n model dat zich met relatief weinig aanpassingen goed leent voor inzet in een PIA is het MAPGOOD-model dat Nederlandse gemeenten in hun informatiebeveiliging gebruiken. De afkorting MAPGOOD staat voor mensen, apparatuur, programmatuur, gegevens, organisatie, omgeving en dienstverlener. De kracht van dit model is dat het een breed scala aan gebeurtenissen met negatieve gevolgen voor de betrokkenen benoemt.

6.5 Afbakening van een (individuele) verwerking

Omdat de AVG geen afbakening kent van een individuele verwerking, worstelen veel organisaties met de vraag in hoeverre een bepaalde activiteit een zelfstandige verwerking is of dat deze onderdeel is van een groter geheel. In de praktijk kan dit tot bizarre uitkomsten leiden, zoals “er komt een PIA voor iedere applicatie in het applicatielandschap”, wat bij een wat grotere organisatie tot honderden PIA’s leidt. Invoering van de AVG wordt op deze wijze inderdaad een loodzware klus. Op basis van de criteria van de Europese toezichthouders voor een PIA is het logischer om basisprocessen die op een bepaald doel gericht zijn te clusteren en dan te kijken naar de gebruikte middelen, gegevens, mensen en doeleinden. Zoals alle bij een bepaald organisatieproces betrokken mensen, ICT-middelen, (online) diensten, organisaties en gegevens. Bedenk wel dat de AVG bij het samenvoegen van verwerkingen vereist dat alle (beveiligings- en continuïteits)maatregelen hetzelfde worden behandeld als bij de verwerking met de hoogste risico’s.

Ook als de afbakening van de PIA geen problemen oplevert, blijkt dat in veel organisaties de proces- en systeembeschrijvingen op een te hoog abstractieniveau zijn om op basis van de bestaande beschrijvingen een PIA te kunnen uitvoeren. In de praktijk is het nuttig voor de opstellers van de PIA om dan schermafdrukken of zelfs functionele specificatiedocumenten op te vragen of op te stellen. Ook het doorlopen van *use cases* met medewerkers die daadwerkelijk betrokken zijn bij de uitvoering kan een nuttige aanpak zijn om lacunes op te vullen. In de praktijk blijkt dat de bewustwording op de werkvloer hierdoor met sprongen toeneemt en dat er zo voorstellen voor maatregelen met draagvlak in de PIA komen. Het heeft dus voordelen om op deze manier de AVG-bril op te zetten.

6.6 Aanbevelingen voor de uitvoering van een PIA

Op basis van bovenstaande observaties uit de praktijk geven de auteurs de volgende aanbevelingen voor het uitvoeren van PIA's:

- Baken af vanuit de processen, niet vanuit de ICT-middelen;
- Reserveer tijd en geld voor gedetailleerde proces- en systeembeschrijvingen;
- Zorg voor senioriteit én pluriformiteit in de bemensing. Een goede PIA vraagt om een interdisciplinariteit die niet van alleen juristen of onervaren medewerkers kan worden verwacht;
- Als een verwerking een matige onderbouwing qua juridische grondslagen heeft, constateer dit dan. Overweeg liever opnieuw of de verwerking broodnodig is dan (als noodgreep) "toestemming van de betrokkenen" te gebruiken;
- Gebruik liever bestaande methoden vanuit de wereld van informatiebeveiliging en continuïteitsmanagement dan een eigen risicoanalyse te bedenken. Spieken mag niet alleen, het móét van de toezichthouders.

7. Verwerkersovereenkomsten

In dit hoofdstuk behandelen we een aantal van de meest voorkomende aspecten van verwerkersovereenkomsten die veel terugkomen in gesprekken tussen verwerkingsverantwoordelijken en hun verwerkers.

7.1 Noodzaak van verwerkersovereenkomsten

Over óf er wel een verwerkersovereenkomst nodig is, is vaak de nodige discussie. Aan de ene kant van het spectrum leeft de vraag of een verwerkingsovereenkomst nodig is bij inhuur, aan de andere kant van het spectrum kom je partijen tegen die vinden dat zij zelf een eigen verwerkingsverantwoordelijkheid hebben. De beslisregels zijn vrij eenvoudig: vindt er verwerking van persoonsgegevens onder verantwoordelijkheid van opdrachtgever plaats, maar zonder directe zeggenschap (gezagsverhouding) ten aanzien van de activiteiten van opdrachtnemer, dan moet die zeggenschap geschapen worden door een verwerkersovereenkomst. Bij de meeste gevallen van inhuur is een verwerkersovereenkomst dus niet nodig.

Een wegbeheerder met een eigen verwerkingsverantwoordelijkheid is een voorbeeld van een situatie waarin de verwerking van persoonsgegevens niet langer direct de verantwoordelijkheid van de opdrachtgever is.

7.2 Los document of integraal onderdeel van voorwaarden

In de voorganger van de AVG, de Wet bescherming persoonsgegevens (Wbp), sprak de Autoriteit Persoonsgegevens een duidelijke voorkeur uit voor een losse overeenkomst als de dienstverlening over meer dan het verwerken van persoonsgegevens ging. De vraag of de verwerkersovereenkomst altijd een los document moet zijn, wordt daarom buiten Nederland zelden gesteld.

Privacytoezichthouders in andere Europese landen hebben hier ten tijde van hun varianten van de Wbp verschillend over geoordeeld. Het is de vraag of het vroegere standpunt van de AP gehandhaafd zal blijven nu de regels in Europa meer gelijkgetrokken zijn door de AVG. Voor nu is het gangbaar om een losse overeenkomst op te stellen, al heeft bijvoorbeeld een partij als Microsoft het opstellen van verwerkersovereenkomsten wel in de algemene voorwaarden geregeld. Voor de herkenbaarheid verdient het aanbeveling om, als de verwerkingsovereenkomst wel onderdeel van een groter geheel is, deze als een apart hoofdstuk op te nemen.

7.3 Aansprakelijkheid en de beperking daarvan

De AVG zegt niets over aansprakelijkheid van partijen bij een verwerkingsovereenkomst, dus partijen dienen dit geheel naar eigen inzicht af te spreken. Wel zou de stelling verdedigd kunnen worden dat als de verwerker geen enkele aansprakelijkheid heeft, de verwerkingsverantwoordelijke ook geen goede machtsmiddelen heeft om zijn gezag over de verwerker uit te oefenen.

Daarbij is de maximale aansprakelijkheid eigenlijk een discussie die niet gevoerd zou hoeven te worden. Zolang duidelijk is dat aansprakelijkheidsbeperkingen doorbroken worden bij roekeloosheid of grove schuld van de zijde van de verwerker (wat gewoon is bij overeenkomsten onder Nederlands recht), is de belangrijkste richtlijn voor de aansprakelijkheid de kosten van bijvoorbeeld het melden aan betrokkenen van een datalek. Dat is een voor partijen verzekerbaar risico. Wie de boeterichtlijnen van

de Europese privacytoezichthouders in ogenschouw neemt, komt tot de conclusie dat de echt interessante boetebedragen pas gaan vallen als er sprake is van situaties waarin je snel van roekeloosheid of grove schuld kunt spreken.

7.4 Vrijwaringen tegen aanspraken van derden

In een samenwerking tussen partijen kan een situatie ontstaan waarbij één van de partijen geconfronteerd wordt met een aanspraak van een derde partij die eigenlijk een zaak van de wederpartij is. In de context van een verwerkersovereenkomst zou dat bijvoorbeeld een boete van de AP voor de wegbeheerder zijn voor gedrag van de verwerker. Of een klacht van een betrokkene over de verwerkingsgrondslag bij de verwerker, terwijl dat een zaak van de wegbeheerder is. Een vrijwaringsclausule beoogt de wederpartij te verplichten dit op te lossen zodat de aangesproken partij hier geen last van heeft.

Iedere praktijkjurist weet het: een contract zonder vrijwaringen tegen aanspraken van derden (denk daarbij aan schadeclaims van betrokkenen, maar ook boetes van de toezichthouder) is broddelwerk maar tegen de tijd dat je vrijwaringen in moet roepen is de vrijwarende partij in dusdanig zwaar weer beland dat ze waardeloos zijn. In de context van verwerkersovereenkomsten is dat nog een tandje erger: tegen een van de grootste risico's, een optreden van een toezichthouder, kan in feite niet gevrijwaard worden. Want het opkomen tegen datzelfde optreden wordt beheerst door het bestuursrecht en daarin speelt het begrip "belanghebbende" een grote rol. Een zinnige vrijwaringsclausule regelt dan ook dat de gevrijwaarde partij gesteund moet worden door de vrijwarende partij bij het bezwaar en beroep tegen de toezichthouder, maar een zuivere vrijwaring zoals we die in het privaatrecht kennen is het dan niet meer.

7.5 Onderaanneming van diensten

De AVG is helder over het onderaannemen van diensten. Er zijn twee varianten mogelijk. In de ene wordt voor iedere onderaannemer toestemming aan de verwerkingsverantwoordelijke gevraagd. In de andere variant deelt de verwerker veranderingen in de situatie voorafgaande aan de verandering mee aan de verwerkingsverantwoordelijke en kan deze laatste bezwaar maken. Lees: de relatie beëindigen. Dit wordt door leveranciers niet zelden als zeer belastend ervaren, maar toch is dit de maximale speelruimte die artikel 28 AVG hiervoor biedt.

7.6 Verantwoordelijkheid voor maatregelen?

In de huidige situatie is het nemen van maatregelen een gezamenlijke verantwoordelijkheid geworden van verwerker en verwerkersverantwoordelijke (lees: opdrachtnemer en opdrachtgever). Voor de praktijk valt te voorzien dat de verwerker een zeker minimum moet hanteren (afhankelijk van wat gebruikelijk is voor het type gegevens op dat moment) en dat de verwerkingsverantwoordelijke in staat moet zijn dit af te dwingen of meer te eisen als dat uit zijn eigen risicoafweging voortvloeit.
De AVG benoemt niet wie verantwoordelijk is voor de wijzigingen in beveiligings- en continuïteitsmaatregelen. Het is niet zo dat een van beide partijen de AVG als een open cheque kan lezen voor een goudgerande beveiliging, maar het is evenmin zo dat elke verandering in dit opzicht vanzelfsprekend in meer werk zou moeten uitmonden. Dit is uiteindelijk een puur commerciële discussie die in zekere zin losstaat van de verwerkersovereenkomst als zodanig. Een logische oplossingsrichting is dat wat 'branchegebruikelijk' is in de prijs inbegrepen zit en dat wat de opdrachtgever meer wil ook meer gaat kosten.

7.7 Wel of niet buiten de Europese Economische Ruimte?

De AVG vergt van verwerkingsverantwoordelijken dat zij ervoor waken dat persoonsgegevens niet buiten de Europese Economische Ruimte (lees: Europese Unie, Noorwegen, IJsland, Liechtenstein en Andorra) worden verwerkt zonder “adequate waarborgen”. Verwerkingsverantwoordelijken slaan hierbij nog weleens door in de veilige richting en eisen dat gegevens binnen Nederland blijven. Dat is onnodig en in de publieke sector zelfs in strijd met het aanbestedingsrecht.

Omgekeerd willen dienstverleners in hun verwerkingsrol vaak clausules voorstellen waarin een zogenaamde adequaatheidsverklaring van de Europese Commissie voldoende wordt gevonden. Zonder erbij te vermelden dat adequaatheidsverklaringen per direct ongeldig kunnen worden verklaard door het Hof van Justitie van de Europese Unie en dat dit in het verleden ook gebeurd is (Safe Harbor was zo’n adequaatheidsverklaring die in de zaak-Schrems per direct ongeldig is verklaard). Een plan B voor dat scenario ontbreekt meestal. Een redelijke middenweg is doorgaans om te beperken tot de Europese Economische Ruimte en Zwitserland.

7.8 Beperkingen in auditbevoegdheden

Een ander groot discussiepunt bij verwerkersovereenkomsten is een inperking van auditbevoegdheden. Vaak met een frase als “verwerkingsverantwoordelijke zal maximaal eens per jaar zijn auditbevoegdheid inroepen”. Overgewaaid uit uitbestedingscontracten en als zodanig verklaarbaar, maar nog steeds niet juist. Want wat te doen als de toezichthouder een halfjaar na de laatste audit om inlichtingen vraagt? Die gaat geen genoegen nemen met de boodschap dat de ICT-leverancier dat onredelijk vindt en dat er een halfjaar geduld geoefend moet worden. Verstandiger is om het inroepen van een auditbevoegdheid te relateren aan een redelijke aanleiding en een verzoek van de toezichthouder als voorbeeld van zo’n redelijke aanleiding te geven.

7.9 Exitregelingen

Voor vrijwel elke vorm van dienstverlening waar een verwerkersovereenkomst noodzakelijk voor is, geldt dat beëindiging van de dienstverlening ook aandacht behoeft in de verwerkersovereenkomst. Dit is voor wegbeheerders niet anders. Hierbij geldt wel dat een exitregeling recht moet doen aan de aard van de dienstverlening. Een contract met een papiervernietiger behoeft geen exitclausule, bijvoorbeeld. Maar dat met een uitbestedingspartij juist wel, en daarbij verdient het aanbeveling om een exitplan op te (laten) stellen en dat jaarlijks te vernieuwen. Bij Software-as-a-Service-leveranciers verdient het aanbeveling om te regelen dat de over te dragen gegevens in een goed gestructureerd en algemeen leesbaar elektronisch formaat worden overgedragen, zo nodig vergezeld van documentatie van de datastructuur.

Bijlage A Voorbeeld van een Verwerkingenregister

Verzamelnaam verwerkingsproces	Verzamelnaam subproces	(interne) eindverantwoordelijke	Verwerkingsdoeleinden	Categorieen van betrokkenen	Categorieen van persoonsgegevens	Categorieen van ontvangers	Doorgiften aan derden (of buiten EER)?	Bewaar- of archiveertermijn	Techn. of organ. maatregelen	Juridische grondslag	Verwerkingsverantwoordelijke of verwerker?	Verwerkersovereenkomst?	Geautomatiseerde of handmatige verwerking?	Ondersteunende applicatie en/of systemen?	Herkomst van persoonsgegevens?	SSO	PIA uitgevoerd?	Contractnummers	Evt toelichting
Verkeersmanagement	Aansturing verkeerregelinstallaties	Hoofd verkeersmanagement	Verbetering doorstroming verkeer	Weggebruikers, Particuliere vervoerders	Locatie en verplaatsingsgegevens	Wegbeheerders, NDW	nee	4 weken		Publieke taak	Verwerkingsverantwoordelijk	-	Geautomatiseerd	-	iVRI	-	ja	?	

Bijlage B Verklarende woordenlijst

Autoriteit Persoonsgegevens (AP): de Nederlandse toezichthouder op de Algemene verordening gegevensbescherming (AVG) en de uitvoeringswet AVG (UAVG).

Chief Information Security Officer (CISO): de verantwoordelijke voor het implementeren van en toezicht houden op het informatiebeveiligingsbeleid in de organisatie.

Correctierecht: het meest verstrekkende recht van een betrokkene, waarbij gegevens die objectief onjuist zijn altijd gecorrigeerd kunnen worden.

Documentatieplicht: de plicht om de persoonsgegevens via de juiste organisatorische en technische maatregelen te documenteren.

Data Protection Impact Assessment (DPIA): verplichte documentatie bij gegevensverwerkingen waarbij vooraf het vermoeden bestaat dat ze een verhoogd risico voor de betrokkenen met zich meebrengen.

Functionaris Gegevensbescherming (FG): de verantwoordelijke voor het vormgeven en bewaken van het privacybeleid in de organisatie.

Gegevenseffectbeoordelingen (GEB): verplichte documentatie bij gegevensverwerkingen waarbij vooraf het vermoeden bestaat dat ze een verhoogd risico voor de betrokkenen met zich meebrengen.

Inzagerecht: een breedstrekkend recht van betrokkenen. Een inzageverzoek kan alleen geweigerd worden als het rechten van derden raakt of wanneer het in strijd is met de eigen belangen van de betrokkene.

Meldplicht datalekken: de meldplicht datalekken houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Opschortingsrecht: het recht van betrokkenen om een verwerking te beperken.

Persoonsgegevens: alle informatie die (her)leidbaar is naar een natuurlijke persoon.

Privacy Impact Assessment (PIA): verplichte documentatie bij gegevensverwerkingen waarbij vooraf het vermoeden bestaat dat ze een verhoogd risico voor de betrokkenen met zich meebrengen.

Software-as-a-Service: software die wordt aangeboden als een online dienst, ook wel software on demand.

Transparantieverplichting: de verplichting waarbij betrokkenen geïnformeerd moeten worden over de verwerking van hun persoonsgegevens en onder welke voorwaarden.

Verantwoordingsplicht: de plicht die ervoor zorgt dat de gegevensbescherming aantoonbaar geborgd is in de organisatie.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Verwerkersovereenkomst: een document met de afspraken over hoe de gegevens worden verwerkt.

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Verwerkingenregister: het register dat alle verwerkingen van persoonsgegevens bijhoudt.

Verwerkingsgrondslagen: de juridische basisbeginselen voor een rechtmatige verwerking van persoonsgegevens.

Verwerkingsverantwoordelijke: degene die beslist wat het doel en de middelen zijn van de gegevensverwerking.

Verwijderingsrecht: officieel het recht op vergetelheid, artikel 17 AVG. Het recht van de betrokkene om de persoonsgegevens te laten verwijderen van de organisatie onder bepaalde omstandigheden.

Vrijwaring: een verplichting van de een contractspartij aan een andere contractspartij om aanspraken van derden op te lossen voor de andere contractspartij.

Wet bescherming persoonsgegevens (Wbp): de voorganger van de AVG. Een belangrijk verschil tussen de twee is de nieuw ingevoerde verantwoordingsplicht: een organisatie moet kunnen aantonen dat aan de eisen van de AVG voldaan wordt.