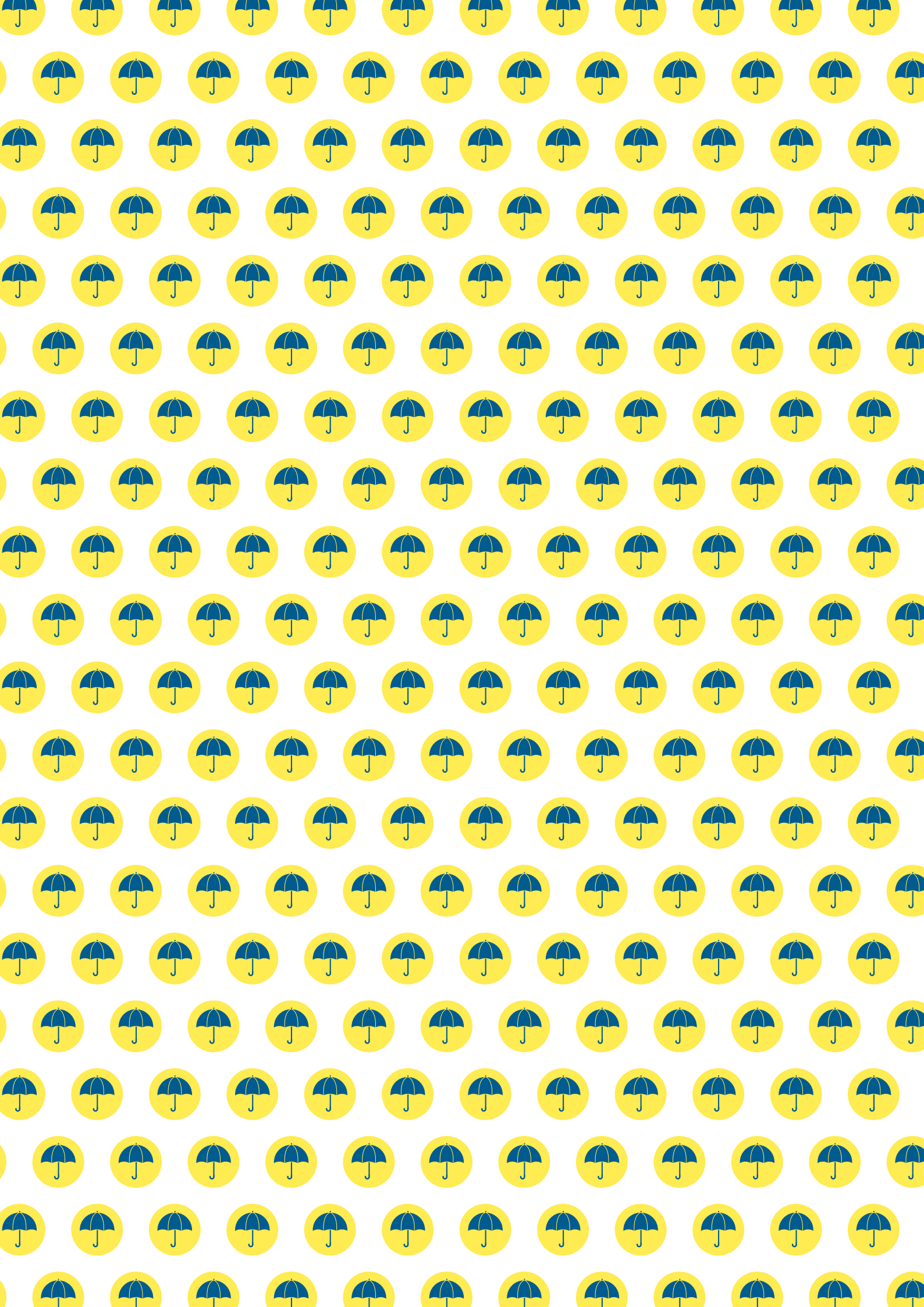
Ministerie van Infrastructuur
en Waterstaat

Leidraad omgaan met persoonsgegevens



Leidraad omgaan met persoonsgegevens

1 Voorwoord

Het stimuleren van gedragsverandering van weggebruikers is van groot belang om het wegennet beter te benutten. Als zij andere reistijden en routes of andere vervoermiddelen kiezen, maken we samen optimaal gebruik van ons wegennet. Uit het succes van spitsmijden- en fietsstimuleringsprojecten blijkt dat reizigers gevoelig zijn voor deze stimulering. Daarom willen we vanuit het ministerie van Infrastructuur en Waterstaat deze vraagbeïnvloedingsprojecten en tegelijkertijd ook verkeersonderzoeken faciliteren met IMMA, de Integrale Mobiliteitsmanagement Architectuur.

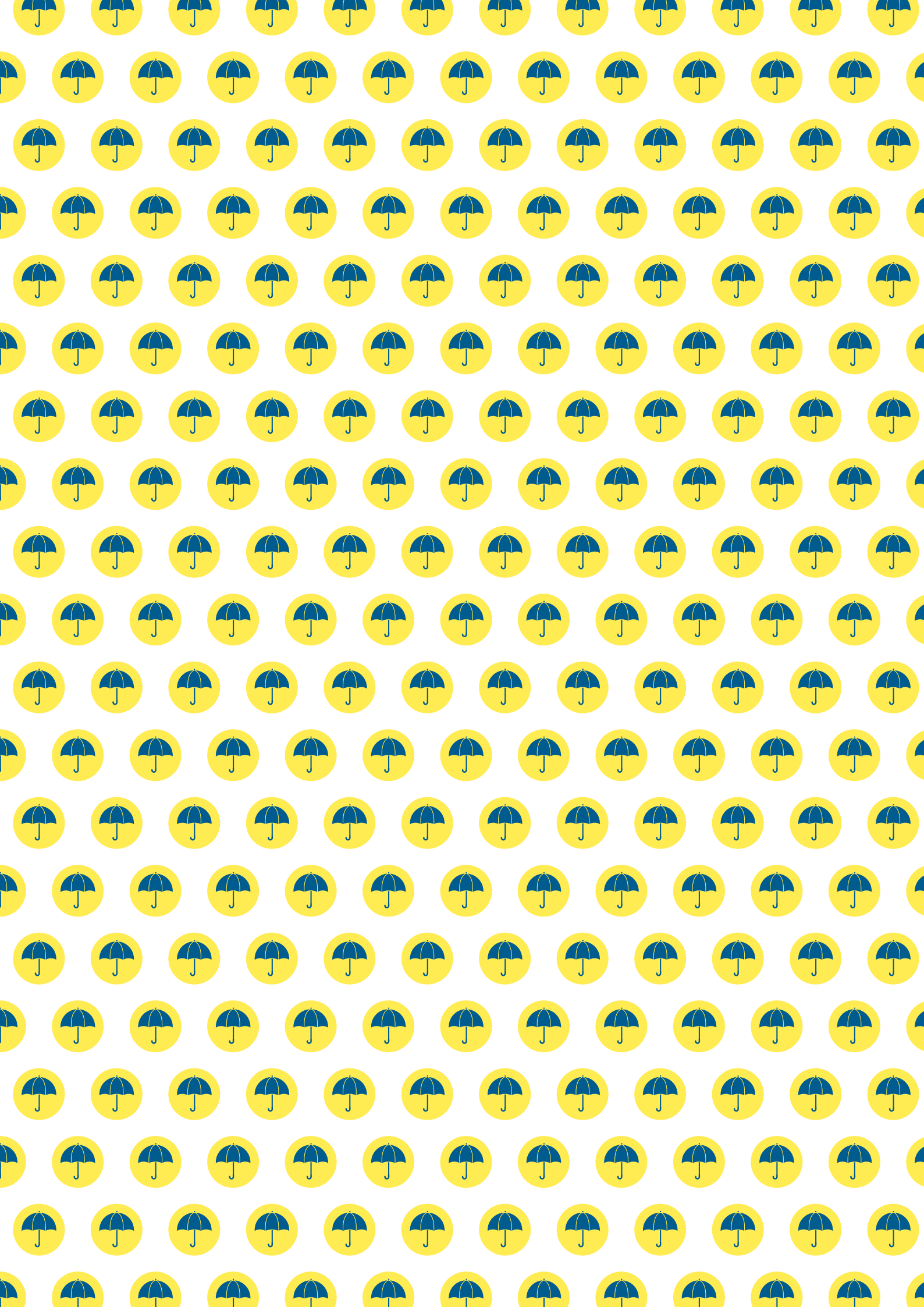
IMMA ontwikkelt op basis van geleerde lessen in vraagbeïnvloedingsprojecten degelijke producten om te komen tot een meer uniforme, efficiënte en verifieerbare manier van organiseren en uitvoeren van vraagbeïnvloedingsprojecten en verkeersonderzoeken. U kunt daarbij denken aan een Programma van Eisen met duidelijke kwalificaties voor marktpartijen. Maar ook aan het gezamenlijk laten ontwikkelen van innovatieve technieken om deelnemers te werven, gedrag te volgen en te belonen. De ontwikkeling van IMMA gaat snel en het project is succesvol. Daaruit blijkt dat dit project voorziet in de behoefte van marktpartijen en de overheid.

Innovatieve technieken en gedragsverandering in mobiliteit zijn nauw verweven met veiligheid en privacy. Om innovatieve technieken verantwoord in te zetten voor gedragsverandering, moeten ze voldoen aan wettelijke eisen op het gebied van privacy en persoonsbescherming en waar mogelijk al inspelen op nieuwe Europese eisen. Maar hoe voldoet u daaraan als overheid en marktpartij? Welke regels en voorwaarden gelden en wie is verantwoordelijk?

In deze *Leidraad omgaan met persoonsgegevens* worden de verschillende wettelijke eisen voor privacy overzichtelijk en degelijk uiteengezet, en duidelijk toegelicht. Voorbeelden zorgen voor de vertaling naar uw praktijk. Deze leidraad is in nauwe samenwerking met Considerati tot stand gekomen.
IMMA-projecten bieden de reiziger zo de zekerheid dat de privacy optimaal wordt geborgd. Wij wensen u succesvolle IMMA-projecten toe.

Katya Ivanova
Programmamanager Maastricht-Bereikbaar, trekkende regio voor IMMA.

Inhoudsopgave



2 Achtergrond

Het ministerie van Infrastructuur en Waterstaat (IenW) wil de ontwikkeling van mobiliteits- en spitsmijdenprojecten faciliteren en de opbrengsten ervan breed inzetbaar maken, binnen de grenzen van de wet. In dat kader is de Integrale Mobiliteitsmanagement Architectuur (IMMA) opgesteld. Deze architectuur maakt een meer uniforme, efficiënte en verifieerbare manier van de uitvoering van vraagbeïnvloedingsprojecten en verkeersonderzoeken mogelijk. Binnen het juridische kader voor mobiliteitsprojecten spelen de verwerking van persoonsgegevens en de eisen van de Algemene Verordening Gegevensbescherming een belangrijke rol. Om te borgen dat nieuw te ontwikkelen projecten ook in overeenstemming zijn met geldende privacywetgeving en -regelgeving is, als onderdeel van IMMA, de *Leidraad omgaan met persoonsgegevens* opgesteld. Uitgangspunt moet zijn dat de dienstaanbieders van mobiliteits- en spitsmijdenprojecten gegevensbescherming gaan zien als een license to operate.

Deze leidraad geeft de 'baseline' waaraan projecten moeten voldoen om privacy compliant te zijn. Concreet betekent dit dat de leidraad principes, standaarden en eisen formuleert waaraan mobiliteits- en spitsmijdenprojecten dienen te voldoen op basis van het geldende wettelijk kader: de Algemene Verordening Gegevensbescherming en de Cookiewet (die op termijn wordt vervangen door de ePrivacy Verordening).

Het is van belang te vermelden dat de IMMA *Leidraad omgaan met persoonsgegevens* geen nieuwe eisen stelt die niet reeds op grond van de wet aan projecten en applicaties worden gesteld. De leidraad dient enkel ter verduidelijking van de plichten. Ook schetst de leidraad slechts een kader en schrijft het geen concrete maatregelen voor, dit is namelijk altijd ter beoordeling van de verwerkingsverantwoordelijke op basis van de concrete toepassing. De verwerkingsverantwoordelijke moet met alle gestelde eisen rekening houden en kunnen verantwoorden waarom bepaalde keuzes voor het invullen van deze eisen zijn gemaakt.

Om deze privacyleidraad toegankelijker en bruikbaarder te maken voor inschrijvende partijen worden per eis ook voorbeelden en waar mogelijk best practices opgenomen.

3 Begrippenlijst

AP
Autoriteit Persoonsgegevens, de Nederlandse toezichthouder op de naleving van de Algemene Verordening Gegevensbescherming. Sinds de inwerkingtreding van de Algemene Verordening Gegevensbescherming heeft de AP een uitgebreidere boetebevoegdheid.

AVG
De Algemene Verordening Gegevensbescherming. De Europese privacyverordening die vanaf 25 mei 2018 de Wet bescherming persoonsgegevens vervangt. Deze verordening is direct toepasbaar in de nationale rechtsorde van EU-lidstaten, maar laat op bepaalde gebieden ruimte voor implementatieverschillen. Voor Nederland zijn deze verschillen opgenomen in de Uitvoeringswet AVG.

Betrokkene
De persoon op wie de gegevens betrekking hebben. Dit kan een consument zijn (een klant van bijvoorbeeld een spitsmijden-app) maar ook een medewerker van een bedrijf (bijvoorbeeld een medewerker wiens verplaatsingen worden gevolgd ten behoeve van fleetmanagement).

Cookie
Kleine tekstbestanden die op de computer, mobiele telefoon, tablet of ander apparaat van een gebruiker kunnen worden geplaatst met als doel het identificeren van het apparaat.

Cookiewet
De regels over cookies zijn opgenomen in art. 11.7a van de Telecommunicatiewet, kortweg ook vaak de Cookiewet genoemd. In deze wet wordt het gebruik van cookies gereguleerd. Deze wetgeving wordt de komende jaren vervangen door de Europese ePrivacy Verordening, die naar verwachting vanaf 2019 gaat gelden.

DPIA
DPIA staat voor data protection impact assessment. In de AVG wordt dit de gegevensbeschermingseffectbeoordeling genoemd. Deze beoordeling is verplicht wanneer sprake is van een verwerking van persoonsgegevens met een hoog risico voor de rechten en vrijheden van betrokkenen, bijvoorbeeld bij stelselmatige en grootschalige monitoring van openbare ruimten.

Derde
Degene die niet de betrokkene, de verwerkingsverantwoordelijke of de verwerker is.

Ontvanger
De derde aan wie persoonsgegevens worden doorgegeven.

Persoonsgegevens
Alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
Geïdentificeerd houdt in dat een natuurlijke persoon uniek te onderscheiden is van andere personen op basis van identificerende gegevens (bijvoorbeeld NAW).

Identificeerbaar betekent dat een natuurlijke persoon direct of indirect kan worden geïdentificeerd ('to single out') door de verwerkingsverantwoordelijke en/of redelijkerwijs door derden, met name aan de hand van een identificator zoals een naam, identificatienummer, locatiegegevens, een online identificator of één of meer kenmerken van de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van deze persoon.

Profilering
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Verwerker
Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Dat wil zeggen: overeenkomstig de instructies van de verwerkingsverantwoordelijke en onder zijn (uitdrukkelijke) verantwoordelijkheid, zonder aan zijn rechtstreeks gezag te zijn onderworpen. De verwerker is dus een buiten de organisatie van de verwerkingsverantwoordelijke staande persoon of instelling die geen hiërarchische relatie met de verwerkingsverantwoordelijke heeft, maar een opdrachtgever-opdrachtnemerrelatie.

Verwerkingsverantwoordelijke
De natuurlijke persoon, rechtspersoon of ieder ander die, of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerking van persoonsgegevens
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt het hele proces dat een persoonsgegeven doorloopt, vanaf het moment van verzamelen tot het moment van vernietigen.

4 Algemene toelichting privacywetgeving

Voor IMMA zijn op het gebied van privacy twee wetten van belang: de Algemene Verordening Gegevensbescherming (AVG) en de zogenoemde Cookiewet. De AVG geeft de regels voor de zorgvuldige verwerking van persoonsgegevens. De Cookiewet (artikel 11.7a Telecommunicatiewet) schrijft voor dat de gebruiker in principe toestemming moet geven voor het plaatsen van informatie op zijn randapparatuur en voor het uitlezen van informatie van de randapparatuur.

In het kader van IMMA spelen twee stukken wetgeving specifiek een belangrijke rol: de Algemene Verordening Gegevensbescherming (AVG) en de Cookiewet.

4.1 Algemene Verordening Gegevensbescherming (AVG)

Vanaf 25 mei 2018 is de AVG volledig van toepassing in Nederland en de andere Europese lidstaten. De Wet bescherming persoonsgegevens (Wbp) is dan niet langer van toepassing en de AVG bepaalt wanneer persoonsgegevens mogen worden verwerkt. Net als in de Wbp, is de kern van de AVG dat persoonsgegevens alleen mogen worden verwerkt voor nadrukkelijk omschreven en gerechtvaardigde doeleinden. Een doel is gerechtvaardigd als het gebaseerd kan worden op één van de grondslagen uit de Algemene Verordening Gegevensbescherming (zie artikel 6 AVG).

Wanneer er een gerechtvaardigd doel is, dan mogen gegevens verwerkt worden, maar alleen als ook aan de materiële eisen uit de AVG is voldaan. Het gaat dan om zaken als beveiliging, transparantie en het respecteren van de rechten van betrokkene.

Schematisch kan de logica van de AVG als volgt worden weergegeven:

De belangrijkste wijzigingen

Ten opzichte van de Wet bescherming persoonsgegevens stelt de AVG een aantal strengere eisen aan de verwerkingsverantwoordelijke, met name op het gebied van controle en verantwoording (accountability). Daarnaast is een aantal al bestaande bepalingen wat duidelijker

beschreven of verder uitgebreid. Overige veranderingen ten opzichte van de Wbp zijn onder meer een uitbreiding van het toepassingsgebied van de wetgeving, een sterkere rol voor de functionaris gegevensbescherming (FG), de verplichting van het uitvoeren van een gegevensbeschermingseffectbeoordeling (de DPIA) voor verwerkingen met een hoog risico en de plicht om een register van verwerkingsactiviteiten bij te houden. Ook zijn de boetes verhoogd en is het mogelijk om voor bepaalde overtredingen van de AVG een maximumboete te krijgen van 20 miljoen euro of 4% van de wereldwijde jaaromzet.

4.2 Cookiewet

Artikel 11.7a Telecommunicatiewet, in de volksmond beter bekend als de Cookiewet, stelt dat het plaatsen van informatie op de randapparatuur van een gebruiker (de betrokkene) of het uitlezen van informatie van de randapparatuur in beginsel alleen mag als daar toestemming van deze gebruiker voor is. Uitgezonderd zijn situaties waar het uitlezen/plaatsen van gegevens technisch noodzakelijk is, of waar het uitlezen/plaatsen slechts een geringe inbreuk op de privacy oplevert.[1]

Omdat het plaatsen van een cookie de meest gebruikte methode is om gegevens op randapparatuur te plaatsen en uit te lezen wordt de wet de Cookiewet genoemd. Maar de wet is nadrukkelijk van toepassing op alle vormen van uitlezen van en plaatsen op randapparatuur. Denk hierbij onder andere aan het gebruiken van Software Development Kits (SDKs), beacons en device fingerprinting. Waar wij in dit document spreken over cookies, worden nadrukkelijk ook al deze andere mogelijkheden bedoeld.

Ook het begrip randapparatuur is heel breed. Dit betekent dat niet alleen computers onder de definitie vallen, maar ook smartphones, smartwatches, navigatiekastjes en zelfs auto's.

In de Europese Unie wordt momenteel gewerkt aan een Europese ePrivacy Verordening die de huidige Cookiewet gaat vervangen. Daarbij zal ook het toezicht op de naleving van deze regelgeving verschuiven van de Autoriteit Consument en Markt (ACM) naar de Autoriteit Persoonsgegevens (AP). Omdat de tekst van deze nieuwe verordening nog niet definitief is en nog niet bekend is wanneer deze in werking treedt, laten we deze verordening buiten beschouwing.

[1] Naast het gebruik van cookies reguleert de Telecommunicatiewet het gebruik van locatiegegevens. Deze bepalingen zijn enkel van toepassing op aanbieders van openbare telecommunicatienetwerken en diensten. Deze bepalingen blijven buiten beschouwing in deze brochure.

5 Overzicht IMMA privacy

Elk IMMA-project moet op het gebied van privacy en de bescherming van persoonsgegevens invulling geven aan zestien eisen. Denk bijvoorbeeld aan eisen voor verwerkingsverantwoordelijkheid, dataminimalisatie, privacy by design en aan eisen voor het bewaren en vernietigen van persoonsgegevens en het melden van datalekken. In dit hoofdstuk zetten we eisen kort op een rij. In de volgende hoofdstukken gaan we dieper op de eisen in.

Elk IMMA-project moet op het gebied van privacy en de bescherming van persoonsgegevens invulling geven aan de volgende eisen:

5.1 Verantwoordelijkheid

- De verwerkingsverantwoordelijke voor de gegevensverwerking is duidelijk benoemd.
- De verwerkingsverantwoordelijke maakt afspraken met de verwerker(s) over de veilige en zorgvuldige verwerking van persoonsgegevens.

5.2 Verantwoording (accountability)

- De verwerkingsverantwoordelijke moet kunnen aantonen dat hij compliant is met (voldoet aan) de AVG.

5.3 Legitiem doel en grondslag

- De reden voor het verwerken van persoonsgegevens in het kader van de IMMA-toepassing (het verwerkingsdoel) is vooraf bepaald en voldoende duidelijk omschreven.
- De verwerking van persoonsgegevens moet gebaseerd kunnen worden op één van de grondslagen van artikel 6 AVG.
- Wanneer ondubbelzinnige toestemming (artikel 6 lid 1 sub a AVG) als grondslag wordt gebruikt, wordt deze voorafgaand aan het verwerken van de persoonsgegevens gevraagd.
- Wanneer voor de toepassing gegevens worden geplaatst op de randapparatuur van de gebruiker, of daarvan informatie wordt uitgelezen, wordt dit gedaan met toestemming of is het gebruik gebaseerd op één van de uitzonderingen van 11.7a Telecommunicatiewet.

5.4 Dataminimalisatie

- Voor de toepassing mogen niet meer gegevens worden gebruikt dan noodzakelijk is om de doelen van de toepassing te bereiken.

5.5 Privacy by design and by default

- Vanaf het ontwerp van IT-systemen en bedrijfsprocessen wordt rekening gehouden met privacybescherming (privacy by design).
- Standaard worden de meeste privacyvriendelijke instellingen gepresenteerd aan betrokkene (privacy by default).

5.6 Data protection impact assessment

- Het uitvoeren van een data protection impact assessment (DPIA) is verplicht voor toepassingen waarvan vermoed wordt dat ze een hoog risico voor de privacyrechten en -vrijheden van betrokkenen met zich meebrengen.

5.7 Doelbinding

- Gegevens mogen alleen verwerkt worden voor het doel waarvoor ze verzameld zijn, tenzij het nieuwe doel verenigbaar is met het oorspronkelijke doel.

5.8 Informatie en transparantie

- Het moet voor de betrokkene helder zijn welke persoonsgegevens worden verwerkt en voor welke doeleinden ze worden gebruikt.

5.9 Delen van gegevens met derden

- Gegevens worden alleen gedeeld met derden als daar een rechtmatige grondslag voor is.

5.10 Rechten van de betrokkene

- In de toepassing wordt rekening gehouden met en invulling gegeven aan de rechten van de betrokkene.

5.11 Informatiebeveiliging

- De toepassing moet voldoende worden beveiligd door passende technische en organisatorische maatregelen te treffen tegen verlies of enige andere vorm van onrechtmatige verwerking.

5.12 Bewaren en vernietigen

- Gegevens zijn voorzien van een bewaartermijn.
- Gegevens worden vernietigd of geanonimiseerd wanneer zij niet langer noodzakelijk zijn voor de verwerkingsdoelen.

5.13 Gegevensexport

- Gegevens mogen niet naar een land worden verstuurd waar géén adequaat niveau van privacybescherming is.

5.14 Meldplicht datalekken

- De verwerkingsverantwoordelijke stelt de Autoriteit Persoonsgegevens (AP) op de hoogte van een beveiligingsinbreuk die leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.
- De verwerkingsverantwoordelijke stelt ook de betrokkene op de hoogte van bovengenoemde beveiligingsinbreuk, wanneer deze waarschijnlijk ongunstige gevolgen heeft voor zijn persoonlijke levenssfeer.

5.15 Aanstellen functionaris voor gegevensbescherming

- De verwerkingsverantwoordelijke stelt een functionaris voor gegevensbescherming (FG) aan wanneer:
  - de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan;
  - het op grote schaal volgen van individuen de kernactiviteit is van de verwerkingsverantwoordelijke;
  - het op grote schaal verwerken van bijzondere persoonsgegevens een kernactiviteit is van de verwerkingsverantwoordelijke.

5.16 Registerplicht

- De verwerkingsverantwoordelijke houdt een register bij van verwerkingen van persoonsgegevens.
- De verwerker houdt een register bij van verwerkingen van persoonsgegevens.
- Deze plicht geldt niet voor een verwerkingsverantwoordelijke of verwerker die minder dan 250 werknemers in dienst heeft, tenzij sprake is van verwerkingen met een hoog risico of verwerkingen van bijzondere categorieën van persoonsgegevens.

6 Verantwoordelijkheid

Op basis van de AVG moet u duidelijk benoemen wie de verwerkingsverantwoordelijke is voor de gegevensverwerking. De verwerkingsverantwoordelijke is de natuurlijke- of rechtspersoon die het doel en de middelen van de verwerking van de persoonsgegevens bepaalt. Zowel de opdrachtgever, als de opdrachtnemer kunnen aangemerkt worden als verwerkingsverantwoordelijke. Binnen een samenwerkingsverband kunnen ook meerdere rechtspersonen verwerkingsverantwoordelijke zijn. Diverse voorbeelden maken duidelijk hoe u de verwerkingsverantwoordelijkheid in de praktijk kunt bepalen.

6.1 Eis

- ***De verwerkingsverantwoordelijke voor de gegevensverwerking is duidelijk benoemd.***

- ***De verwerkingsverantwoordelijke maakt afspraken met de verwerker(s) over de veilige en zorgvuldige verwerking van persoonsgegevens.***

6.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:
- Artikel 3 AVG
- Artikel 4 onder 7 AVG
- Artikel 28 AVG

6.3 Toelichting

De verwerkingsverantwoordelijke
De verwerkingsverantwoordelijke is de natuurlijke of rechtspersoon die verantwoordelijk is voor de gegevensverwerking. Omdat de AVG van toepassing is op de verwerkingsverantwoordelijke, is het van groot belang dat helder is wie de verwerkingsverantwoordelijke is. Met name als er sprake is van samenwerkingsverbanden.

De verwerkingsverantwoordelijke is degene die het doel en de middelen van de verwerking bepaalt. Wanneer in het kader van een project persoonsgegevens worden verwerkt, moet dus worden gekeken wie degene is die uiteindelijk bepaalt welke persoonsgegevens worden verwerkt, voor welk doel dit is en welke middelen (geld, mensen, IT-voorzieningen) daarvoor worden ingezet. In aanbestedingstrajecten kan de opdrachtgever verwerkingsverantwoordelijke zijn, maar ook de opdrachtnemer. Dit moet van geval tot geval worden bekeken. Het enkele aanbesteden betekent nog niet automatisch dat de opdrachtgever ook verwerkingsverantwoordelijke is.
De verwerkingsverantwoordelijke is niet een individu binnen een organisatie, maar de organisatie (de rechtspersoon) zelf.

Wanneer er meerdere verwerkingsverantwoordelijken zijn, bijvoorbeeld binnen een samenwerkingsverband, dan worden de onderlinge verhoudingen en afspraken over deze (mede) verantwoordelijkheid duidelijk vastgelegd.

Verwerkers

Wanneer de verwerkingsverantwoordelijke een derde partij inhuurt die in opdracht van de betrokkene persoonsgegevens verwerkt, dan is de verwerkingsverantwoordelijke verplicht contractuele afspraken te maken met de verwerker over de omgang met persoonsgegevens. In het bijzonder zijn afspraken over de beveiliging van persoonsgegevens van belang.

6.4 Voorbeelden

Voorbeeld 1

SnellerThuis BV ontwikkelt een spitsmijdenapplicatie voor het ov. SnellerThuis geeft mensen korting als ze buiten de spits reizen. SnellerThuis verzamelt onder andere naam, adres, woonplaats, rekeningnummer en reisgedrag. SnellerThuis laat de app ontwikkelen door SoftwareBouwer BV. De app draait bij GoedeHost BV. In dit voorbeeld is SnellerThuis de verwerkingsverantwoordelijke: zij bepalen het doel (de gegevens verzamelen ten behoeve van spitsmijden) en de middelen (het maken van een app en het hiertoe inhuren van derden). SoftwareBouwer BV is in dit scenario niet relevant voor de AVG, GoedeHost BV is een verwerker.

Voorbeeld 2

Een voorbeeld van een privacy policy waarin de verwerkingsverantwoordelijke duidelijk is benoemd, is de privacy policy van MyOV. MyOV is een website en app die de treinreizen van gebruikers volgt en kortingen of aanbiedingen geeft als zij reizen buiten de spits. In hun privacy policy heeft Data-Lab B.V. heel duidelijk aangegeven wie zij zijn, waar ze gevestigd zijn en dat zij de verwerkingsverantwoordelijke zijn voor de verwerking van persoonsgegevens door deze app.

MyOV privacy policy

Om u goed van dienst te kunnen zijn moeten wij bepaalde gegevens van u verwerken. Data-lab neemt uw privacy zeer serieus en behandelt uw gegevens daarom uiterst zorgvuldig.

MyOV is een spitsmijdenprogramma dat u wordt aangeboden door Data-Lab B.V, Stationsplein 61, 3818 LE Amersfoort. Data-Lab B.V. is de verantwoordelijke voor de verwerking van persoonsgegevens door MyOV in de zin van de Wet bescherming persoonsgegevens.

Voorbeeld 3

Een ander voorbeeld is de privacy policy van Praktijkproef Amsterdam, een initiatief dat onder de naam Amsterdam onderweg reizigers adviseert welke route te nemen als ze de spits willen mijden in Amsterdam. Hier is niet alleen de verwerkingsverantwoordelijke duidelijk vastgesteld, maar ook de verwerker is benoemd.

De Praktijkproef Amsterdam (PPA) is een initiatief van de gemeente Amsterdam, provincie Noord-Holland, Rijkswaterstaat en de stadsregio Amsterdam. De PPA is een grootschalige proef die zich richt op het verminderen van files in de regio Amsterdam. Tijdens de proef wordt gebruik gemaakt van innovatieve technologieën in de auto en op de weg.

Rijkswaterstaat West-Nederland Noord , gevestigd te Haarlem, is de opdrachtgever van Amsterdam onderweg en is verantwoordelijk voor de verwerking van persoonsgegevens.
Amsterdam onderweg, een samenwerking van TNO en ARS Traffic & Transport Technology, gevestigd te Den Haag, is de opdrachtnemer van de PPA en de bewerker van persoonsgegevens.

Voorbeeld 4

De app van vervoersmaatschappij Syntus (Inmiddels Keolis genaamd) biedt gebruikers onder andere de mogelijkheid hun reis te plannen, vervoersbewijzen te kopen en punten te sparen door de spits te mijden bij hun treinreis. In de privacy policy is duidelijk vermeld dat Syntus de verwerkingsverantwoordelijke is en zijn ook de contactgegevens en het KVK-nummer van Syntus vermeld.

Algemeen

De Syntus app is een applicatie (app) voor de smartphone waarmee u een reis kunt plannen en vervoersbewijzen kunt kopen. Het heeft een geïntegreerd programma waarbinnen gebruikers van de app punten kunnen sparen voor o.a. het reizen buiten de Spits. Syntus B.V. (Syntus) biedt de Syntus app aan en is gevestigd op de Visbystraat 5, 7418 BE Deventer en ingeschreven bij de KvK onder handelsregisternummer 09102634. Syntus is verantwoordelijke in de zin van de Wet Bescherming Persoonsgegevens voor de verwerking van persoonsgegevens van de Syntus app.

7 Verantwoording

Een belangrijke aanvullende verplichting die de AVG ten op zichte van de Wbp stelt, is dat de verwerkingsverantwoordelijke niet alleen in overeenstemming met de AVG moet handelen, maar dit ook moet kunnen aantonen. U moet dus verantwoorden hoe u de wet naleeft.

7.1 Eis

De verwerkingsverantwoordelijke moet kunnen aantonen dat hij compliant is met de AVG.

7.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepaling:

- Artikel 5 lid 2 AVG

7.3 Toelichting

Een van de belangrijkste wijzigingen in de AVG ten opzichte van de Wbp is dat de gegevensverwerkingen niet meer aan de Autoriteit Persoonsgegevens (AP) gemeld hoeven te worden. Hiervoor in de plaats geldt het accountability-principe: de verantwoordingsplicht. Dit houdt in dat de naleving van de AVG door de verwerkingsverantwoordelijke aantoonbaar moet zijn. De verwerkingsverantwoordelijke moet kunnen aantonen dat hij de persoonsgegevens rechtmatig, behoorlijk en transparant verwerkt, dat deze voldoende beveiligd zijn en voldoen aan de eis van doelbinding. Ook moeten de persoonsgegevens toereikend en juist zijn en niet langer bewaard worden dan noodzakelijk. Met onder meer het verwerkingenregister en de documentatie over uitgevoerde DPIA's kan de verwerkingsverantwoordelijke aantonen dat hij voldoet aan de vereisten van de AVG.

7.4 Voorbeelden

Voorbeeld 1

Car-Online.nl verwerkt persoonsgegevens van klanten, bezoekers van de website en van eigen medewerkers. Door middel van een privacystatement, interne beleidsstukken, DPIA-procedures, DPIA-rapportages en een verwerkingenregister kan Car-Online.nl aantonen hoe het voldoet aan de eisen van de AVG. Hierdoor is het voor betrokkenen, medewerkers en de toezichthouder duidelijk welke persoonsgegevens door het bedrijf worden verwerkt, waarom deze persoonsgegevens worden verwerkt en wat er vervolgens allemaal met die persoonsgegevens wordt gedaan.

8 Legitiem doel en grondslag

De AVG schrijft voor dat u persoonsgegevens alleen mag verwerken met een vooraf vastgesteld en duidelijk omschreven doel. Bovendien moet de verwerking gebaseerd zijn op een wettelijke grondslag, zoals het geven van toestemming of noodzakelijk voor de uitvoering van een overeenkomst. In dit hoofdstuk worden de verschillende grondslagen beschreven en toegelicht. Ook wordt duidelijk welke voorwaarden gelden voor het verkrijgen van toestemming van de gebruiker en wanneer sprake is van een noodzakelijke verwerking. Voorbeelden laten zien hoe u in de praktijk toestemming voor verwerking van persoonsgegevens regelt en een doel duidelijk omschrijft.

8.1 Eis

- ***De reden voor het verwerken van persoonsgegevens in het kader van het project (het verwerkingsdoel) is vooraf bepaald en voldoende duidelijk omschreven.***

- ***De verwerking van persoonsgegevens moet gebaseerd zijn op één van de grondslagen uit artikel 6 AVG.***

- ***Wanneer ondubbelzinnige toestemming als grondslag wordt gebruikt, wordt deze voorafgaand aan het verwerken van de persoonsgegevens gevraagd en moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven.***

- ***Wanneer voor de toepassing gegevens worden geplaatst op de randapparatuur van de gebruiker, of daarvan informatie wordt uitgelezen, wordt dit gedaan met toestemming of is het gebruik gebaseerd op één van de uitzonderingen van 11.7a Telecommunicatiewet.***

8.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:
- Artikel 5 lid 1 sub b AVG
- Artikel 6 sub a en sub f AVG
- Artikel 7 lid 1 AVG
- Artikel 11.7a Telecommunicatiewet

8.3 Toelichting

8.3.1 Doel

De beoogde verwerking dient een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel te hebben. Het is niet toegestaan om persoonsgegevens te verzamelen zonder van tevoren een precieze omschrijving van het doel te hebben bepaald. De omschrijving mag niet te vaag of ruim geformuleerd zijn. Wel is het toegestaan om meerdere doelen te formuleren per toepassing.

Tevens is van belang dat de noodzakelijkheid van de verwerking van persoonsgegevens wordt beoordeeld. Dit houdt in dat u zich moet afvragen of het doel ook bereikt kan worden met minder persoonsgegevens of op een andere manier waarbij minder persoonsgegevens worden verwerkt.

8.3.2 Grondslagen

Om een doel gerechtvaardigd te maken, moet dit doel gebaseerd kunnen worden op één van de grondslagen uit artikel 6 AVG. Kan de verwerking niet gerechtvaardigd worden op basis van één van deze doelen, dan is zij niet toegestaan.

De zes grondslagen zijn:

a) De betrokkene heeft toestemming gegeven voor een of meer specifieke doeleinden.
b) De verwerking is noodzakelijk om de overeenkomst met de betrokkene uit te voeren, of om op verzoek van betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
c) De verwerking is noodzakelijk om te voldoen aan een wettelijke plicht die op de verwerkingsverantwoordelijke rust.
d) De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.
e) De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
f) De verwerking is noodzakelijk om een gerechtvaardigd belang van de verwerkingsverantwoordelijke of van een derde te waarborgen dat zwaarder weegt dan de privacyinbreuk bij de betrokkene.

Voor IMMA-projecten zullen met name 6a, 6b en 6f AVG relevant zijn.[2]

[2] De grondslag 'wettelijke plicht' heeft betrekking op een wettelijke plicht die rust op de verwerkingsverantwoordelijke, zoals het verstrekken van gegevens aan de Belastingdienst voor de uitvoering van de belastingwetgeving. Hoewel deze grondslag van toepassing kan zijn, zal zij niet snel de basis vormen voor het uitvoeren van een mobiliteitsproject. De grondslag 'vrijwaring vitaal belang' heeft betrekking op leven-en-dood-situaties en zal niet van toepassing zijn op mobiliteitsprojecten. De grondslag 'vervulling taak van algemeen belang' kan alleen worden gebruikt door publiekrechtelijke organisaties zoals ministeries en uitvoeringsinstanties.

6a AVG: Toestemming van de betrokkene

Wanneer een verwerking niet per se noodzakelijk is, dan mogen de gegevens alleen verwerkt worden als daar toestemming voor is.

Als u gebruik maakt van toestemming van de betrokkene als grondslag, dan moet deze toestemming aan de volgende eisen voldoen:

- De toestemming moet vrij gegeven zijn. Dit betekent dat het weigeren van de toestemming geen negatieve gevolgen voor de betrokkene mag hebben. Houd er rekening mee dat in de meeste gevallen werknemers geen toestemming kunnen geven. Zij zijn niet vrij omdat ze in een afhankelijkheidsrelatie tot de werkgever staan. Voor bijvoorbeeld telematica en fleet-management is de toestemming daarom een minder geschikte grondslag.
- De toestemming moet op duidelijke informatie berusten. De betrokkene moet weten waarvoor hij toestemming geeft, bijvoorbeeld dat zijn locatiegegevens worden gebruikt om de verkeersstromen op zijn route in kaart te brengen. Deze informatie moet ook eenvoudig toegankelijk zijn. De informatie wegstoppen in de algemene voorwaarden en de betrokkene daarmee akkoord laten gaan, is bijvoorbeeld niet toegestaan.
- Uit de voorgaande eis vloeit ook voort dat de toestemming concreet en afgebakend moet zijn. Alleen als het doel voldoende concreet is, dan kan er toestemming voor worden gegeven. ‘Wij verwerken uw gegevens voor onze goede bedrijfsvoering en het verbeteren van de mobiliteit in Nederland’ bijvoorbeeld is te vaag. Er mag bij de betrokkene geen twijfel bestaan waarvoor hij toestemming geeft.
- De toestemming moet voorafgaand aan de verwerking worden gegeven. Met andere woorden, de gegevens mogen niet verwerkt worden (zelfs niet verzameld) voordat de toestemming gegeven is. Wanneer er iets substantieel verandert in de verwerking (meer persoonsgegevens, nieuwe doelen), moet u de toestemming hernieuwen.
- De toestemming moet ondubbelzinnig zijn. Dit betekent dat het helder moet zijn dat betrokkene toestemming heeft gegeven en waarvoor. Voor de toestemming geldt geen vormvereiste, maar de toestemming moet wel geuit zijn. Geïmpliceerde toestemming (wie zwijgt, stemt toe bijvoorbeeld) is niet geldig. Er moet een actieve handeling zijn van

de betrokkene waaruit u de toestemming op kunt maken. Dit kan zowel in woord, schrift of gedrag. Een vooraf aangevinkt hokje mag bijvoorbeeld niet. De betrokkene moet zelf het hokje aankruisen, alleen dan is duidelijk dat de betrokkene daadwerkelijk zijn wil heeft geuit.
- De betrokkene kan zijn toestemming te allen tijde intrekken. Dit moet in dezelfde vorm mogelijk zijn als hoe de toestemming gegeven wordt. Bijvoorbeeld: wanneer de toestemming wordt gegeven door het aanvinken van een hokje, moet het intrekken van deze toestemming net zo gemakkelijk gaan door het uitvinken van dit hokje.

De bewijslast voor het verkregen hebben van de toestemming en voor de kennisname door betrokkene van de verstrekte informatie ligt bij u als verwerkingsverantwoordelijke. U moet dus kunnen aantonen dat er bij de betrokkene geen twijfel heeft kunnen bestaan over de doelen van de verwerking en het verlenen van de toestemming. Het is daarom van belang dat uw 'opt-in flow' voldoende duidelijk is. Documenteer ook deze 'opt-in flow' goed, zodat u kunt aantonen hoe de toestemming is verkregen. Hierbij is ook versiebeheer van belang: als de toestemming voor uw 1.0 app anders is dan de toestemming voor uw 2.0 app (u verwerkt bijvoorbeeld gegevens voor nieuwe doelen), leg dan vast wat de verschillen tussen de verschillende versies zijn.

Houd er tenslotte rekening mee dat de betrokkene zijn toestemming weer kan intrekken. Het gevolg hiervan is dat u als verwerkingsverantwoordelijke dan géén grondslag meer heeft om de persoonsgegevens van deze betrokkene te verwerken. Concreet betekent dit dat u niet langer de persoonsgegevens van deze betrokkene mag gebruiken voor het doel waarvoor u ze verkregen heeft, tenzij er een andere grondslag is waarop u de verwerking kunt baseren (u heeft bijvoorbeeld een wettelijke plicht om de gegevens voor de Belastingdienst beschikbaar te houden).

11.7a Telecommunicatiewet: Toestemming voor cookies en soortgelijke technieken

Indien u cookies of soortgelijke technieken gebruikt binnen uw toepassing, dan moet u in een aantal gevallen ook toestemming vragen. Let er goed op dat deze toestemming specifiek voor het plaatsen van de cookies is (en het uitlezen daarvan). Deze toestemming komt bovenop de wettelijke grondslag voor het verwerken van persoonsgegevens. U vraagt dus toestemming voor het plaatsen van de cookies, maar vervolgens moet u voor de gegevens die u met behulp van deze cookie verzamelt, ook een gerechtvaardigd doel hebben (bijvoorbeeld wederom toestemming).

Voor de toestemming op grond van de Cookiewet gelden dezelfde eisen zoals hierboven reeds opgesomd.
Voor wat betreft het plaatsen van cookies of soortgelijke technieken bestaan drie uitzonderingen op de toestemmingplicht. In de volgende drie gevallen hoeft niet aan de eis van toestemming te worden voldaan:

- Technisch noodzakelijke cookies, bijvoorbeeld load balancing cookies.
- Functionele cookies: deze cookies zijn nodig omdat de gevraagde dienst zonder het gebruik van deze cookies niet of minder goed functioneert. Bijvoorbeeld afrekenen bij een webshop, taalinstellingen en valuta-instellingen.
- Cookies om de effectiviteit en kwaliteit van een dienst te meten.[3] Bijvoorbeeld:
  - analytische cookies die gebruik van de app analyseren en in kaart brengen, zodat kwaliteit en/of effectiviteit kan worden verbeterd;
  - affiliate cookies: om bij te houden welke advertentie leidt tot aankoop van een bepaald product, zodat degene die deze advertentie heeft getoond (de affiliate) daarvoor een bepaalde beloning kan ontvangen van de adverteerder.

[3] Nota bene: deze uitzondering geldt alleen indien de cookie geen of slechts geringe gevolgen voor de persoonlijke levenssfeer van de betrokkene heeft. Meer dan geringe gevolgen zijn bijvoorbeeld het (onbedoeld) doorsturen van de gegevens aan derden.

6b AVG: Noodzakelijk voor de uitvoering van de overeenkomst

Wanneer de gegevens noodzakelijk zijn voor het uitvoeren van de overeenkomst met de betrokkene, mogen zij worden verwerkt. Denk bijvoorbeeld aan het verwerken van NAW-gegevens en een rekeningnummer zodat vergoedingen voor bijvoorbeeld spitsmijden kunnen worden gestort.

6f AVG: Noodzakelijk voor de behartiging van uw gerechtvaardigd belang

Als u het gebruik van de toepassing baseert op deze grondslag, dient u een uitdrukkelijke afweging te maken tussen uw gerechtvaardigd belang en het privacybelang van de betrokkene. Bij deze afweging spelen de volgende aspecten een rol:

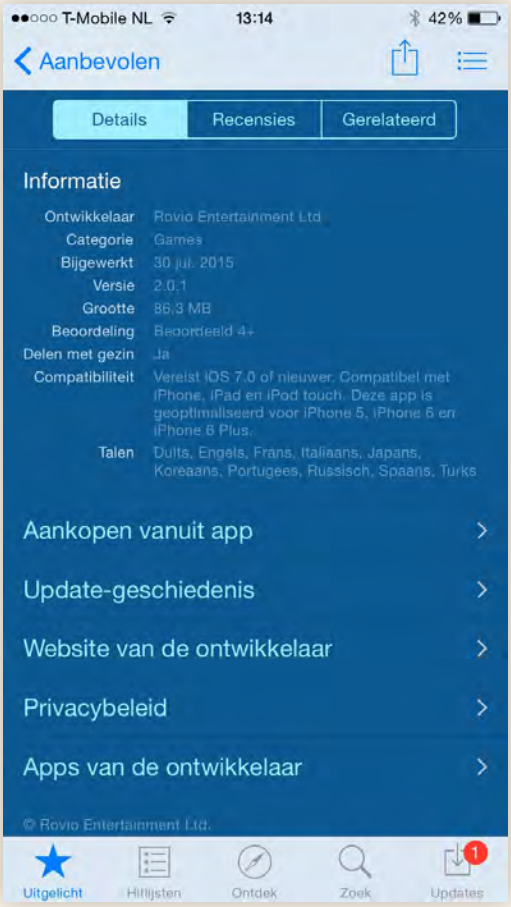
- de aard van uw gerechtvaardigd belang;
- de gevoeligheid van de gegevens;
- de impact voor de betrokkene en zijn redelijke verwachting met betrekking tot wat met zijn gegevens zal gebeuren, alsook de aard van de gegevens en hoe deze worden verwerkt;
- aanvullende waarborgen die de impact voor de betrokkene kunnen minimaliseren, zoals dataminimalisatie en privacy-enhancing technologies.

Geo-locatiegegevens worden bijvoorbeeld als gevoelige gegevens beschouwd, omdat ze een indringend beeld van de gewoonten en patronen van de betrokkene geven. Wanneer u deze gegevens voor andere doelen gebruikt dan het uitvoeren van de overeengekomen mobiliteits-diensten, dan zal de afweging over het algemeen doorslaan in het voordeel van de betrokkene. Wilt u de geo-locatiegegevens bijvoorbeeld gebruiken voor marketing of analyses, dan ligt de ondubbelzinnige toestemming dus meer voor de hand.
Ook dient de verwerking noodzakelijk te zijn ter behartiging van uw belang. Dit houdt in dat uw belangen niet op een andere manier, met minder ingrijpende middelen of met minder gegevens, kunnen worden gediend (subsidiariteit).

Wanneer heeft u een gerechtvaardigd belang?

Als u uw activiteiten niet goed kunt uitoefenen zonder het verwerken van persoonsgegevens, dan heeft u een gerechtvaardigd belang. Een voorbeeld van gerechtvaardigd belang is het voeren van een goede bedrijfsvoering. Het gerechtvaardigd belang is niet alleen beperkt tot uw kernactiviteiten maar kan ook betrekking hebben op activiteiten die daarmee nauw verbonden zijn. Wel moet u uw belang kunnen rechtvaardigen naar de individuele betrokkene toe.

8.4 Voorbeelden



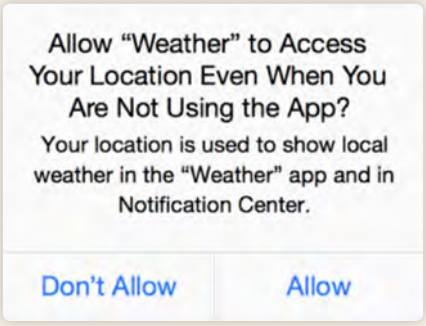
Voorbeeld 1 (toestemming)

Hiernaast ziet u een screenshot van de App Store. Voor het downloaden van de applicatie (Angry Birds 2) kan het privacybeleid van Rovio worden ingezien. Hoewel hiermee invulling wordt gegeven aan het informatie-vereiste, mag uit het downloaden van de applicatie géén ondubbelzinnige toestemming voor het verwerken van de persoonsgegevens worden afgeleid.

Voorbeeld 2 (toestemming)

Een goed voorbeeld van een app die netjes en duidelijk toestemming vraagt na installatie van de app (maar voor de verwerking van persoonsgegevens) is de TomTom App.

De app vraagt duidelijk toestemming na installatie van de app alvorens het gegevens gaat verwerken. Het stelt ten eerste de exacte gegevens die verzameld worden (locatie), waarvoor deze verzameld worden (het doel van de gegevensverzameling), vraagt vervolgens om toestemming van de gebruiker en geeft daarbij duidelijk aan waar meer informatie gevonden kan worden.



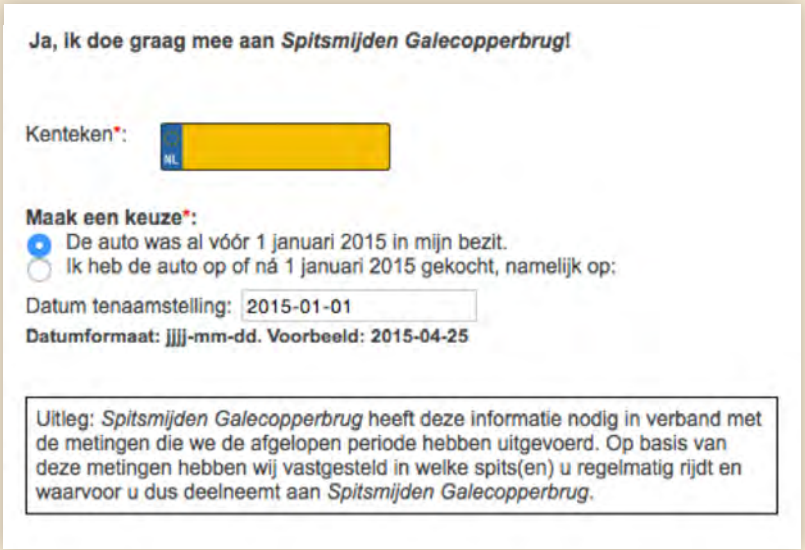
Voorbeeld 3 (toestemming)

Voorbeeld van een opt-in via de ingebouwde permissies in iOS. Deze weer-app vraagt voor het gebruik en de verwerking van de gegevens of de gebruiker instemt met het verwerken van zijn locatiegegevens. Deze toestemming is voldoende afgebakend en concreet.

Voorbeeld 4 (doelomschrijving)

Een goed voorbeeld van een voldoende duidelijk omschreven doel voor verwerking was te vinden bij de aanmelding op de web-site voor het spitsmijdenproject Spitsmijden Galecopperbrug.

Bij aanmelding werd kort uitgelegd voor welk doel de gevraagde informatie in het aanmeldingsformulier nodig was.



Voorbeeld 5 (doelomschrijving)

Een ander voorbeeld is de MyOV-app, die voor aanmelding bij de app nogmaals herhaalt wat de doeleinden zijn van de gegevensverwerking.

Voorbeeld 6 (toestemming voor nulmeting)
Een voorbeeld van een juiste toestemming als grondslag voor nulmeting is:

'Ik ga akkoord met het verzamelen van mijn gegevens bestaande uit X,Y, Z met als doel het doen van metingen op basis waarvan ik mogelijk word geselecteerd voor een spitsmijden-project.'

Deze opt-in staat overigens los van alle andere mogelijk noodzakelijke toestemmingen (voor eventuele andere doelen van de app of toepassing). Idealiter zou deze ook los gevraagd moeten worden en niet mee moeten worden genomen in alle andere toestemmingen.

9 Dataminimalisatie

Persoonsgegevens mogen uitsluitend worden verwerkt wanneer deze strikt noodzakelijk zijn voor het doel van de verwerking. Dit is de kern van de eis voor dataminimalisatie. Ook het anoniem of onder pseudoniem verwerken van persoonsgegevens komt aan de orde. De AVG is niet van toepassing op volledig geanonimiseerde gegevens. Ter verduidelijking geven we twee praktijkvoorbeelden van dataminimalisatie.

9.1 Eis

Voor de toepassing mogen (zonder toestemming van de betrokkene) niet meer gegevens worden gebruikt dan noodzakelijk is om de doelen van de toepassing te bereiken.

9.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepaling:

- Artikel 5 lid 1 sub c AVG

9.3 Toelichting

Gegevens mogen op grond van de wet alleen verwerkt worden als zij voor het te bereiken doel (zie eis legitiem doel en grondslag) noodzakelijk zijn. Gegevens die niet strikt noodzakelijk zijn voor het doel van de verwerking, mogen niet worden verwerkt.

Nota bene: zorg er tegelijkertijd voor dat er ook niet te weinig gegevens worden verzameld (de gegevens moeten toereikend zijn)!

Anonimisering en pseudonimisering
In het kader van dataminimalisatie zijn naast het niet verzamelen van persoonsgegevens ook de concepten anonimisering en pseudonimisering relevant.

Anonimiseren
Anonieme gegevens zijn gegevens waarvan de persoon niet geïdentificeerd kan worden door u of een derde, rekening houdend met alle aannemelijke technieken die gebruikt kunnen worden om iemand te identificeren.
Er bestaan meerdere technieken voor anonimisering, de AVG schrijft echter geen specifieke techniek voor. De optimale keuze dient per casus te worden bepaald.

Bij volledige anonimisering wordt voldaan aan de volgende drie criteria:
1. het is niet meer mogelijk een individu uit een dataset te halen;
2. het is niet meer mogelijk om de gegevens te linken aan een individu;
3. er kan geen informatie over een individu worden afgeleid.

De AVG is niet van toepassing op anonieme gegevens (omdat het geen persoonsgegevens zijn).

Pseudonimiseren
Pseudonimisering is het vervangen van direct identificerende kenmerken (naam, voornaam etc.) door een niet-identificerend gegeven (X,Y,Z of 1,2,3 etc.)
Dit maakt het mogelijk extra gegevens te verwerken met betrekking tot betrokkene, zonder dat zijn identiteit bekend is. Hierdoor is de mogelijkheid om de dataset te linken aan het individu gereduceerd. Het verschil met anonimisering is, dat het voor u als verwerkingsverantwoordelijke mogelijk is om het proces weer om te draaien (de verwerkingsverantwoordelijke heeft de 'sleutel'). Pseudonimisering is dus niet een manier om dataminimalisatie te bewerkstelligen.

9.4 Voorbeelden

Om het verkeer in kaart te brengen op een bepaalde route, is het alleen noodzakelijk om de locatiegegevens van de voertuigen te registreren. Het is bijvoorbeeld niet noodzakelijk om ook kenteken, naam, adres en woonplaats van de betrokkene te registreren. Tenzij het de bedoeling is dat deze persoon op basis van zijn locatiegegevens in aanmerking kan komen voor een uitnodiging voor een spitsmijdenprogramma.

Voorbeeld 1

De MyOV-app verwerkt persoonsgegevens om persoonlijke reisadviezen te geven. Echter, MyOV gebruikt ook reisgegevens om inzicht te krijgen in reisbewegingen. Aangezien het voor dit doel niet nodig is om gegevens te hebben die te herleiden zijn naar een persoon, heeft MyOV-app deze geanonimiseerd. Op deze manier wordt het principe van dataminimalisatie geborgd.

Waarom heeft MyOV mijn reisgegevens nodig?
Wij analyseren uw reisgedrag zodat we u persoonlijke reisadviezen kunnen geven. Het gaat primair om mogelijkheden om de spits te mijden. Als er over uw route relevante informatie beschikbaar is (bijvoorbeeld informatie over bezetting, storingen of het weer), dan kunnen wij deze informatie ook meenemen en uw persoonlijke reisadvies daarop afstemmen. Hiermee kunnen we u dan een comfortabeler of sneller alternatief voorstellen.

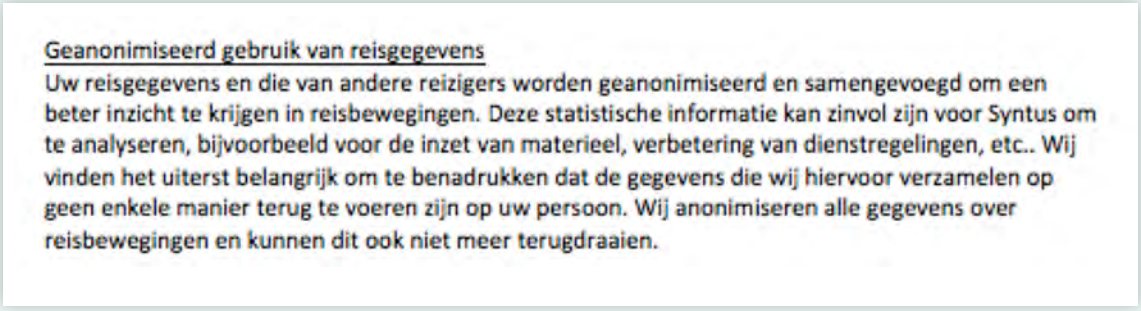
Uw reisgegevens zijn ook nodig om uw restitutieaanvragen bij een vergeten check out of geld terug bij vertraging te kunnen verwerken.

Geanonimiseerd gebruik van reisgegevens
Uw reisgegevens en die van andere reizigers worden geanonimiseerd en samengevoegd gebruikt om een beter inzicht te krijgen in reisbewegingen. Deze statistische informatie kan zinvol zijn voor vervoerders om bijvoorbeeld inzet van materieel, dienstregelingen, plaats van check-in/out palen et cetera te verbeteren.

Wij vinden het heel belangrijk om te benadrukken dat de gegevens die wij hiervoor verzamelen op geen enkele manier terug te voeren zijn op uw persoon. Wij anonimiseren alle gegevens over reisbewegingen en kunnen dit ook niet meer terugdraaien.

Voorbeeld 2

De Syntus-app verwerkt persoonsgegevens om persoonlijke reisadviezen te geven en de reiziger aanbiedingen te doen. Echter, Syntus (inmiddels Keolis genaamd) gebruikt deze reisgegevens ook om inzicht te krijgen in reisbewegingen. Aangezien het voor dit doel niet nodig is om gegevens te hebben die te herleiden zijn naar een persoon, heeft de Syntus-app deze geanonimiseerd. Op deze manier wordt het principe van dataminimalisatie geborgd.



Geanonimiseerd gebruik van reisgegevens

Uw reisgegevens en die van andere reizigers worden geanonimiseerd en samengevoegd om een beter inzicht te krijgen in reisbewegingen. Deze statistische informatie kan zinvol zijn voor Syntus om te analyseren, bijvoorbeeld voor de inzet van materieel, verbetering van dienstregelingen, etc.. Wij vinden het uiterst belangrijk om te benadrukken dat de gegevens die wij hiervoor verzamelen op geen enkele manier terug te voeren zijn op uw persoon. Wij anonimiseren alle gegevens over reisbewegingen en kunnen dit ook niet meer terugdraaien.

10 Privacy by design and by default

Een van de nieuwe bepalingen uit de AVG is het vereiste van privacy by design. Dit houdt in dat al vanaf het ontwerp van IT-systemen en bedrijfsprocessen rekening gehouden moet worden met privacybescherming. Daarnaast vereist het principe van privacy by default dat standaard de meest privacyvriendelijke instellingen moeten worden gepresenteerd aan betrokkenen.

10.1 Eis

- ***Vanaf het ontwerp van IT-systemen en bedrijfsprocessen wordt rekening gehouden met privacybescherming (privacy by design).***

- ***Standaard worden de meest privacyvriendelijke instellingen gepresenteerd aan betrokkene (privacy by default).***

10.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepaling:

- Artikel 25 AVG

10.3 Toelichting

Bij het ontwerp van nieuwe (IT-)systemen en bedrijfsprocessen moet rekening worden gehouden met privacy en gegevensbescherming. Dit principe wordt privacy by design genoemd. Door al bij het ontwerp na te denken wat voor privacy-implicaties het nieuwe proces of systeem met zich meebrengt, kunt u bij de keuzes voor het ontwerp hiermee rekening houden. Bij de ontwikkeling van een nieuw systeem of proces is het uitgangspunt dat de standaard is dat de privacy van de betrokkene het beste wordt gewaarborgd (privacy by default). Hierdoor wordt aan de betrokkene de keuze gelaten om eventuele extra gegevens te delen.

10.4 Voorbeelden

Voorbeeld 1

Smoelenboek BV richt een platform op waarop haar gebruikers foto's en berichtjes met elkaar kunnen delen. Bij het aanmaken van een profiel door een nieuwe gebruiker is het opgeven van de eigen naam en het e-mailadres verplicht. De gebruiker beslist zelf of hij ook zijn profielfoto wil uploaden en zijn woonplaats wil doorgeven. Met deze werkwijze borgt Smoelenboek BV dat alleen de noodzakelijke gegevens voor het gebruik van het platform verplicht worden ingevuld bij het aanmaken van een profiel. Het is dan aan de gebruiker om te beslissen of hij meer gegevens wil delen met het platform, zoals zijn foto en woonplaats.

Voorbeeld 2

Mobility BV is een organisatie die opkomt voor de belangen van weggebruikers en heeft ook een app met een filemeldingservice ontwikkeld. Piet reist voor zijn werk vaak naar Utrecht via de A12 en staat hier regelmatig in de file. Via een collega hoort hij over de tijdige en accurate filemeldingen van Mobility BV. Daarom besluit Piet deze app te downloaden. Na het downloaden van de app wordt Piet gevraagd naar zijn naam en op welke wegen hij vaak rijdt. Op basis van deze opgegeven informatie ontvangt Piet nu dagelijks een pushmelding: 'Hallo Piet, momenteel staat er een file op de A12 met een vertraging van ongeveer 10 minuten.' Aanvullend kan Piet ervoor kiezen om zijn locatiegegevens met de app te delen, waardoor hij ook realtime filemeldingen kan krijgen van wegen waarop hij op dat moment rijdt. Piet kan er dus zelf voor kiezen om meer gegevens met de app te delen, als hij gebruik wil maken van deze extra service van Mobility BV.

11 Data protection impact assessment

Met een data protection impact assessment (DPIA) beoordeelt u de beoogde effecten van de beoogde gegevensverwerking. Deze beoordeling is verplicht wanneer sprake is van een verwerking van persoonsgegevens met een hoog risico voor de rechten en vrijheden van personen, bijvoorbeeld bij stelselmatige en grootschalige monitoring van openbare ruimten. In dit hoofdstuk leest u wanneer u zo'n DPIA moet doen en waaruit deze in ieder geval moet bestaan.

11.1 Eis

Het uitvoeren van een data protection impact assessment (DPIA) is verplicht voor toepassingen waarvan vermoed wordt dat ze een hoog risico voor de privacy-rechten en vrijheden van betrokkenen met zich mee te brengen.

11.2 Wettelijke bepaling

Deze eis is gebaseerd op de volgende wettelijke bepaling:

- Artikel 35 AVG

11.3 Toelichting

Het uitvoeren van een data protection impact assessment (DPIA) is verplicht, als gelet op de aard, de omvang, de context en de doeleinden van de verwerking, sprake is van een hoog risico voor de rechten en vrijheden van natuurlijke personen. Dit is onder meer het geval bij:

- 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 hen op vergelijkbare wijze wezenlijk kunnen treffen;
- grootschalige verwerking van bijzondere categorieën van gegevens[4] of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten;
- stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

[4] Bijzondere categorieën van persoonsgegevens zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Ook voor verwerkingen waarvoor een DPIA niet verplicht is, kan het verstandig zijn om toch een DPIA uit te (laten) voeren om inzicht te krijgen in de risico's van een nieuwe toepassing. Op basis van de uitkomsten van de DPIA kunt u de nodige maatregelen nemen.
Een DPIA moet in ieder geval de volgende informatie bevatten:

- een systematische beschrijving van de beoogde verwerkingen en verwerkingsdoeleinden;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
- de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheids-maatregelen en mechanismen om de bescherming van persoonsgegevens te waarborgen en om aan te tonen dat aan de AVG is voldaan.

De Europese privacy-toezichthouders hebben richtsnoeren[5] opgesteld waarin meer uitleg wordt gegeven over wanneer een DPIA verplicht is en hoe u deze moet uitvoeren.

[5] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking 'waarschijnlijk een hoog risico inhoudt' in de zin van Verordening 2016/679. (https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf)

11.4 Voorbeelden

Voorbeeld 1

In het kader van voorgenomen renovatiewerkzaamheden op de A4 wil Rijkswaterstaat als wegbeheerder met behulp van een kentekenregistratiesysteem het rijgedrag op de snelweg A4 meten. Op basis van deze nulmeting kan de wegbeheerder de kentekenhouders aanschrijven, die regelmatig tijdens de spits op de A4 rijden, met de vraag of zij mee willen doen aan een spitsmijdenproject. Omdat sprake is van stelselmatige monitoring van een openbare ruimte, is Rijkswaterstaat verplicht een DPIA uit te voeren voordat hij het kentekenregistratiesysteem voor dit doel kan gebruiken.

Voorbeeld 2

Autobaan BV wil klanten een korting gaan geven op de premie van hun autoverzekering op basis van goed rijgedrag. Met behulp van een stick in de auto krijgt Autobaan BV inzicht in het rijgedrag door te meten hoe snel de verzekerde optrekt en afremt en hoe scherp hij door de bochten gaat. Als de klant goed rijgedrag vertoont, krijgt hij 10% korting op zijn maandelijkse premie voor de autoverzekering. Aangezien hier sprake is van systematische beoordeling van het rijgedrag van de klant, is Autobaan BV verplicht een DPIA uit te voeren voordat deze autoverzekering aan klanten kan worden aangeboden.

12 Doelbinding

U mag in principe alleen persoonsgegevens verwerken voor het doel waarvoor deze zijn verzameld. Verdere verwerking is uitsluitend toegestaan, wanneer het nieuwe doel verenigbaar is met het oorspronkelijke doel. Dit wordt afgewogen aan de hand van verschillende factoren, zoals de gevoeligheid van de persoongegevens en de gevolgen van verdere verwerking voor de gebruiker. In dit hoofdstuk komen vijf factoren voor een goede beoordeling aan de orde.

12.1 Eis

Gegevens mogen alleen verwerkt worden voor het doel waarvoor ze verzameld zijn, tenzij het nieuwe doel verenigbaar is met het oorspronkelijk doel.

12.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepaling:

- Artikel 5 lid 1 sub b en c AVG

12.3 Toelichting

De beoogde verwerking dient een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel te hebben. Hierbij is het van belang dat de noodzakelijkheid van de verwerking van persoonsgegevens wordt beoordeeld. Dit houdt in dat u zich moet afvragen of het doel ook bereikt kan worden met minder gegevens of op een andere manier, waarbij minder persoonsgegevens worden verwerkt.

Ook mogen de gegevens niet verder worden verwerkt op een wijze die onverenigbaar is met het oorspronkelijke doel.

Om te beoordelen of de verdere verwerking is toegestaan, moet u alle relevante omstandigheden van het geval meewegen. Met name moet rekening gehouden worden met de volgende belangrijke factoren:

- De mate van verwantschap tussen het oorspronkelijke doel en het doel van de verdere verwerking. Hoe dichter de twee doeleinden bij elkaar liggen (oftewel hoe meer verwant ze zijn), hoe eerder de verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens zijn verzameld.
- De context waarin de persoonsgegevens zijn verzameld en de redelijke verwachting van de betrokkene over het verdere gebruik van zijn gegevens.

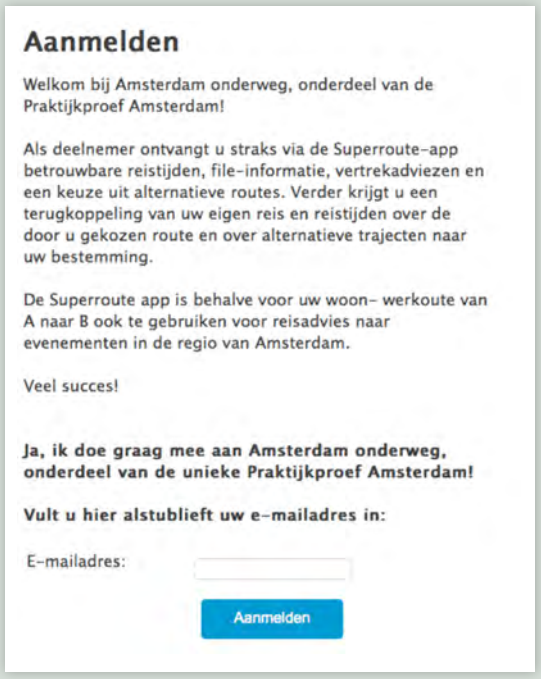
- De aard van de persoonsgegevens. Hoe gevoeliger de gegevens voor de betrokkene zijn, hoe minder snel u mag aannemen dat deze persoonsgegevens ook voor andere doeleinden mogen worden gebruikt. Met gevoelige gegevens worden niet specifiek de bijzondere persoonsgegevens bedoeld, maar ook gegevens die over het algemeen als gevoelig worden ervaren, zoals geo-locatiegegevens.
- De gevolgen van de verdere verwerking op de betrokkene. Met name als de verdere verwerking tot gevolg heeft dat een bepaalde beslissing over de betrokkene wordt genomen, is die verwerking al snel onverenigbaar.
- De waarborgen die zijn gerealiseerd door de verwerkingsverantwoordelijke om te borgen dat de persoonsgegevens op een behoorlijke en zorgvuldige wijze worden verwerkt en die onnodige impact op de betrokkene voorkomen.

U moet alle factoren meenemen bij uw beoordeling. De ene factor weegt niet per definitie zwaarder dan een andere.

12.4 Voorbeelden

Voorbeeld 1

Een supermarkt introduceert een gepersonaliseerde loyaltykaart voor haar klanten. Klanten krijgen met de loyaltykaart korting op hun boodschappen. In ruil daarvoor registreert de supermarkt alle aankopen van de klant op naam en doet op basis daarvan gerichte aanbiedingen. Klanten geven toestemming voor dit doel. Vervolgens besluit de supermarkt de gegevens ook te verkopen aan een verzekeringsmaatschappij. Dit doel is niet verenigbaar met het oorspronkelijke doel waarvoor de gegevens zijn verzameld.



Voorbeeld 2

Bij aanmelding bij Amsterdam onderweg komt het onderstaande scherm in beeld. Als later een wachtwoord moet worden opgegeven, wordt gevraagd om de privacy policy goed te keuren. Hierin staat vermeld dat de verantwoordelijke, RWS, alleen de gegevens van gebruikers mag verwerken om zogenaamde 'mystery users' te werven. Hij mag dus deze gegevens niet gebruiken voor andere doelen, bijvoorbeeld marketing-doeleinden.

4. Verzamelen, beheren en verwerken van persoonsgegevens

Het verzamelen, beheren en verwerken van persoonsgegevens verloopt conform de Wet bescherming persoonsgegevens. De smartphone-app registreert de route die een deelnemer heeft gereden. De exacte vertreklocatie is niet traceerbaar. Deelnemers kunnen hun eigen ritregistraties nazien op hun persoonlijke pagina (zie 9). Geaggregeerde, geanonimiseerde analyses van de projectresultaten worden gedeeld met de opdrachtgever en verantwoordelijke: RWS. Deze heeft geen inzage in de persoonsgegevens die horen bij het reisgedrag van de deelnemer aan PPA. RWS heeft slechts inzage in persoonsgegevens van deelnemers (te weten: naam, adres, woonplaats, telefoonnummer) ten behoeve van het werven van zogenaamde 'mystery users'. De genoemde gegevens mogen alleen voor dit doel worden gebruikt en alleen na expliciete toestemming van de deelnemer. Daarnaast worden individuele reisgedraggegevens die worden gekoppeld aan enquêteresultaten, gedeeld met het Ministerie van Infrastructuur en Milieu (Directoraat-Generaal Mobiliteit). Dit om de effecten van de mobiliteitsprojecten in Nederland te kunnen analyseren en onderling te vergelijken. Ook deze gegevensstroom is geanonimiseerd en bevat geen persoonsgegevens.

De verwerking is beperkt tot die gegevens die relevant zijn voor het verwerkingsdoel.

13 Informatie en transparantie

De AVG en de Telecommunicatiewet bepalen dat een gebruiker moet weten welke persoonsgegevens u verwerkt over hem en voor welk doel dat gebeurt. Gebruikers hebben recht op volledige informatie. In dit hoofdstuk staat puntsgewijs over welke zaken u gebruikers precies moet informeren en hoe u dat goed vormgeeft. Zo moet u bijvoorbeeld gemakkelijk leesbare informatie op een zichtbare plaats presenteren. Ook de transparantie-eisen voor cookies en soortgelijke technieken passeren de revue.

13.1 Eis

Het moet voor de betrokkene helder zijn welke persoonsgegevens worden verwerkt en voor welke doeleinden ze worden gebruikt.

13.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 13 AVG
- Artikel 14 AVG
- Artikel 11.7a Telecommunicatiewet

13.3 Toelichting

De betrokkene moet vooraf volledig worden geïnformeerd over wat u met de persoonsgegevens doet die u verzamelt. Dit houdt in dat zij moeten worden ingelicht over het doel van de verwerking en hun rechten voordat hun persoonsgegevens worden verwerkt.

Betrokkenen moeten worden geïnformeerd over de volgende zaken:

- wie de verwerkingsverantwoordelijke is;
- wat de doelen van de toepassing zijn;
- welke persoonsgegevens worden verwerkt;
- waarvoor de persoonsgegevens worden gebruikt;
- derden aan wie u persoonsgegevens verstrekt;
- hoe lang de persoonsgegevens worden bewaard;
- hoe de betrokkene zijn rechten kan uitoefenen (zie hoofdstuk 15).

Verder gelden de volgende eisen:

- De informatie moet altijd op een (direct) zichtbare plek getoond worden. Voorbeelden zijn een duidelijk vindbare link op een website of app, of een speciaal scherm dat tijdens het installeren wordt getoond.
- U moet informeren in een taal die bij de doelgroep aansluit. Zorg in ieder geval dat teksten zo veel mogelijk op het niveau B1 Nederlands zijn en voorkom ingewikkelde juridische teksten.

- Informeren door middel van een globale verwijzing naar algemene voorwaarden, privacy- en/of permission-statements is onvoldoende.
- Zorg dat de informatie goed gestructureerd is, zodat de gebruiker makkelijk zijn weg kan vinden door de informatie. Een goed voorbeeld is een gelaagd privacystatement. Houd ook rekening met het type apparaat. Zo is een link naar een privacystatement op een website vaak niet goed leesbaar op het kleinere scherm van een smartphone.

Afzonderlijk regime voor cookies en soortgelijke technieken

Wanneer u cookies of soortgelijke technieken gebruikt binnen uw toepassing, dient u de betrokkenen voor het plaatsen van de cookie via een privacy- of cookie policy te informeren over de volgende aspecten:

- welke cookies er worden geplaatst;
- de soorten persoonsgegevens die via de cookies worden verzameld en verwerkt;
- de doeleinden van de gegevensverwerking;
- derden aan wie u de persoonsgegevens verstrekt;
- de levensduur van de cookie.[6]

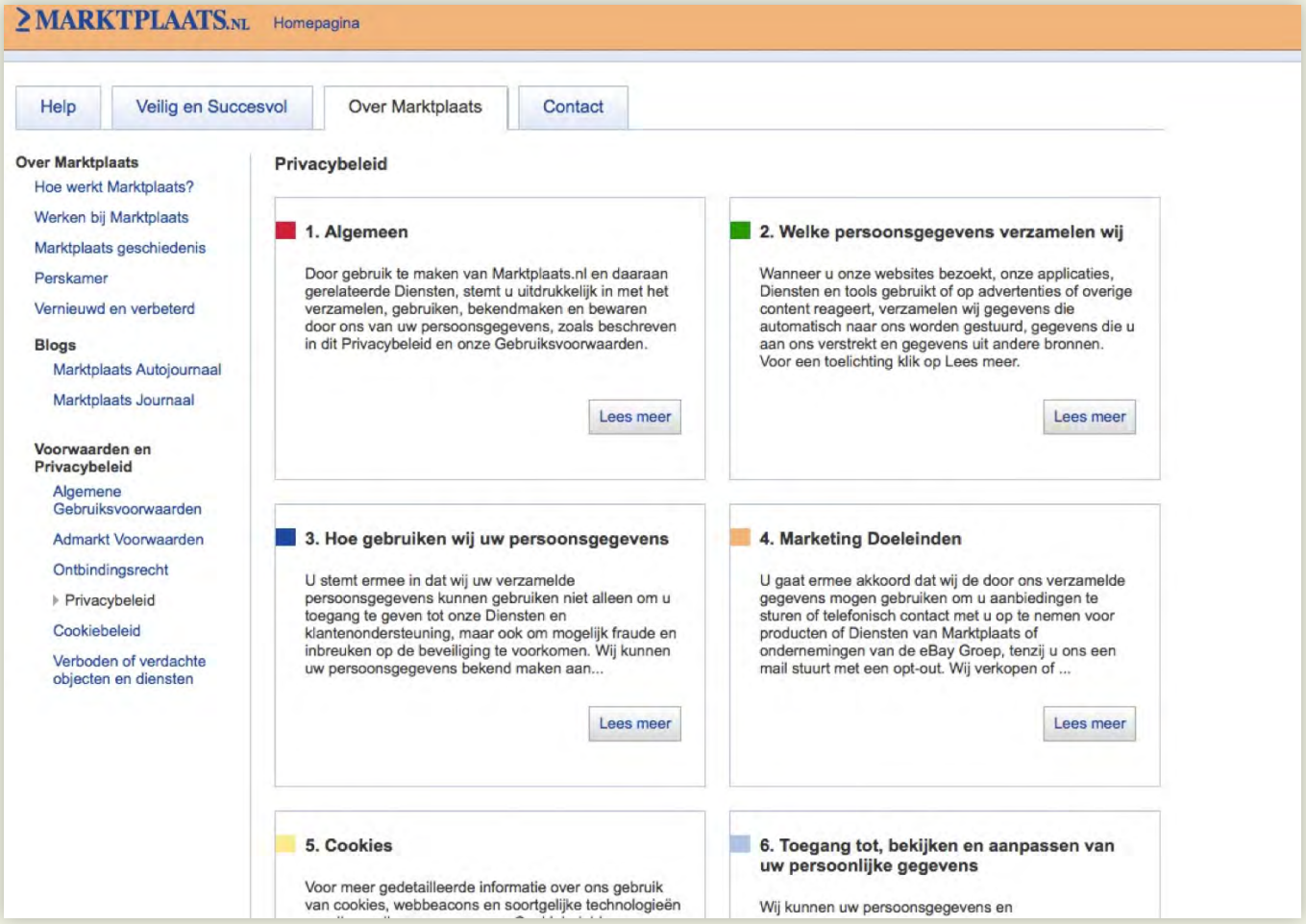
Voor wat betreft het plaatsen van cookies of soortgelijke technieken bestaan drie uitzonderingen op de informatieplicht. Over het gebruik van strikt noodzakelijke technische cookies, functionele cookies waar de gebruiker om gevraagd heeft en analyse cookies met een geringe invloed op de privacy hoeft niet geïnformeerd te worden. Zo is het ook niet nodig om de betrokkene om toestemming te vragen voor deze cookies.

[6] Voor meer informatie zie: https://www.acm.nl/nl/onderwerpen/telecommunicatie/internet/cookies/

13.4 Voorbeelden

Voorbeeld van een gelaagd privacystatement

De blokjes geven op hoofdlijnen weer wat er gebeurt met de gegevens, onder ‘lees meer’ is uitgebreide informatie te vinden.

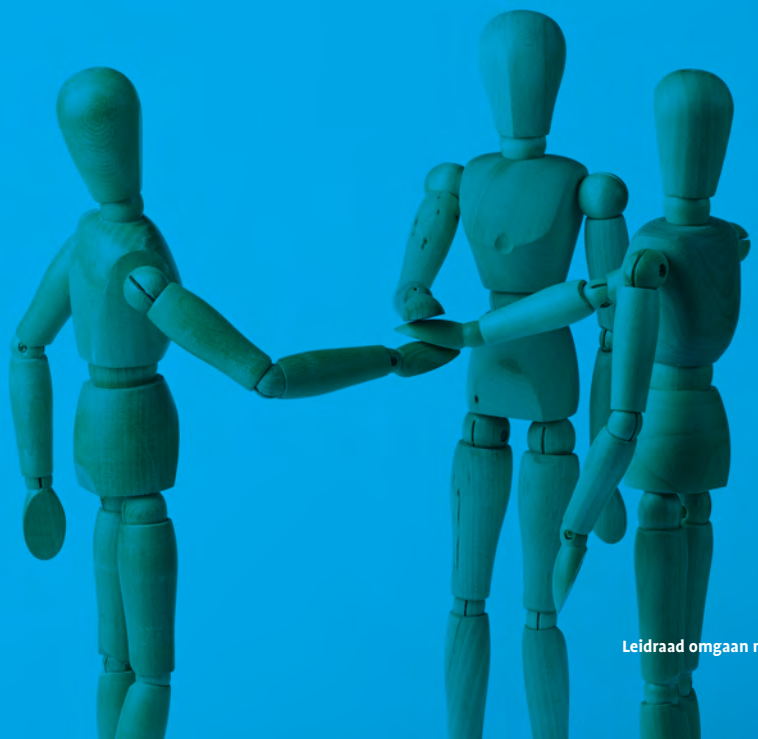


Voorbeeld cookiemelding

De NPO geeft duidelijk de doelen van het cookiegebruik aan en biedt de mogelijkheid om advertentiecookies te weigeren.

14 Delen van persoonsgegevens met derden

Voor het delen van persoonsgegevens met derden is een wettelijke grondslag nodig. Zo kan artikel 6c van de AVG als grondslag gelden als u wettelijk verplicht bent om bepaalde persoonsgegevens te delen. Maar in de meeste gevallen zal toestemming van de gebruiker nodig zijn voor het mogen delen van zijn persoonsgegevens met derden.



14.1 Eis

Persoonsgegevens worden alleen gedeeld met derden als daar een rechtmatige grondslag voor is.

14.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepaling:

- Artikel 6 AVG

14.3 Toelichting

Omdat het delen van persoonsgegevens met derden een verwerking is, is ook hiervoor een grondslag nodig. Wanneer het delen noodzakelijk voortvloeit uit het uitvoeren van de overeenkomst, kan gebruik worden gemaakt van artikel 6 lid 1 sub b AVG. Wanneer er een wettelijke plicht rust op de verwerkingsverantwoordelijke, dan kan artikel 6 lid 1 sub c AVG als grondslag dienen. Maar in de meeste gevallen zal voor verstrekking van persoonsgegevens aan derden toestemming nodig zijn van de betrokkene (artikel 6 lid 1 sub a AVG).

Nota bene: Houd er rekening mee dat wanneer bij de ontwikkeling van apps gebruik wordt gemaakt van componenten van derden (bijvoorbeeld software development kits) of API's van derden, dat er ook persoonsgegevens doorgestuurd kunnen worden naar deze derden. Zorg dat u afspraken maakt met uw appbouwer over het gebruik van dit soort componenten en controleer welke (persoons)gegevens worden uitgewisseld via plug-ins en API's.

14.4 Voorbeelden

Voorbeeld 1

Wanneer een gebruiker een sociaal platform in een app van een partij gebruikt, worden allerlei (persoons)gegevens gedeeld tussen de partij van die app en het sociale platform. De gebruiker moet hiervoor zijn toestemming geven.

Voorbeeld 2

De Syntus-app heeft duidelijk in zijn privacybeleid aangegeven dat persoonsgegevens in principe niet aan derden worden doorgegeven. Wanneer gegevens wel aan derden worden gegeven, zorgt Syntus ervoor dat dit op een rechtmatige grondslag is gebaseerd: ofwel expliciete toestemming van de gebruiker (artikel 6 lid 1 sub a AVG), ofwel het voldoen aan een wettelijk voorschrift (artikel 6 lid 1 sub c AVG).

Doorgifte aan derden
Syntus geeft uw persoonsgegevens niet door aan derden, tenzij een wettelijk voorschrift dat vereist of er expliciet toestemming aan u hiervoor gevraagd is.

15 Rechten van betrokkene

Als persoonsgegevens van een gebruiker worden verwerkt, heeft hij recht op inzage, recht op rectificatie, recht op gegevenswissing en in sommige gevallen recht op beperking van de verwerking. Op basis van deze rechten kan hij zich verweren tegen onjuiste of incomplete gegevensverwerking. In dit hoofdstuk beschrijven we hoe u een inzageverzoek en een rectificatieverzoek goed kunt afhandelen en hoe u de overige rechten kunt naleven.

15.1 Eis

In de toepassing wordt rekening gehouden met en invulling gegeven aan de rechten van de betrokkene.

15.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 12 tot en met 23 AVG

15.3 Toelichting

De betrokkene heeft bepaalde rechten met betrekking tot de verwerking van zijn persoonsgegevens. Dit is om te borgen dat de betrokkene weet welke persoonsgegevens over hem verwerkt worden, hij zich kan verweren tegen onjuiste of incomplete persoonsgegevens en ervoor kan zorgen dat persoonsgegevens die niet meer relevant zijn, verwijderd worden. Over de rechten van betrokkenen moet transparant, in begrijpelijke taal, gemakkelijk en in toegankelijke vorm gecommuniceerd worden.

Aan betrokkenen komen op grond van de AVG de volgende rechten toe:

Recht op inzage

De betrokkene heeft het recht op inzage in zijn persoonsgegevens en mag een dergelijk verzoek met redelijke tussenpozen doen. Om de privacy van derden te beschermen is het van belang om de identiteit van de betrokkene goed vast te stellen, zodat geen persoonsgegevens aan de verkeerde persoon ter beschikking worden gesteld. Tenzij het vaststellen van de identiteit van de betrokkene op een minder ingrijpende manier mogelijk is (bijvoorbeeld door middel van vooraf vastgestelde controlevragen), kunt u bij een inzageverzoek om een ID vragen. Geef wel aan dat betrokkene zijn pasfoto, BSN en MRZ (de onderste rij getallen en letters op een paspoort) moet doorstrepen. Deze gevoelige gegevens zijn niet noodzakelijk voor de identificatie.

De beantwoording van het inzageverzoek moet de volgende onderdelen bevatten:

- Een volledig overzicht van de verwerkte persoonsgegevens van de betrokkene.
- Een omschrijving van:
  - de bewaartermijn;
  - de rechten van betrokkene;
  - de geautomatiseerde besluitvorming, nuttige informatie over de onderliggende logica en het belang en de gevolgen voor betrokkene;
  - het doel van de persoonsgegevensverwerking;
  - de categorieën van persoonsgegevens waarop de verwerking betrekking heeft;
  - de ontvangers of categorieën van ontvangers.
- Alle beschikbare informatie over de herkomst van de persoonsgegevens.

De betrokkene heeft ook het recht toegang te krijgen tot mogelijke profielen die gebaseerd zijn op zijn locatie-data.

U moet de persoonsgegevens verstrekken in 'begrijpelijke vorm'. U moet dus kunnen duiden welke persoonsgegevens het betreft en hoe ze worden gebruikt. Wat begrijpelijk is, hangt af van de situatie. Een uitgeprinte lijst met GPS-coördinaten is voor een gebruiker bijvoorbeeld niet goed te interpreteren. Het kan dan helpen om de GPS-coördinaten te plotten op een kaart.

Het is niet uit te sluiten dat inzage in persoonsgegevens ook enig inzicht kan geven in persoonsgegevens over anderen. Op het moment dat u redelijkerwijs kunt verwachten dat een derde bedenkingen zal hebben, moet u deze derde op de hoogte stellen van het verzoek tot inzage.
Wanneer de inzage ook inzicht geeft in persoonsgegevens van derden, zal u ook een belangenafweging moeten maken. U kunt eventueel een inzage weigeren met een beroep op artikel 23 AVG (noodzakelijk in het belang van de bescherming van rechten en vrijheden van anderen).

Recht op rectificatie

De betrokkene heeft recht op rectificatie van zijn onjuiste persoonsgegevens en het recht om onvolledige persoonsgegevens aan te vullen. Als verwerkingsverantwoordelijke bent u verplicht iedere ontvanger aan wie u de persoonsgegevens heeft verstrekt, in kennis te stellen van de rectificatie. Tenzij dit een onmogelijke of onevenredige inspanning vereist.

Recht op het wissen van persoonsgegevens en het recht op vergetelheid

De verwerkingsverantwoordelijke is verplicht persoonsgegevens van betrokkenen te wissen in de volgende situaties:

- De persoonsgegevens zijn niet langer nodig voor de doelen waarvoor ze zijn verzameld.
- De betrokkene trekt zijn toestemming in of maakt bezwaar.
- De persoonsgegevens zijn onrechtmatig verwerkt.
- In een wettelijke verplichting is vastgelegd dat u persoonsgegevens moet wissen.

Wanneer u als verwerkingsverantwoordelijke verplicht bent de persoonsgegevens te wissen, neemt u redelijke maatregelen om derden die deze persoonsgegevens verwerken op de hoogte te stellen van een verzoek om iedere koppeling, kopie en reproductie van de persoonsgegevens te wissen.

Recht op beperking van de verwerking

Persoonsgegevens mogen (tijdelijk) beperkt of niet verwerkt worden, wanneer bijvoorbeeld de juistheid van de persoonsgegevens wordt betwist of wanneer u de gegevens niet meer nodig heeft, maar de betrokkene wel. Hierdoor kunt u zijn persoonsgegevens nog niet laten wissen.

U moet dan aan derden (bijvoorbeeld ontvangers) duidelijk maken dat er een beperking op de verwerking rust en de betrokkene op de hoogte stellen zodra deze beperking wordt opgeheven.

Recht op dataportabiliteit

Betrokkene heeft het recht zijn persoonsgegevens die hij aan u heeft verstrekt in een gestructureerde, gangbare en machine-leesbare vorm te verkrijgen, en hij heeft het recht die persoonsgegevens aan een andere verantwoordelijke over te dragen, zonder daarbij te worden gehinderd, wanneer:

- de verwerking berust op toestemming of op een overeenkomst;
- de verwerking via geautomatiseerde procedés wordt verricht.

Ook kan de betrokkene verzoeken zijn persoonsgegevens rechtstreeks aan de nieuwe verwerkingsverantwoordelijke te verstrekken.
Het recht op dataportabiliteit kan alleen aan de verwerkingsverantwoordelijke worden opgelegd, als dit technisch mogelijk is en dit geen afbreuk doet aan de rechten en vrijheden van anderen.

Recht van bezwaar

Vanwege redenen die verband houden met zijn specifieke situatie kan betrokkene gebruik maken van het recht van bezwaar tegen de verwerking van zijn persoonsgegevens. Als de betrokkene bezwaar maakt, moet u de verwerking staken, tenzij dwingende gerechtvaardigde gronden anders bepalen.

Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming

De betrokkene heeft het recht om niet onderworpen te worden aan uitsluitend automatische besluitvorming waaraan voor hem rechtsgevolgen zijn verbonden. Denk bijvoorbeeld aan het automatisch weigeren van een online ingediende kredietaanvraag.

Geautomatiseerde besluitvorming is wel mogelijk wanneer:

- het noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst;
- het is toegestaan bij wet;
- de betrokkene hiervoor zijn uitdrukkelijke toestemming heeft gegeven.

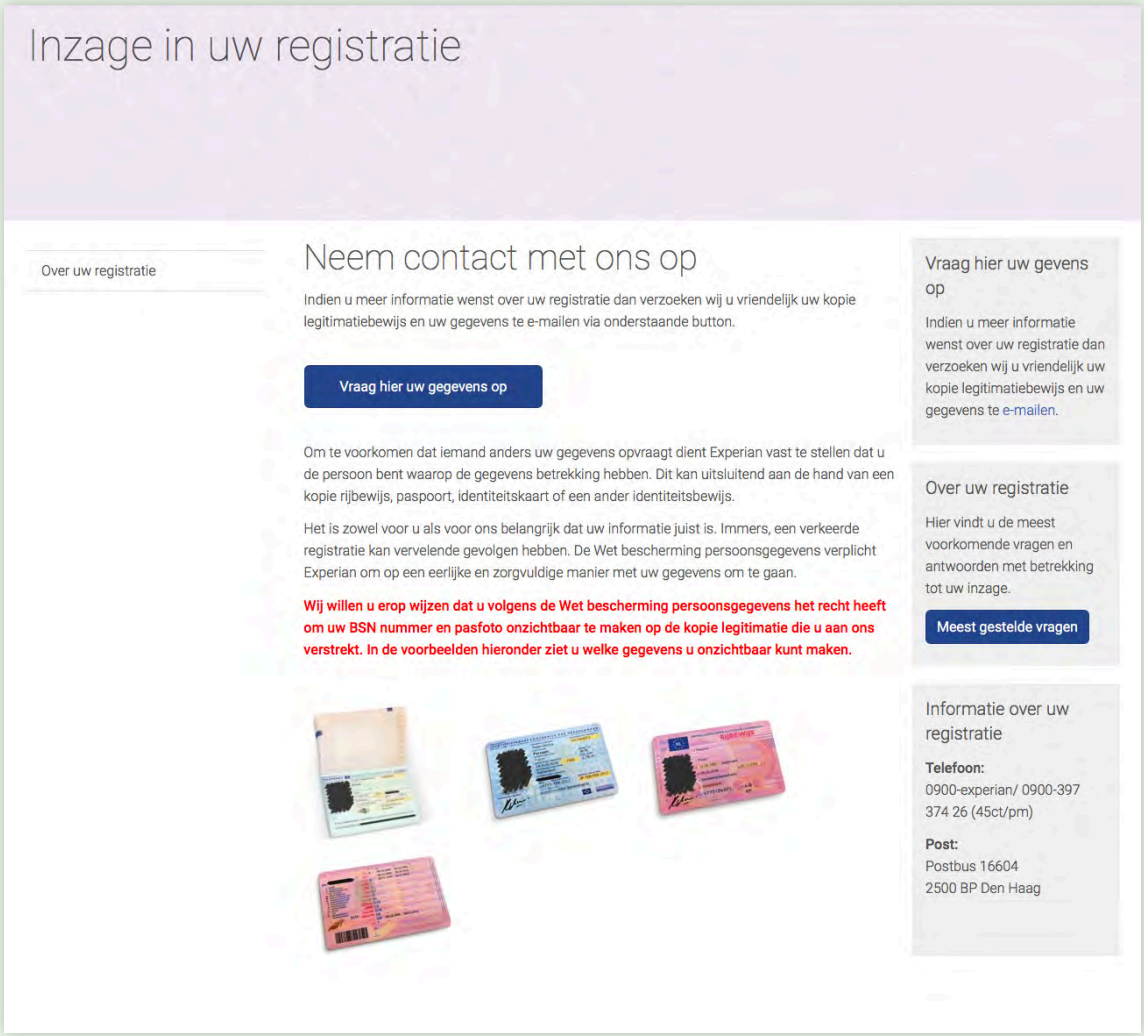
Bij een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor de betrokkene rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft, heeft betrokkene:

- ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke;
- het recht om zijn standpunt kenbaar te maken;
- het recht om het besluit aan te vechten;
- het recht op uitleg van de genomen beslissing. Als verwerkingsverantwoordelijke moet u de effectiviteit kunnen aantonen, passende wiskundige en statistische procedures hebben gevolgd en zorgen dat onjuistheden in de persoonsgegevens en het risico op fouten is geminimaliseerd.

15.4 Voorbeeld

Voorbeeld 1

Databedrijf Experian heeft een heldere inzageprocedure die zeer goed toegankelijk is voor betrokkenen. Ook laten ze zien hoe een betrokkene zich online kan legitimeren zonder dat daarbij gevoelige gegevens met Experian worden gedeeld.



16 Informatie-beveiliging

Om verlies of onrechtmatige verwerking van persoonsgegevens te voorkomen zijn passende fysieke, technische en organisatorische maatregelen nodig. De zwaarte van deze maatregelen hangt af van de risico's en de aard van de persoonsgegevens en van de (technische) mogelijkheden en kosten.
Het is raadzaam om aan te sluiten bij erkende standaarden hiervoor. In dit hoofdstuk leest u verder welke concrete maatregelen u kunt nemen; van beveiligingsbeleid tot het sluiten van verwerkersovereenkomsten.

16.1 Eis

De toepassing moet voldoende worden beveiligd door passende technische en organisatorische maatregelen te treffen tegen verlies of enige andere vorm van onrechtmatige verwerking.

16.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 28 AVG
- Artikel 32 AVG

16.3 Toelichting

U dient passende fysieke, technische en organisatorische maatregelen te nemen om verlies of onrechtmatige verwerking van persoonsgegevens tegen te gaan. Hierbij dienen de risico's en aard van de persoonsgegevens te worden meegewogen, rekening houdend met de stand van de techniek en de kosten. Een passende beveiliging voorkomt onnodige verwerking. Ook dient de beveiliging adequaat te zijn, daarom dient periodiek te worden nagegaan of de beveiliging moet worden aangepast aan de technologische ontwikkelingen. Het wordt aanbevolen om voor het realiseren van de beveiliging aan te sluiten bij erkende standaarden, zoals ISO 27001 en 27002. Als u creditcardgegevens verwerkt, dan moet u ook de PCI-standaard meenemen.[7]

De Autoriteit Persoonsgegevens (AP) heeft richtsnoeren voor de beveiliging van persoonsgegevens opgesteld die een kader bieden voor het goed beveiligen van persoonsgegevens.[8] De AP heeft echter geen standaard vastgesteld voor de beveiliging, daarvoor zijn de ISO-standaarden.

[7] Zie: http://www.iso.org/ - https://www.pcisecuritystandards.org

[8] Zie: http://wetten.overheid.nl/BWBR0033572/geldigheidsdatum_02-07-2015

Verwerkersovereenkomst

Indien u gebruik maakt van een verwerker, moet u met deze partij een verwerkersovereenkomst (artikel 28 lid 3 AVG) afsluiten waarin u vastlegt dat de verwerker:

- uitsluitend de persoonsgegevens verwerkt in uw opdracht;
- de beveiligingsverplichtingen nakomt die op u rusten op grond van de AVG;
- u het recht geeft erop toe te zien dat de verwerker daadwerkelijk de beveiligingsverplichtingen naleeft.

16.4 Voorbeelden

Hieronder worden enkele voorbeelden gegeven van de soorten maatregelen die u kunt nemen. Houd er rekening mee dat het niveau van beveiliging altijd gerelateerd moet zijn aan de gevoeligheid van de persoonsgegevens en de risico's voor de privacy die deze gegevens opleveren als zij lekken. Wat een 'adequate beveiliging' is, is dus afhankelijk van uw concrete situatie. Deze lijst is niet uitputtend en dient slechts als voorbeeld. Standaarden als de ISO 27001 en 27002 geven een volledig overzicht van maatregelen in het kader van informatiebeveiliging.

Fysieke maatregelen

Toegangsbeveiliging

Door middel van toegangscontrole (pasjes, camera's) kunnen onbevoegden worden geweerd.

Beveiligde ruimtes voor IT-systemen

Zorg voor extra beveiliging op die plekken waar de persoonsgegevens daadwerkelijk zijn opgeslagen en zorg dat alleen de personen die belast zijn met het beheer en onderhoud van IT-systemen deze ruimtes kunnen betreden.

Organisatorische maatregelen

Beveiligingsbeleid
Vertrekpunt voor een effectieve beveiliging is een beveiligingsbeleid of beveiligingsplan. In het beveiligingsplan is de verantwoordelijkheid voor de beveiliging vastgesteld, worden maatregelen beschreven en worden zaken als monitoring en handhaving uiteengezet.

Incident-response
Geen enkele beveiliging is 100% waterdicht. Het kan dus altijd gebeuren dat er een beveiligingsincident is en dat persoonsgegevens lekken. Hoe u met een dergelijke situatie moet omgaan, legt u vast in een incident-response-plan. Hierin kunt u ook aangeven wanneer en hoe een beveiligingsinbreuk moet worden gemeld bij de toezichthouder (zie ook hoofdstuk 19 Meldplicht datalekken).

Beveiligingsbewustzijn
Een goede beveiliging staat of valt met bewustzijn bij de medewerkers. Zorg dat iedereen op de hoogte is van risico's en gevaren en de maatregelen die getroffen zijn om deze risico's en gevaren te ondervangen. Denk hierbij aan trainingen, workshops enzovoorts.

Technische maatregelen

Beveiliging van IT-voorzieningen
Zorg ervoor dat alle IT-voorzieningen beveiligd zijn. Denk hierbij aan wachtwoorden voor alle apparaten, een patchbeleid zodat alle systemen altijd up to date zijn en encryptie van belangrijke bestanden en databases. Een belangrijk onderdeel van de beveiliging is toegangscontrole: wie mag erbij welke data? Zorg daarom dat u een helder autorisatiebeleid heeft.

Netwerkbeveiliging
Zorg ervoor dat uw netwerk beschermd is tegen aanvallers. Denk hierbij aan antivirussoftware en firewalls. Bij meer risicovolle gegevens kunt u denken aan intrusion detection systems (IDS) en permanente monitoring van data.

Logging en monitoring
Houd het gebruik van en de toegang tot systemen bij, zodat u achteraf (of in real time) onregelmatigheden kunt constateren.

17 Bewaren

Persoonsgegevens mag u niet langer bewaren dan noodzakelijk is om het doel te realiseren. Wanneer u het doel van de verwerking van persoonsgegevens vaststelt, moet u ook de bewaartermijn bepalen. Als deze termijn is verstreken, vernietigt of anonimiseert u de persoonsgegevens. Vermeld de bewaar-termijnen ook in het privacy-statement.

17.1 Eis

- ***Persoonsgegevens zijn voorzien van een bewaartermijn.***

- ***Persoonsgegevens worden vernietigd of geanonimiseerd wanneer zij niet langer noodzakelijk zijn voor de verwerkingsdoelen.***

17.2 Wettelijke bepaling

Deze eis is gebaseerd op de volgende wettelijke bepaling:
- Artikel 5 lid 1 sub e AVG

17.3 Toelichting

De persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk om het doel van de verwerking te realiseren. Bij het vaststellen van het doel dient ook de bewaartermijn te worden bepaald. Als het niet langer noodzakelijk is om de persoonsgegevens te bewaren, moeten deze gegevens verwijderd worden of alle identificerende kenmerken worden verwijderd (anonimiseren). Vermeld ook de bewaartermijnen in uw privacy-statement.

17.4 Voorbeelden

Voorbeeld 1

Wanneer een gebruiker de dienst van SnellerThuis BV opzegt, dan begint de bewaartermijn te lopen. Accountgegevens die niet relevant zijn om te bewaren, zoals de profielfoto van de gebruiker, worden direct vernietigd. Snellerthuis BV bewaart met het oog op wettelijke bewaarverplichtingen van de Belastingdienst factuurgegevens zeven jaar.

Voorbeeld 2

Het privacybeleid van spitsmijdenproject Spitsmijden Galecopperbrug stelt dat gegevens na tien werkweken worden verwijderd.

Bewaren van uw persoonsgegevens

Opgevraagde persoonsgegevens van automobilisten, die vaak van het projecttraject gebruikmaken, maar niet ingaan op de uitnodiging of eenmalige herinnering om deel te nemen aan '*Spitsmijden Galecopperbrug*', worden binnen tien werkweken na registratie verwijderd uit de database van *Spitsmijden Galecopperbrug*, onder voorbehoud van onvoorziene omstandigheden.

Statistische gegevens, die worden gebruikt voor verkeersonderzoek door Rijkswaterstaat (bijvoorbeeld voor maatregelen om de files te verminderen) worden mogelijk langer bewaard. Deze gegevens zijn geanonimiseerd en dus niet te herleiden naar een persoon.

18 Gegevensexport

Persoonsgegevens mag u niet naar landen versturen waar geen goede privacyscherming is. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt binnen de Europese Economische Ruimte (lidstaten van de EU, IJsland, Noorwegen en Liechtenstein), en in landen die volgens de Europese Commissie een adequaat beschermingsniveau bieden. Voor gegevensexport naar andere landen kunt u gebruik maken van 'standaard contractuele bepalingen'.

18.1 Eis

Persoonsgegevens mogen niet naar een land worden verstuurd waar géén adequaat niveau van privacybescherming is.

18.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 44 AVG
- Artikel 45 AVG
- Artikel 46 AVG
- Artikel 47 AVG
- Artikel 48 AVG
- Artikel 49 AVG

18.3 Toelichting

Uitgangspunt is dat persoonsgegevens alleen mogen worden verwerkt in landen waar goede privacywetgeving is. Landen waar een adequaat niveau van bescherming is zijn:

- De landen binnen de Europese Economische Ruimte. De Europese Economische Ruimte bestaat uit de lidstaten van de Europese Unie plus IJsland, Noorwegen en Liechtenstein.
- Landen die volgens de Europese Commissie een adequaat niveau van bescherming bieden. Op het moment van de publicatie van deze leidraad zijn dat: Andorra, Argentinië, Canada, Zwitserland, de Faeröer eilanden, Guernsey, Israël, the Isle of Man, Jersey, Uruguay, Nieuw Zeeland en organisaties in de Verenigde Staten die zich hebben aangesloten bij het EU-US Privacy Shield.

Wanneer een land geen adequaat niveau van bescherming biedt en u wilt toch persoonsgegevens in dat land laten verwerken, dan moet u gebruikmaken van één van de uitzonderingen die artikel 46 AVG biedt. De belangrijkste uitzondering is het gebruik maken van 'standaard contractuele bepalingen'. Deze bepalingen zijn opgesteld door de Europese Commissie en zijn erop gericht de privacy van betrokkene te waarborgen. Als deze contractuele bepalingen zijn opgenomen, dan mogen de persoonsgegevens ook worden doorgestuurd.

18.4 Voorbeeld

Voorbeeld 1

SnellerThuis BV wil haar applicatie en de bijbehorende klantendatabase hosten in India. Omdat India geen land is met een passend beschermingsniveau, moet van één van de uitzonderingen gebruik worden gemaakt.

[7] Voor meer informatie zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer

19 Meldplicht datalekken

Bij een datalek gaan persoonsgegevens verloren of bestaat er een risico dat deze gegevens onrechtmatig worden verwerkt. De AVG schrijft voor dat de verwerkingsverantwoordelijke een datalek bij de Autoriteit Persoonsgegevens moet melden, wanneer het gevoelige persoonsgegevens betreft, zoals financiële gegevens of inloggegevens, of de omvang van het datalek aanzienlijk is. Als een datalek ongunstige gevolgen kan hebben voor de betrokken personen, bent u als verwerkingsverantwoordelijke verplicht om ook hen hierover onmiddellijk te informeren. In dit hoofdstuk krijgt u inzicht wanneer en aan wie u een datalek moet melden.

19.1 Eis

- ***De verwerkingsverantwoordelijke stelt de Autoriteit Persoonsgegevens (AP) op de hoogte van een beveiligingsinbreuk die leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.***

- ***De verwerkingsverantwoordelijke stelt ook de betrokkene op de hoogte van bovengenoemde beveiligingsinbreuk indien deze waarschijnlijk ongunstige gevolgen heeft voor zijn persoonlijke levenssfeer.***

19.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:
- Artikel 33 AVG
- Artikel 34 AVG

19.3 Toelichting

Melding aan de Autoriteit Persoonsgegevens

U moet zo snel mogelijk en binnen 72 uur een melding doen bij de Autoriteit Persoonsgegevens wanneer sprake is van een ernstig datalek. Een datalek is een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of waarbij onrechtmatige verwerking redelijkerwijs niet uit kan worden gesloten. Voorbeelden van een datalek zijn: het kwijtraken van een USB-stick, een inbraak door een hacker, een malwarebesmetting of een brand in een datacentrum.

Als verwerkingsverantwoordelijke hoeft u alleen een datalek te melden, wanneer dit datalek leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Hierbij spelen de aard en de omvang van de persoonsgegevens een rol. In de regel is het zo dat u verlies van persoonsgegevens van gevoelige aard moet melden. Dit zijn bijvoorbeeld bijzondere persoonsgegevens (zoals gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging of strafrechtelijke gegevens), gegevens over de financiële of economische situatie van de betrokkene, gegevens die kunnen leiden tot stigmatisering of uitsluiting van

de betrokkene, gebruikersnamen, wachtwoorden en andere inloggegevens en gegevens die misbruikt kunnen worden voor (identiteits)fraude.

Bij de beoordeling of u een datalek moet melden, speelt ook de hoeveelheid persoonsgegevens per persoon en/of het aantal betrokkenen waarvan persoonsgegevens zijn gelekt een rol. Voor melding aan de AP vult u het webformulier in dat op de website van de AP staat. Als u geen gebruik kunt maken van het webformulier, kunt u de melding aan de AP faxen.

Documentatieplicht

Ondanks dat niet iedere datalek gemeld moet worden aan de AP, moet wel elk datalek gedocumenteerd worden. In deze documentatie moet worden vastgesteld wat de feiten zijn over de inbreuk, de gevolgen hiervan en de genomen corrigerende maatregelen. Vermeld daarbij waarom ervoor gekozen is om de datalek niet te melden.

Melding aan de betrokkene

Als u een datalek moet melden aan de AP, moet u afwegen of u dit datalek ook aan de betrokkene moet melden. U bent verplicht het datalek onverwijld te melden aan de betrokkene indien het datalek waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer. Dit betekent dat betrokkene door het datalek in zijn belangen kan worden geschaad. Voorbeelden hiervan zijn een onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Bij een datalek van gevoelige gegevens kunt u ervan uitgaan dat u deze aan de betrokkene moet melden.

Door de betrokkene op de hoogte te stellen van het datalek, kan hij maatregelen nemen om zichzelf te beschermen tegen de gevolgen van het datalek. Daarom moet u ook zo snel mogelijk de betrokkene informeren.

U kunt de melding aan betrokkene achterwege laten, wanneer u passende beveiligingsmaatregelen heeft genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden. Voorbeelden hiervan zijn encryptie en hashing. Beoordeel per geval of de getroffen beveiligingsmaatregelen zodanige bescherming bieden dat melding aan betrokkene niet nodig is.

In de melding aan de betrokkene moet u als verwerkingsverantwoordelijke in ieder geval vermelden:

- de aard van het datalek;
- de instanties waar betrokkene meer informatie over het datalek kan krijgen, en
- de maatregelen die u de betrokkene aanbeveelt om de negatieve gevolgen van het datalek te beperken.

Beleidsregels voor de beoordeling of melding moet worden gedaan

De AP heeft beleidsregels opgesteld voor de beoordeling of u een beveiligingsincident aan de AP en eventueel ook aan de betrokkene moet melden.

19.4 Voorbeelden

Voorbeeld 1

Hackers verschaffen zich toegang tot de database van SnellerThuis BV en maken een kopie. In deze database staan de onversleutelde inloggegevens van alle gebruikers van de app van SnellerThuis BV.

SnellerThuis BV doet binnen 72 uur een melding van dit datalek aan de AP via het web-formulier. Ook informeert SnellerThuis BV alle gebruikers over dit datalek en geeft daarbij aan dat de gebruikers hun wachtwoord moeten veranderen.

Voorbeeld 2

Er komt een malwaremelding binnen op een computer van een medewerker van SnellerThuis BV. Er blijkt een virus op de systemen van SnellerThuis BV te zijn binnengekomen waardoor onbevoegden toegang hebben tot de geëncrypteerde inloggegevens van de gebruikers van de app van SnellerThuis BV, maar geen toegang tot de sleutel om de inloggegevens te kunnen ontsleutelen.

SnellerThuis BV doet binnen 72 uur een melding van dit datalek aan de AP via het webformulier. SnellerThuis BV kan de melding van dit datalek aan alle gebruikers achterwege laten, omdat de inloggegevens op een adequate wijze waren versleuteld, waardoor het datalek geen ongunstige gevolgen heeft voor de bescherming van de persoonlijke levenssfeer van de gebruikers.

20 Aanstellen functionaris voor gegevens-bescherming

De functionaris voor gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de AVG. In dit hoofdstuk leest u wanneer een FG verplicht is.

20.1 Eis

De verwerkingsverantwoordelijke stelt een functionaris voor de gegevensbescherming (FG) aan wanneer:
- de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan;
- het op grote schaal volgen van individuen de kernactiviteit is van verwerkingsverantwoordelijke;
- het op grote schaal verwerken van bijzondere persoonsgegevens een kernactiviteit is van verwerkingsverantwoordelijke.

20.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:
- Artikel 37 AVG

20.3 Toelichting

De functionaris voor gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de AVG. Een FG is verplicht wanneer:
- de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan;
- de organisaties vanuit hun kernactiviteit op grote schaal individuen volgen, bijvoorbeeld door cameratoezicht. Het gaat hier ook om profilering van mensen voor het maken van risico-inschattingen;
- er op grote schaal bijzondere persoonsgegevens verwerkt worden en dit een kernactiviteit is. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over ras, gezondheid, politieke voorkeur of geloofsovertuiging.

20.4 Voorbeeld

Voorbeeld 1
ToetToet BV heeft als primaire dienstverlening het aanbieden van kentekenregistratiesystemen die boven de weg worden gehangen. Omdat sprake is van stelselmatige monitoring van individuen, is ToetToet BV verplicht een FG aan te stellen.

21 Registerplicht

Als verwerkingsverantwoordelijke moet u een register bijhouden van alle verwerkingsactiviteiten die onder uw verantwoordelijkheid plaatsvinden. Bent u een verwerker, dan moet u een register bijhouden van alle categorieën van verwerkingsactiviteiten die u in opdracht van de verwerkingsverantwoordelijke hebt verricht.

21.1 Eis

- ***De verwerkingsverantwoordelijke houdt een register bij van verwerkingen van persoonsgegevens.***
- ***De verwerker houdt een register bij van verwerkingen van persoonsgegevens.***
- ***Deze plicht geldt niet voor een verwerkingsverantwoordelijke of verwerker die minder dan 250 personen in dienst heeft, tenzij sprake is van verwerkingen met een hoog risico, niet incidentele verwerkingen of verwerkingen van bijzondere categorieën van persoonsgegevens.***

21.2 Wettelijke bepaling

Deze eis is gebaseerd op de volgende wettelijke bepaling:

- Artikel 30 AVG

21.3 Toelichting

Zowel de verwerkingsverantwoordelijke als een verwerker moet schriftelijk een register van verwerkingsactiviteiten bijhouden.

In het verwerkingenregister van de verwerkingsverantwoordelijke staan in ieder geval:

- de naam en contactgegevens van de verwerkingsverantwoordelijke, eventuele gezamenlijke verwerkingsverantwoordelijken en de functionaris voor de gegevensbescherming (de FG);
- de doeleinden voor persoonsgegevensverwerking;
- een beschrijving van de categorieën betrokkenen en categorieën persoonsgegevens;
- de (voorgenomen) categorieën ontvangers;
- een vermelding van een verstrekking van persoonsgegevens aan een derde land of een internationale organisatie;
- de (voorgenomen) bewaartermijnen en
- een algemene beschrijving van de beveiligingsmaatregelen.

In het verwerkingenregister van de verwerker staan in ieder geval:

- de naam en contactgegevens van de verwerker(s), verantwoordelijk(en) en de eventuele FG;
- de categorieën verwerkingsactiviteiten;
- een vermelding van een verstrekking van persoonsgegevens aan een derde land of een internationale organisatie en
- een algemene beschrijving van de beveiligingsmaatregelen.

Er zijn geen vormvereisten aan het verwerkingenregister, behalve dat het register schriftelijk (waaronder elektronisch) moet zijn.

De registerplicht geldt niet voor organisaties die minder dan 250 personen in dienst hebben, tenzij er sprake is van verwerkingen die waarschijnlijk een hoog risico voor betrokkenen inhouden, de verwerkingen niet van incidentele aard zijn of bijzondere categorieën van persoonsgegevens worden verwerkt.

21.4 Voorbeelden

Voorbeeld 1

Het bedrijf EyeSeeYou B.V. verkoopt hard- en software waarmee verkeersregelinstallaties kunnen registreren hoeveel auto's op een bepaalde tijd over een kruising rijden. De organisatie heeft in totaal 300 medewerkers in dienst. Omdat EyeSeeYou B.V. meer dan 250 medewerkers in dienst heeft, is het verplicht een register van verwerkingen van persoonsgegevens bij te houden.

Voorbeeld 2

ToetToet BV ondersteunt wegbeheerders door het aanbieden van kentekenregistratiesystemen die boven de weg worden gehangen. Voor gemeente Vaartje wordt ToetToet BV ingeschakeld om op de lokale weg van Vaartje de kentekenregistratiecamera's op te hangen om een nulmeting uit te voeren in het kader van aankomende renovatiewerkzaamheden aan deze weg. Omdat ToetToet BV zo een database opbouwt met kentekens en dit als een verwerking met een hoog risico wordt gezien, is ToetToet BV verplicht deze verwerking bij te houden in het verwerkingenregister.

22 Bijlage: Wetsartikelen per hoofdstuk

In verband met de leesbaarheid van de hoofdstukken is ervoor gekozen om in de hoofdstukken slechts te verwijzen naar de wetsartikelen. Als referentiemateriaal zijn de wetsartikelen integraal in deze bijlage opgenomen. Daarbij volgen we de hoofdstukindeling.

22.1 Verantwoordelijkheid

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 3 AVG - Territoriaal toepassingsgebied

1. Deze verordening is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt.

2. Op de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie is Verordening van toepassing.

3. Deze verordening is van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met:
   a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of
   b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt.

4. Deze verordening is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet in de Unie is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het lidstatelijke recht van toepassing is.

Artikel 4 onder 7 AVG - Verwerkingsverantwoordelijke

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

Artikel 28 AVG – Verwerker

1. Wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

2. De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

3. De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Die overeenkomst of andere rechtshandeling bepaalt met name dat de verwerker:
   a) de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een

op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;

b) waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;

c) alle overeenkomstig artikel 32 vereiste maatregelen neemt;

d) aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;

e) rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III vastgestelde rechten van de betrokkene te beantwoorden;

f) rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36;

g) na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;

h) de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt.

Waar het gaat om de eerste alinea, punt h), stelt de verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

4. Wanneer een verwerker een andere verwerker in dienst neemt om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst of een andere rechtshandeling krachtens Unierecht of lidstatelijk recht dezelfde verplichtingen inzake gegevensbescherming

opgelegd als die welke in de in lid 3 bedoelde overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker zijn opgenomen, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de verwerking aan het bepaalde in deze verordening voldoet. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de eerste verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker.

5. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat voldoende garanties als bedoeld in de leden 1 en 4 van dit artikel worden geboden.

6. Onverminderd een individuele overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker kan de in de leden 3 en 4 van dit artikel bedoelde overeenkomst of andere rechtshandeling geheel of ten dele gebaseerd zijn op de in de leden 7 en 8 van dit artikel bedoelde standaardcontractbepalingen, ook indien zij deel uitmaken van de certificering die door een verwerkingsverantwoordelijke of verwerker uit hoofde van de artikelen 42 en 43 is verleend.

7. De Commissie kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure standaardcontractbepalingen vaststellen.

8. Een toezichthoudende autoriteit kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens het in artikel 63 bedoelde coherentiemechanisme standaardcontractbepalingen opstellen.

9. De in de leden 3 en 4 bedoelde overeenkomst of andere rechtshandeling wordt in schriftelijke vorm, waaronder elektronische vorm, opgesteld.

10. Indien een verwerker in strijd met deze verordening de doeleinden en middelen van een verwerking bepaalt, wordt die verwerker onverminderd de artikelen 82, 83 en 84 met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd.

22.2 Verantwoording

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 5 AVG - Beginselen inzake verwerking van persoonsgegevens

1. Persoonsgegevens moeten:
   a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is ("rechtmatigheid, behoorlijkheid en transparantie");
   b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd ("doelbinding");
   c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking");
   d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren ("juistheid");
   e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen ("opslagbeperking");
   f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ("integriteit en vertrouwelijkheid").

2. De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen ("verantwoordingsplicht").

22.3 Legitiem doel en grondslag

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 5 lid 1 sub b AVG - doelbinding

Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd ("doelbinding").

Artikel 6 sub a en sub f AVG - rechtmatigheid van de verwerking

De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Artikel 7 AVG – voorwaarden voor toestemming

1. Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

2. Indien de betrokkene toestemming geeft in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft, wordt het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.

3. De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming is even eenvoudig als het geven ervan.

4. Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.

Artikel 11.7a Telecommunicatiewet

1. Onverminderd de Wet bescherming persoonsgegevens is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker:
   a) is voorzien van duidelijke en volledige informatie overeenkomstig de Wet bescherming persoonsgegevens, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en
   b) daarvoor toestemming heeft verleend.

2. De in het eerste lid, onder a en b, genoemde vereisten zijn ook van toepassing in het geval op een andere wijze dan door middel van een elektronisch communicatienetwerk wordt bewerkstelligd dat via een elektronisch communicatienetwerk informatie wordt opgeslagen of toegang wordt verleend tot op het randapparaat opgeslagen informatie.

3. Het bepaalde in het eerste lid is niet van toepassing indien het de opslag of toegang betreft:
   a) met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren,

b) die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren of – mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij.

4. Een handeling als bedoeld in het eerste lid, die tot doel heeft gegevens over het gebruik van verschillende diensten van de informatiemaatschappij door de gebruiker of de abonnee te verzamelen, combineren of analyseren zodat de betrokken gebruiker of abonnee anders behandeld kan worden, wordt vermoed een verwerking van persoonsgegevens te zijn, als bedoeld in artikel 1, onderdeel b, van de Wet bescherming persoonsgegevens.

5. De toegang van de gebruiker tot een dienst van de informatiemaatschappij die wordt geleverd door of namens een krachtens publiekrecht ingestelde rechtspersoon wordt niet afhankelijk gemaakt van het verlenen van toestemming als bedoeld in het eerste lid.

6. Bij of krachtens algemene maatregel van bestuur kunnen in overeenstemming met onze Minister van Veiligheid en Justitie nadere regels worden gegeven met betrekking tot de in het eerste lid, onder a en b, genoemde vereisten en de in het derde lid genoemde uitzonderingen. Het College bescherming persoonsgegevens wordt om advies gevraagd over een ontwerp van bedoelde algemene maatregel van bestuur.

22.4 Dataminimalisatie

Deze eis is gebaseerd op de volgende wettelijke bepaling:

Artikel 5 lid 1 sub c (dataminimalisatie)
Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking").

22.5 Privacy by design and by default

Deze eis is gebaseerd op de volgende wettelijke bepaling:

Artikel 25 - Privacy by design and by default

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.

2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

3. Een overeenkomstig artikel 42 goedgekeurd certificeringsmechanisme kan worden gebruikt als element om aan te tonen dat aan de voorschriften van de leden 1 en 2 van dit artikel is voldaan.

22.6 Data protection impact asessment

Deze eis is gebaseerd op de volgende wettelijke bepaling:

Artikel 35 AVG – data protection impact assessment

1. 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.

2. Wanneer een functionaris voor gegevensbescherming is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.

3. Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:
   a) 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;
   b) 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
   c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

4. De toezichthoudende autoriteit stelt een lijst op van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling overeenkomstig lid 1 verplicht is, en maakt deze openbaar. De toezichthoudende autoriteit deelt die lijsten mee aan het in artikel 68 bedoelde Comité.

5. De toezichthoudende autoriteit kan ook een lijst opstellen en openbaar maken van het soort verwerking waarvoor geen gegevensbeschermingseffectbeoordeling is vereist. De toezichthoudende autoriteit deelt deze lijst mee aan het Comité.

6. Wanneer de in de leden 4 en 5 bedoelde lijsten betrekking hebben op verwerkingen met betrekking tot het aanbieden van goederen of diensten aan betrokkenen of op het observeren van hun gedrag in verschillende lidstaten, of op verwerkingen die het vrije verkeer van persoonsgegevens in de Unie wezenlijk kunnen beïnvloeden, past de bevoegde toezichthoudende autoriteit voorafgaand aan de vaststelling van die lijsten het in artikel 63 bedoelde coherentiemechanisme toe.

7. De beoordeling bevat ten minste:
   a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
   b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
   c) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en
   d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

8. Bij het beoordelen van het effect van de door een verwerkingsverantwoordelijke of verwerker verrichte verwerkingen, en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van de in artikel 40 bedoelde goedgekeurde gedragscodes naar behoren in aanmerking genomen.

9. De verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.

10. Wanneer verwerking uit hoofde van artikel 6, lid 1, onder c) of e), haar rechtsgrond heeft in het Unierecht of in het recht van de lidstaat dat op de verwerkingsverantwoordelijke van toepassing is, de specifieke verwerking of geheel van verwerkingen in kwestie daarbij wordt geregeld, en er reeds als onderdeel van een algemene effectbeoordeling in het kader van de vaststelling van deze rechtsgrond een gegevensbeschermingseffectbeoordeling is uitgevoerd, zijn de leden 1 tot en met 7 niet van toepassing, tenzij de lidstaten het noodzakelijk achten om voorafgaand aan de verwerkingen een dergelijke beoordeling uit te voeren.

11. Indien nodig verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.

22.7 Doelbinding

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 5 lid 1 sub b AVG - doelbinding
Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd (“doelbinding”);

Artikel 5 lid 1 sub c (dataminimalisatie)
Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (“minimale gegevensverwerking”);

22.8 Informatie en transparantie

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 13 AVG

1. Wanneer persoonsgegevens betreffende een betrokkene bij die persoon worden verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene bij de verkrijging van de persoonsgegevens al de volgende informatie:
   a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;
   b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;
   c) de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, alsook de rechtsgrond voor de verwerking;
   d) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd;
   e) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
   f) in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of een internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of, in het geval van in artikel 46, artikel 47 of artikel 49, lid 1, tweede alinea, bedoelde doorgiften, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

2. Naast de in lid 1 bedoelde informatie verstrekt de verwerkingsverantwoordelijke de betrokkene bij de verkrijging van de persoonsgegevens de volgende aanvullende informatie om een behoorlijke en transparante verwerking te waarborgen:
   a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria ter bepaling van die termijn;
   b) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van de persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid;

c) wanneer de verwerking op artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;
d) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
e) of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
f) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

3. Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2.

4. De leden 1, 2 en 3 zijn niet van toepassing wanneer en voor zover de betrokkene reeds over de informatie beschikt.

Artikel 14 AVG

1. Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie:
a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;
b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;
c) de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking;
d) de betrokken categorieën van persoonsgegevens;

e) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;
f) in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een ontvanger in een derde land of aan een internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of, in het geval van de in artikel 46, artikel 47 of artikel 49, lid 1, tweede alinea, bedoelde doorgiften, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.

2. Naast de in lid 1 bedoelde informatie verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie om ten overstaan van de betrokkene een behoorlijke en transparante verwerking te waarborgen:
a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
b) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd;
c) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van persoonsgegevens of om beperking van de hem betreffende verwerking, alsmede het recht tegen verwerking van bezwaar te maken en het recht op gegevensoverdraagbaarheid;
d) wanneer verwerking op artikel 6, lid 1, punt a) of artikel 9, lid 2, punt a), is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;
e) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
f) de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen;
g) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

3. De verwerkingsverantwoordelijke verstrekt de in de leden 1 en 2 bedoelde informatie:
   a) binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;
   b) indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of
   c) indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

4. Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2.

5. De leden 1 tot en met 4 zijn niet van toepassing wanneer en voor zover:
   a) de betrokkene reeds over de informatie beschikt;
   b) het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, bedoelde voorwaarden en waarborgen, of voor zover de in lid 1 van dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt de verwerkingsverantwoordelijke passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;
   c) het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unie- of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen; of
   d) de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of lidstatelijke recht, waaronder een statutaire geheimhoudingsplicht.

Artikel 11.7a Telecommunicatiewet

1. Onverminderd de Wet bescherming persoonsgegevens is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker:
   a) is voorzien van duidelijke en volledige informatie overeenkomstig de Wet bescherming persoonsgegevens, in ieder geval over de doeleinden waarvoor deze informatie wordt gebruikt, en
   b) daarvoor toestemming heeft verleend.

2. De in het eerste lid, onder a en b, genoemde vereisten zijn ook van toepassing in het geval op een andere wijze dan door middel van een elektronisch communicatienetwerk wordt bewerkstelligd dat via een elektronisch communicatienetwerk informatie wordt opgeslagen of toegang wordt verleend tot op het randapparaat opgeslagen informatie.

3. Het bepaalde in het eerste lid is niet van toepassing indien het de opslag of toegang betreft:
   a) met als uitsluitend doel de communicatie over een elektronisch communicatienetwerk uit te voeren,
   b) die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren of - mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker - om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij.

4. Een handeling als bedoeld in het eerste lid, die tot doel heeft gegevens over het gebruik van verschillende diensten van de informatiemaatschappij door de gebruiker of de abonnee te verzamelen, combineren of analyseren zodat de betrokken gebruiker of abonnee anders behandeld kan worden, wordt vermoed een verwerking van persoonsgegevens te zijn, als bedoeld in artikel 1, onderdeel b, van de Wet bescherming persoonsgegevens.

5. De toegang van de gebruiker tot een dienst van de informatiemaatschappij die wordt geleverd door of namens een krachtens publiekrecht ingestelde rechtspersoon wordt niet afhankelijk gemaakt van het verlenen van toestemming als bedoeld in het eerste lid.

Bij of krachtens algemene maatregel van bestuur kunnen in overeenstemming met Onze Minister van Veiligheid en Justitie nadere regels worden gegeven met betrekking tot de in het eerste lid, onder a en b, genoemde vereisten en de in het derde lid genoemde uitzonderingen.

Het College bescherming persoonsgegevens wordt om advies gevraagd over een ontwerp van bedoelde algemene maatregel van bestuur.

22.9 Delen van persoonsgegevens met derden

Deze eis is gebaseerd op de volgende wettelijke bepaling:

Artikel 6 sub a en sub f AVG rechtmatigheid van de verwerking

De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Artikel 9 AVG

1. Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

2. Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan:
   a) de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven;
   b) de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het socialezekerheids- en sociale-beschermingsrecht, voor zover zulks is toegestaan bij Unierecht of lidstatelijk recht of

bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt;

c) de verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven;

d) de verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt;

e) de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;

f) de verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid;

g) de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene;

h) de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen;

i) de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim;

j) de verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.

3. Wanneer die gegevens worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden, of door een andere persoon die eveneens krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels tot geheimhouding is gehouden.

4. De lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren.

22.10 Rechten van de betrokkene

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 15 AVG – recht op inzage

1. De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens en van de volgende informatie:
   a) de verwerkingsdoeleinden;
   b) de betrokken categorieën van persoonsgegevens;
   c) de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
   d) indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

e) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
f) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
g) wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
h) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

2. Wanneer persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie, heeft de betrokkene het recht in kennis te worden gesteld van de passende waarborgen overeenkomstig artikel 46 inzake de doorgifte.

3. De verwerkingsverantwoordelijke verstrekt de betrokkene een kopie van de persoonsgegevens die worden verwerkt. Indien de betrokkene om bijkomende kopieën verzoekt, kan de verwerkingsverantwoordelijke op basis van de administratieve kosten een redelijke vergoeding aanrekenen. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt.

4. Het in lid 3 bedoelde recht om een kopie te verkrijgen, doet geen afbreuk aan de rechten en vrijheden van anderen.

Artikel 16 AVG – recht op rectificatie

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken.

Artikel 17 AVG – recht op gegevenswissing

1. De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is:
   a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
   b) de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), berust, in, en er is geen andere rechtsgrond voor de verwerking;
   c) de betrokkene maakt overeenkomstig artikel 21, lid 1, bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking, of de betrokkene maakt bezwaar tegen de verwerking overeenkomstig artikel 21, lid 2;
   d) de persoonsgegevens zijn onrechtmatig verwerkt;
   e) de persoonsgegevens moeten worden gewist om te voldoen aan een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
   f) de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij als bedoeld in artikel 8, lid 1.

2. Wanneer de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt en overeenkomstig lid 1 verplicht is de persoonsgegevens te wissen, neemt hij, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen, waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.

3. De leden 1 en 2 zijn niet van toepassing voor zover verwerking nodig is:
   a) voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
   b) voor het nakomen van een in een het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;

c) om redenen van algemeen belang op het gebied van volksgezondheid overeenkomstig artikel 9, lid 2, punten h) en i), en artikel 9, lid 3;
d) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, voor zover het in lid 1 bedoelde recht de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
e) voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Artikel 21 AVG – recht van bezwaar

1. De betrokkene heeft te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens op basis van artikel 6, lid 1, onder e) of f), van artikel 6, lid 1, met inbegrip van profilering op basis van die bepalingen. De verwerkingsverantwoordelijke staakt de verwerking van de persoonsgegevens tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

2. Wanneer persoonsgegevens ten behoeve van direct marketing worden verwerkt, heeft de betrokkene te allen tijde het recht bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens voor dergelijke marketing, met inbegrip van profilering die betrekking heeft op direct marketing.

3. Wanneer de betrokkene bezwaar maakt tegen verwerking ten behoeve van direct marketing, worden de persoonsgegevens niet meer voor deze doeleinden verwerkt.

4. Het in de leden 1 en 2 bedoelde recht wordt uiterlijk op het moment van het eerste contact met de betrokkene uitdrukkelijk onder de aandacht van de betrokkene gebracht en duidelijk en gescheiden van enige andere informatie weergegeven.

5. In het kader van het gebruik van diensten van de informatiemaatschappij, en niettegenstaande Richtlijn 2002/58/EG, mag de betrokkene zijn recht van bezwaar uitoefenen via geautomatiseerde procedés waarbij wordt gebruikgemaakt van technische specificaties.

6. Wanneer persoonsgegevens overeenkomstig artikel 89, lid 1, met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt, heeft de betrokkene het recht om met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens, tenzij de verwerking noodzakelijk is voor de uitvoering van een taak van algemeen belang.

Artikel 22 AVG - Geautomatiseerde individuele besluitvorming, waaronder profilering

1. De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.

2. Lid 1 geldt niet indien het besluit:
   a) noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
   b) is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
   c) berust op de uitdrukkelijke toestemming van de betrokkene.

3. In de in lid 2, punten a) en c), bedoelde gevallen treft de verwerkingsverantwoordelijke passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene, waaronder ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, het recht om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten.

4. De in lid 2 bedoelde besluiten worden niet gebaseerd op de in artikel 9, lid 1, bedoelde bijzondere categorieën van persoonsgegevens, tenzij artikel 9, lid 2, punt a) of g), van toepassing is en er passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene zijn getroffen.

22.11 Informatiebeveiliging

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 28 AVG (verwerker)

1. Wanneer een verwerking namens een verwerkingsverantwoordelijke wordt verricht, doet de verwerkingsverantwoordelijke uitsluitend een beroep op verwerkers die afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden opdat de verwerking aan de vereisten van deze verordening voldoet en de bescherming van de rechten van de betrokkene is gewaarborgd.

2. De verwerker neemt geen andere verwerker in dienst zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.

3. De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht die de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Die overeenkomst of andere rechtshandeling bepaalt met name dat de verwerker:
   a) de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt;
   b) waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;

c) alle overeenkomstig artikel 32 vereiste maatregelen neemt;
d) aan de in de leden 2 en 4 bedoelde voorwaarden voor het in dienst nemen van een andere verwerker voldoet;
e) rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III vastgestelde rechten van de betrokkene te beantwoorden;
f) rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36;
g) na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;
h) de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt.

Waar het gaat om de eerste alinea, punt h), stelt de verwerker de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

4. Wanneer een verwerker een andere verwerker in dienst neemt om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst of een andere rechtshandeling krachtens Unierecht of lidstatelijk recht dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in de in lid 3 bedoelde overeenkomst of andere rechtshandeling tussen de verwerkingsverantwoordelijke en de verwerker zijn opgenomen, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de verwerking aan het bepaalde in deze verordening voldoet. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de eerste verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker.

5. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat voldoende garanties als bedoeld in de leden 1 en 4 van dit artikel worden geboden.

6. Onverminderd een individuele overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker kan de in de leden 3 en 4 van dit artikel bedoelde overeenkomst of andere rechtshandeling geheel of ten dele gebaseerd zijn op de in de leden 7 en 8 van dit artikel bedoelde standaardcontractbepalingen, ook indien zij deel uitmaken van de certificering die door een verwerkingsverantwoordelijke of verwerker uit hoofde van de artikelen 42 en 43 is verleend.

7. De Commissie kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure standaardcontractbepalingen vaststellen.

8. Een toezichthoudende autoriteit kan voor de in de leden 3 en 4 van dit artikel genoemde aangelegenheden en volgens het in artikel 63 bedoelde coherentiemechanisme standaardcontractbepalingen opstellen.

9. De in de leden 3 en 4 bedoelde overeenkomst of andere rechtshandeling wordt in schriftelijke vorm, waaronder elektronische vorm, opgesteld.

10. Indien een verwerker in strijd met deze verordening de doeleinden en middelen van een verwerking bepaalt, wordt die verwerker onverminderd de artikelen 82, 83 en 84 met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd.

Artikel 32 AVG - Beveiliging van de verwerking

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
   a) de pseudonimisering en versleuteling van persoonsgegevens;
   b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
   c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
   d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

3. Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat dat de in lid 1 van dit artikel bedoelde vereisten worden nageleefd.

4. De verwerkingsverantwoordelijke en de verwerker treffen maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de verwerkingsverantwoordelijke of van de verwerker en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt, tenzij hij daartoe Unierechtelijk of lidstaatrechtelijk is gehouden.

22.12 Bewaren en vernietigen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 5 lid 1 sub e AVG – opslagbeperking

Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen („opslagbeperking").

22.13 Gegevensexport

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 44 AVG

Persoonsgegevens die worden verwerkt of die zijn bestemd om na doorgifte aan een derde land of een internationale organisatie te worden verwerkt, mogen slechts worden doorgegeven indien, onverminderd de overige bepalingen van deze verordening, de verwerkingsverantwoordelijke en de verwerker aan de in dit hoofdstuk neergelegde voorwaarden hebben voldaan; dit geldt ook voor verdere doorgiften van persoonsgegevens vanuit het derde land of een internationale organisatie aan een ander derde land of een andere internationale organisatie. Alle bepalingen van dit hoofdstuk worden toegepast opdat het door deze verordening voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd.

22.14 Meldplicht datalekken

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 33 AVG – mededeling aan de AP

1. 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 overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

2. De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

3. In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:
   a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
   b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
   c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
   d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

5. De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

Artikel 34 AVG – mededeling aan betrokkene

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

2. De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.

3. De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:
   a) de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
   b) de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
   c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

4. Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan.

22.15 Aanstellen functionaris voor gegevensbescherming

Deze eis is gebaseerd op de volgende wettelijke bepaling:

Artikel 37 - Aanwijzing van de functionaris voor gegevensbescherming

1. De verwerkingsverantwoordelijke en de verwerker wijzen een functionaris voor gegevensbescherming aan in elk geval waarin:
   a) de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve in het geval van gerechten bij de uitoefening van hun rechterlijke taken;
   b) een verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen; of
   c) de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens uit hoofde van artikel 9 en van persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10.

2. Een concern kan één functionaris voor gegevensbescherming benoemen, mits de functionaris voor gegevensbescherming vanuit elke vestiging makkelijk te contacteren is.

3. Wanneer de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie of overheidsorgaan is, kan één functionaris voor gegevensbescherming worden aangewezen voor verschillende dergelijke instanties of organen, met inachtneming van hun organisatiestructuur en omvang.

4. In andere dan de in lid 1 bedoelde gevallen kunnen of, indien dat Unierechtelijk of lidstaatrechtelijk is verplicht, moeten de verwerkingsverantwoordelijke of de verwerker of verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen, een functionaris voor gegevensbescherming aanwijzen. De functionaris voor gegevensbescherming kan optreden voor dergelijke verenigingen en andere organen die categorieën van verwerkingsverantwoordelijken of verwerkers vertegenwoordigen.

5. De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen.

6. De functionaris voor gegevensbescherming kan een personeelslid van de verwerkingsverantwoordelijke of de verwerker zijn, of kan de taken op grond van een dienstverleningsovereenkomst verrichten.

7. De verwerkingsverantwoordelijke of de verwerker maakt de contactgegevens van de functionaris voor gegevensbescherming bekend en deelt die mee aan de toezichthoudende autoriteit.

22.16 Registerplicht

Deze eis is gebaseerd op de volgende wettelijke bepaling:

Artikel 30 - Register van de verwerkingsactiviteiten

1. De verwerkingsverantwoordelijken en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens:
   a) de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
   b) de verwerkingsdoeleinden;
   c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
   d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
   e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;

f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

2. De verwerker, en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit register bevat de volgende gegevens:
a) de naam en de contactgegevens van de verwerkers en van iedere verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker en van de functionaris voor gegevensbescherming;
b) de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd;
c) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;
d) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

3. Het in de leden 1 en 2 bedoelde register is in schriftelijke vorm, waaronder in elektronische vorm, opgesteld.

4. Desgevraagd stellen de verwerkingsverantwoordelijke of de verwerker en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker het register ter beschikking van de toezichthoudende autoriteit.

5. De in de leden 1 en 2 bedoelde verplichtingen zijn niet van toepassing op ondernemingen of organisaties die minder dan 250 personen in dienst hebben, tenzij het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of de verwerking bijzondere categorieën van gegevens, als bedoeld in artikel 9, lid 1, of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10 betreft.

Colofon

Leidraad omgaan met persoonsgegevens is
een uitgave van het ministerie van Infrastructuur
en Waterstaat, programma Beter Benutten,
februari 2018

Tekst en inhoud
Considerati, Legal partners in a digital world,
Amsterdam

Ontwerp en vormgeving
Lexenzo, Voorburg

www.beterbenutten.nl/imma