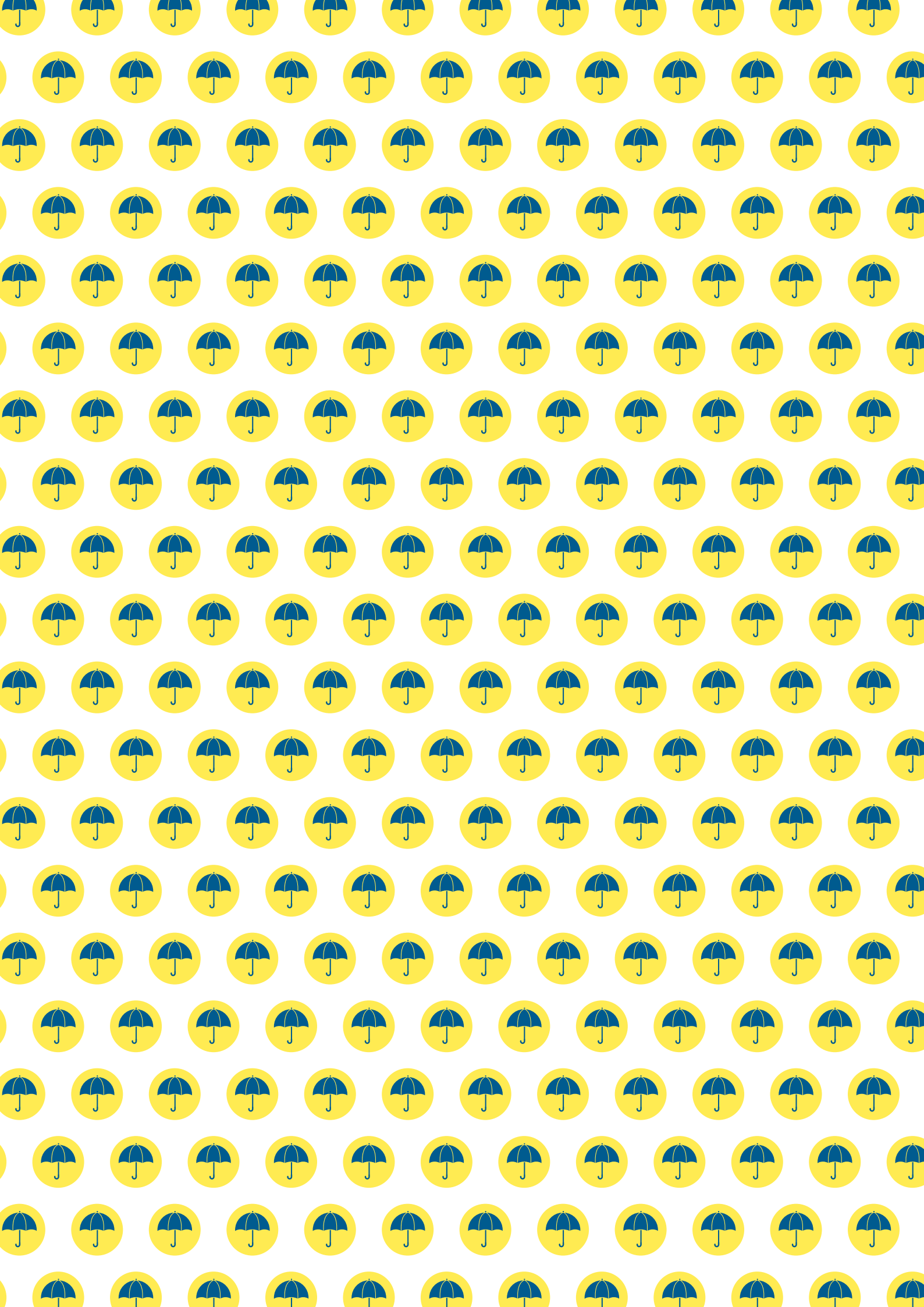
Ministerie van Infrastructuur en Milieu

IMMA Privacy referentiearchitectuur



IMMA Privacy referentiearchitectuur

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 spits-mijden- en fietsstimuleringsprojecten blijkt dat reizigers gevoelig zijn voor deze stimulering. Daarom willen we vanuit het programma Beter Benutten deze vraagbeïnvloedingsprojecten en tegelijkertijd ook verkeersonderzoeken faciliteren met IMMA, de Integrale Mobiliteits-management 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 IMMA Privacy referentiearchitectuur worden de verschillende wettelijke eisen voor privacy overzichtelijk en degelijk uiteengezet, en duidelijk toegelicht. Voorbeelden zorgen voor de vertaling naar uw praktijk. Deze handleiding is in nauwe samenwerking met Considerati tot stand gekomen.

IMMA-projecten bieden de reiziger zo de zekerheid dat zijn privacy optimaal wordt geborgd. Wij wensen u succesvolle IMMA-projecten toe.

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

Inhoudsopgave

2 Achtergrond

Het Programma Beter Benutten van het ministerie van Infrastructuur en Milieu (IenM) wil de ontwikkeling van mobiliteits- en spitsmijdenprojecten faciliteren en de opbrengsten ervan breed inzetbaar maken, binnen de grenzen van de wet. In dat kader wordt de Integrale Mobiliteitsmanagement Architectuur (IMMA) opgesteld. Deze architectuur maakt een meer uniforme, efficiënte en verifieerbare manier van de uitvoering van vraagbeïnvloedings-projecten en verkeersonderzoeken mogelijk. Binnen het juridische kader voor mobiliteits-projecten spelen de verwerking van persoonsgegevens en de eisen van de Wet bescherming persoonsgegevens een belangrijke rol. Om te borgen dat nieuw te ontwikkelen projecten ook in overeenstemming zijn met geldende privacy wet- en regelgeving is, als onderdeel van de IMMA, deze privacy referentiearchitectuur opgesteld. Uitgangspunt moet zijn dat de dienstaanbieders van mobiliteits- en spitsmijdenprojecten gegevensbescherming gaan zien als een license to operate.

Deze referentiearchitectuur geeft de ‘baseline’ waaraan projecten moeten voldoen om privacy compliant te zijn. Concreet betekent dit dat de privacy referentiearchitectuur privacyprincipes, standaarden en eisen formuleert waaraan mobiliteits- en spitsmijdenprojecten dienen te voldoen op basis van het geldende wettelijk kader (Wet bescherming persoonsgegevens, aankomende Europese Algemene Verordening Gegevensbescherming en de Cookiewet).

Het is van belang te vermelden dat de IMMA Privacy referentiearchitectuur géén nieuwe eisen stelt die niet reeds op grond van de wet aan projecten en applicaties worden gesteld. De referentiearchitectuur dient enkel ter verduidelijking van de plichten. Ook schetst de architectuur slechts een kader en schrijft het geen concrete maatregelen voor, dit is namelijk altijd ter beoordeling van de verantwoordelijke op basis van de concrete toepassing. De verantwoordelijke moet met alle gestelde eisen rekening houden en kunnen verantwoor-den waarom bepaalde keuzes met betrekking tot het invullen van deze eisen zijn gemaakt.

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

3 Begrippenlijst

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 fleet management).

Bewerker

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

AP

Autoriteit Persoonsgegevens, de toezichthouder op de naleving van de Wet bescherming persoonsgegevens.

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.

Derde

Degene die niet de betrokkene, de verantwoordelijke of de bewerker is.

Ontvanger
De derde aan wie persoonsgegevens worden doorgegeven.

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Geïdentificeerd houdt in dat een natuurlijk persoon uniek te onderscheiden is van andere personen op basis van identificerende gegevens (bijvoorbeeld NAW), of dat de persoon geïndividualiseerd kan worden binnen een groep (to single out).

Identificeerbaar betekent dat een persoon nog niet geïdentificeerd is, maar dat identificatie door de verantwoordelijke en/of derden redelijkerwijs mogelijk is.

Verantwoordelijke
De natuurlijke persoon, rechtspersoon of ieder ander die, of het bestuursorgaan dat, alleen of tezamen 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.

Wbp
De Wet bescherming persoonsgegevens. De nationale uitwerking van de Europese richtlijn 95/46/EC die toeziet op bescherming van persoonsgegevens.

4 Algemene toelichting privacywetgeving

Voor IMMA zijn op het gebied van privacy twee wetten van belang: de Wet bescherming persoonsgegevens (Wbp) en de zogenoemde Cookiewet. De Wbp 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 Wet bescherming persoonsgegevens en de 'Cookiewet'.

4.1 Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens bepaalt wanneer persoonsgegevens mogen worden verwerkt. Kern van de wet is 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 Wet bescherming persoonsgegevens (zie artikel 8 Wbp).

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

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

4.2 Algemene Verordening Gegevensbescherming

Binnen de Europese Unie wordt momenteel gewerkt aan de opvolger van de Wet bescherming persoonsgegevens: de Algemene Verordening Gegevensbescherming. Deze wet stelt een aantal strengere eisen aan de verantwoordelijke, met name op het gebied van controle en verantwoordelijkheid (accountability). Omdat deze wet nog niet definitief is vastgesteld worden deze nieuwe eisen nog niet meegenomen in deze referentiearchitectuur. Wel wordt, waar relevant, alvast vooruitgeblikt naar de eisen van de Verordening zodat u daarop kunt anticiperen.

4.3 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.

[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 Privacy by Design

In de toekomst zal de Europese Algemene Verordening Gegevensbescherming de Wet bescherming persoonsgegevens opvolgen. Op basis van deze verordening moet al in het ontwerp van IT-systemen en bedrijfsprocessen rekening gehouden worden met privacybescherming.

Op basis van de aankomende Europese Algemene Verordening Gegevensbescherming moeten alle toepassingen waarbij persoonsgegevens worden verwerkt ‘Privacy by Design’ zijn. Dit houdt in dat in het ontwerp van IT systemen en bedrijfsprocessen rekening wordt gehouden met privacy.

Het uitgangspunt voor IMMA projecten is dat de eisen uit de privacy referentiearchitectuur, zoals hieronder beschreven, mee worden genomen in het ontwerp van IMMA toepassingen.

Om zicht te krijgen op de risico’s van uw toepassing, kunt u een Privacy Impact Assessment (PIA) doen of laten doen. Op basis van de uitkomsten van de PIA kunt u de benodigde maatregelen op het gebied van Privacy by Design nemen. Met de Verordening worden PIAs in de toekomst verplicht voor meer risicovolle toepassingen.

6 Overzicht IMMA privacy eisen

Elk IMMA-project moet op het gebied van privacy en de bescherming van persoonsgegevens invulling geven aan elf eisen. Denk bijvoorbeeld aan eisen voor verantwoordelijkheid, dataminimalisatie en eisen voor het bewaren en vernietigen van persoonsgegevens. In dit hoofdstuk zetten we de 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:

6.1 Verantwoordelijkheid

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

6.2 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 uit de Wbp (artikel 8 Wbp).
- Wanneer ondubbelzinnige toestemming (artikel 8a Wbp) 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.

6.3 Dataminimalisatie

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

6.4 Doelbinding

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

6.5 Informatie en transparantie

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

6.6 Delen van gegevens met derden

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

6.7 Rechten van de betrokkene

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

6.8 Informatiebeveiliging

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

6.9 Bewaren en vernietigen

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

6.10 Gegevensexport

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

6.11 Meldplicht datalekken

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

7 Verantwoordelijkheid

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

7.1 Eis

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

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

7.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:
- Artikel 1 onder d Wet bescherming persoonsgegevens
- Artikel 4 Wet bescherming persoonsgegevens
- Artikel 14 Wet bescherming persoonsgegevens

7.3 Toelichting

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

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

Nota bene: De verantwoordelijke is niet een individu binnen een organisatie, maar de organisatie (de rechtspersoon) zelf.

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

Bewerkers

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

7.4 Voorbeelden

Voorbeeld 1

SnellerThuis BV ontwikkelt een spitsmijden applicatie 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 verantwoordelijke: 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 Wbp, GoedeHost BV is een bewerker.

Voorbeeld 2

Een voorbeeld van een privacy policy waarin de verantwoordelijke 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 verantwoordelijke 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 verantwoordelijke duidelijk vastgesteld, maar ook de bewerker 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 nieuwe app van vervoersmaatschappij Syntus 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 verantwoordelijke is en zijn ook hun contactgegevens en KvK-nummer 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.

8 Legitiem doel en grondslag

De Wet bescherming persoonsgegevens schrijft voor dat u persoonsgegevens alleen mag verwerken met een vooraf vastgesteld en duidelijk omschreven doel. Bovendien moet de verwerking gebaseerd zijn op wettelijke grondslagen, zoals het geven van toestemming of een duidelijke noodzaak voor de uitvoering van een overeenkomst. In dit hoofdstuk worden de verschillende grondslagen beschreven en toegelicht. Zo 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 men in de praktijk toestemming voor verwerking van persoons-gegevens regelt en een doel duidelijk omschrijft.

8.1 Eis

- ***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 zijn op één van de grondslagen uit de Wbp (artikel 8 Wbp).***

- ***Wanneer ondubbelzinnige toestemming (artikel 8a Wbp) 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.***

8.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 7 Wet bescherming persoonsgegevens
- Artikel 8 sub a en sub f Wet bescherming persoonsgegevens
- 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 gegevens 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 men zich moet afvragen of het doel ook bereikt kan worden met minder gegevens 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 8 Wbp. Kan de verwerking niét gerechtvaardigd worden op basis van één van deze doelen, dan is zij niét toegestaan.

De zes grondslagen zijn:

a) De betrokkene heeft zijn/haar ondubbelzinnige toestemming gegeven.
b) De verwerking is noodzakelijk om de overeenkomst met de betrokkene uit te voeren.
c) De verwerking is noodzakelijk om te voldoen aan een wettelijke plicht die op de verantwoordelijke rust.
d) De verwerking is noodzakelijk om de vitale belangen van de betrokkene te waarborgen.
e) De verwerking is noodzakelijk voor de verantwoordelijke om diens publiekrechtelijke taak uit te voeren.
f) De verwerking is noodzakelijk om een gerechtvaardigd belang van de verantwoordelijke te waarborgen dat zwaarder weegt dan de privacy inbreuk bij de betrokkene.

Voor IMMA projecten zullen met name 8a Wbp, 8b Wbp en 8f Wbp relevant zijn.[2]

8a Wbp: Ondubbelzinnige toestemming van de betrokkene

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

[2] De grondslag 'wettelijke plicht' heeft betrekking op een wettelijke plicht die rust op de verantwoordelijke, zoals bijvoorbeeld 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 'uitvoering van de publiekrechtelijke taak' kan alleen worden gebruikt door publiekrechtelijke organisaties zoals ministeries en uitvoeringsinstanties.

Als u gebruik maakt van ondubbelzinnige 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. Bijvoorbeeld “wij verwerken uw gegevens voor onze goede bedrijfsvoering en het verbeteren van de mobiliteit in Nederland” 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 bewijslast voor het verkregen hebben van de toestemming en voor de kennisname door betrokkene van de verstrekte informatie ligt bij u als verantwoordelijke. 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 was 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 verantwoordelijke dan géén grondslag meer hebt om de persoonsgegevens van deze betrokkene te verwerken. Concreet betekent dit dat u niet langer de gegevens 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 Tw: 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.

8b Wbp: 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.

8f Wbp: 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 privacy belang 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.

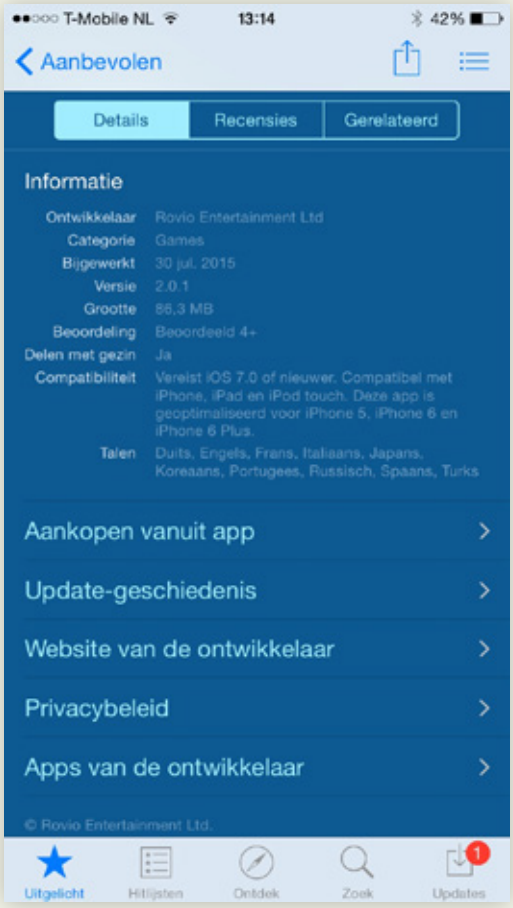
Ook dient de verwerking noodzakelijk te zijn ter behartiging van uw belang. Dit houdt in dat uw belangen niet op een andere manier, met minder ingrijpende middelen of met minder gegevens, kan worden gediend (subsidiariteit).

[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.

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

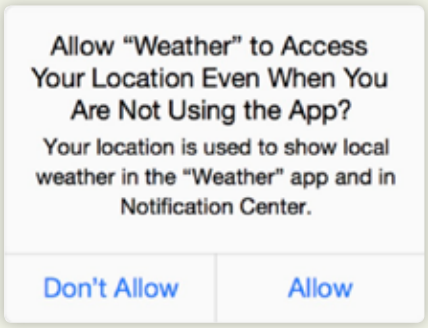


Voorbeeld 1 (toestemming)

Screenshot van de Apple 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 informatievereiste, 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 gegevens worden verwerkt. De app 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 is te vinden bij de aanmelding op de website voor het spitsmijdenproject Spitsmijden Galecopperbrug.

Bij aanmelding wordt kort uitgelegd voor welk doel de gevraagde informatie in het aanmeldingsformulier nodig is.

Voorbeeld 5 (toestemming)
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 spitsmijdenproject."

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 Wet bescherming persoonsgegevens is niet van toepassing op anonieme 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 bepalingen:

- Artikel 11 lid 1 Wet bescherming persoonsgegevens

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 niét 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 gegevens ook de concepten anonimisering en pseudonimisering relevant.

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 Wbp schrijft echter geen specifieke techniek voor. De optimale keuze dient per casus te worden bepaald.

Bij volledige anonimisering wordt voldaan aan de volgende 3 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 Wbp 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 verantwoordelijke mogelijk is om het proces weer om te draaien (de verantwoordelijke heeft de 'sleutel'). Pseudonimisering is dus niét 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. Gezien voor dit doel het niet nodig is om gegevens te hebben die te herleiden zijn naar een persoon, heeft MyOV 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.

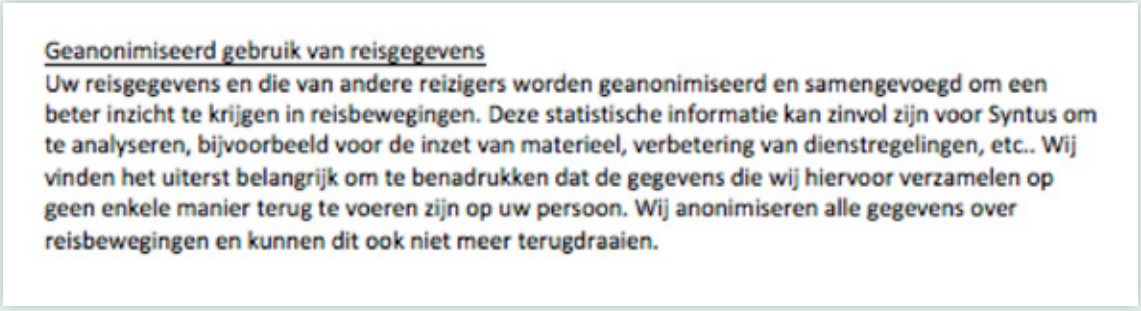
Uw reisgegevens zijn ook nodig om uw **restitutieaanvragen bij een vergeten check out of geld terug bij vertraging te kunnen verwerken.**

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 gebruikt ook deze reisgegevens om inzicht te krijgen in reisbewegingen. Aangezien voor dit doel het niet nodig is om gegevens te hebben die te herleiden zijn naar een persoon, heeft Syntus 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 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 persoonsgegevens en de gevolgen van verdere verwerking voor de gebruiker. In dit hoofdstuk komen vijf factoren voor een goede beoordeling aan de orde.

10.1 Eis

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

10.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 7 Wet bescherming persoonsgegevens
- Artikel 9 lid 1 en 2 Wet bescherming persoonsgegevens
- Artikel 11 lid 1 Wet bescherming persoonsgegevens

10.3 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 men 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, moeten alle relevante omstandigheden van het geval worden meegewogen. 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 gegevens zijn verzameld;

- De context waarin de gegevens zijn verzameld en de redelijke verwachting van de betrokkene over het verdere gebruik van zijn gegevens;

- De aard van de gegevens. Hoe gevoeliger de gegevens voor de betrokkene zijn, hoe minder snel u mag aannemen dat deze gegevens 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;

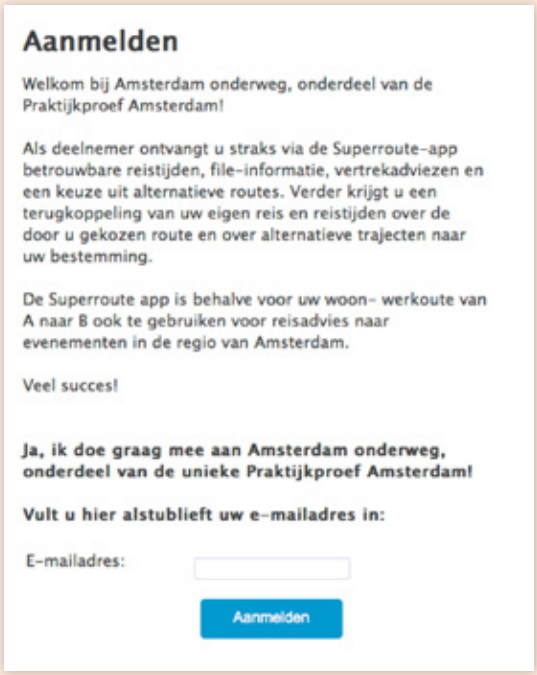
- De waarborgen die zijn gerealiseerd door de verantwoordelijke om te borgen dat de gegevens op een behoorlijke en zorgvuldige wijze worden verwerkt en die onnodige impact op de betrokkene voorkomen.

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

10.4 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.



Vooreeld 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 voor marketingdoeleinden.

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.

11 Informatie en transparantie

De Wet bescherming persoonsgegevens 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.

11.1 Eis

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

11.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 33 Wet bescherming persoonsgegevens
- Artikel 34 Wet bescherming persoonsgegevens
- Artikel 11.7a Telecommunicatiewet

11.3 Toelichting

De betrokkene moet vooraf volledig worden geïnformeerd over wat u met de gegevens 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 verantwoordelijke is;
- wat de doelen van de toepassing zijn;
- welke gegevens worden verwerkt;
- waarvoor de gegevens worden gebruikt;
- derden aan wie u gegevens verstrekt;
- hoe lang de gegevens worden bewaard;
- hoe de betrokkene zijn rechten kan uitoefenen (zie hoofdstuk 13).

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 een 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 gelaagde privacy statement. Houd ook rekening met het type apparaat. Zo is een link naar een privacy statement op een website vaak niet goed leesbaar op het kleinere scherm van een smartphone.

Afzonderlijk regime voor cookies en soortgelijke technieken

Indien 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 worden geplaatst;
- de soorten persoonsgegevens die via de cookies worden verzameld en verwerkt;
- de doeleinden van de gegevensverwerking;
- derden aan wie u de gegevens verstrekt;
- de levensduur van de cookie.[4]

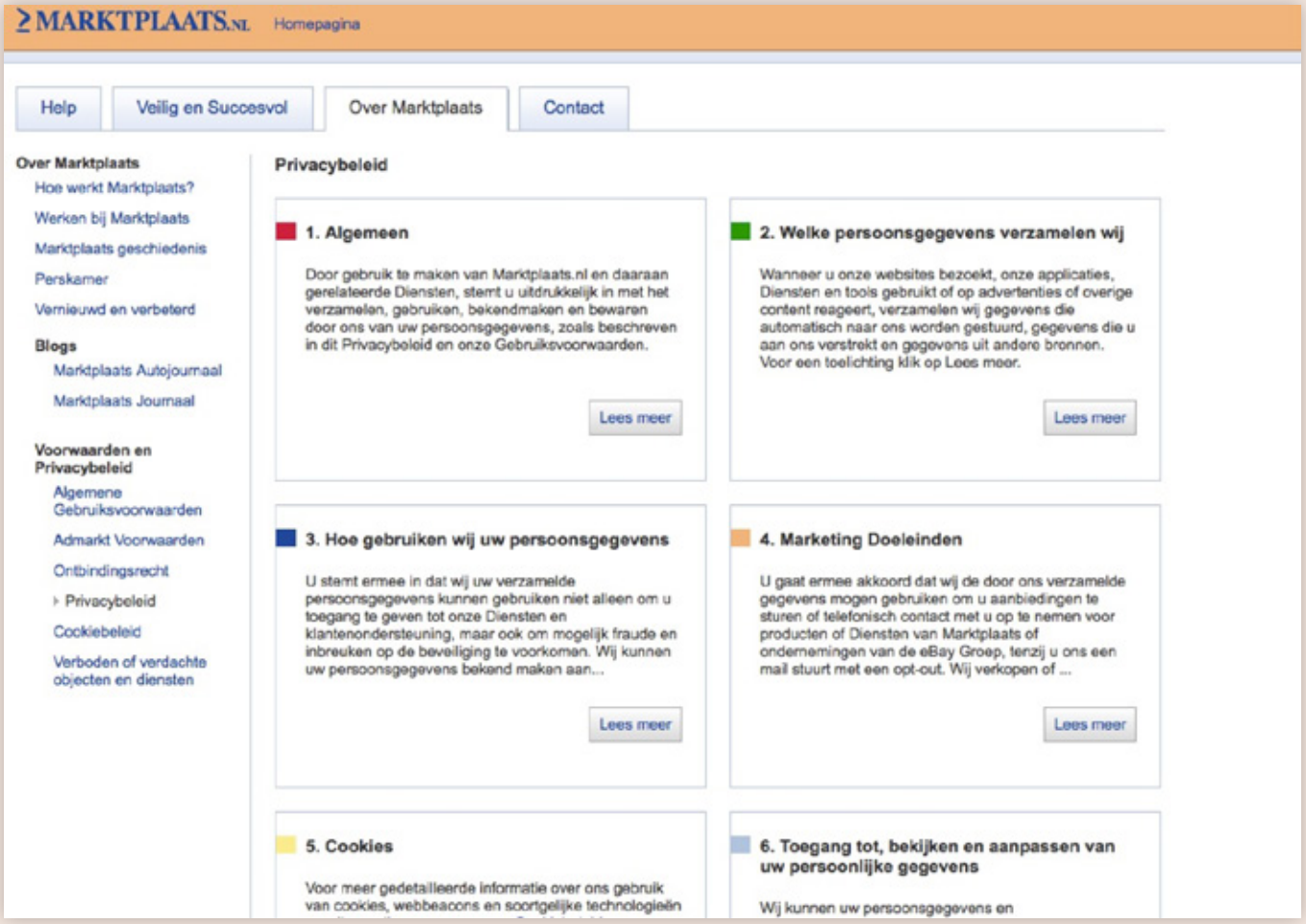
Voor wat betreft het plaatsen van cookies of soortgelijke technieken bestaan drie uitzonderingen op de informatieplicht. Over het gebruik van strikt noodzakelijke technische cookies, functionele cookies waar de gebruiker om gevraagd heeft en analyse cookies met een geringe invloed op de privacy hoeft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

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

11.4 Voorbeelden

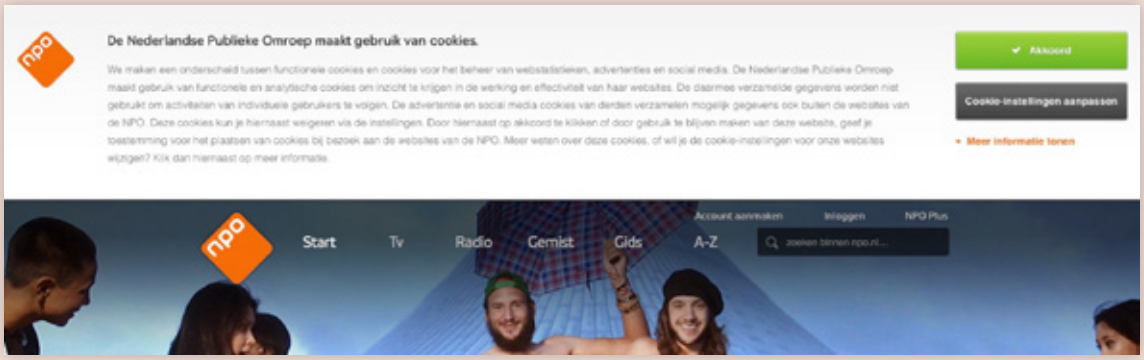
Voorbeeld 1

Een voorbeeld van een gelaagde privacy statement. De blokjes geven op hoofdlijnen weer wat er gebeurt met de gegevens, onder ‘lees meer’ is uitgebreide informatie te vinden.



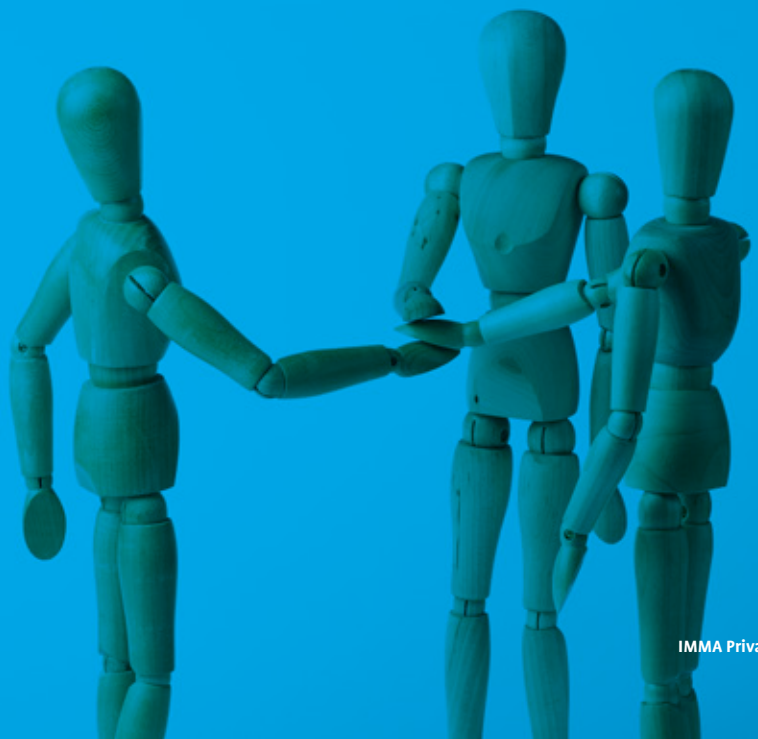
Voorbeeld 2

Voorbeeld van een cookiemelding (NPO). De doelen worden duidelijk aangegeven en er is een mogelijkheid om advertentiecookies te weigeren.



12 Delen van persoonsgegevens met derden

Voor het delen van persoonsgegevens met derden is een wettelijke grondslag nodig. Zo kan artikel 8c van de Wet bescherming persoonsgegevens 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.



12.1 Eis

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

12.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

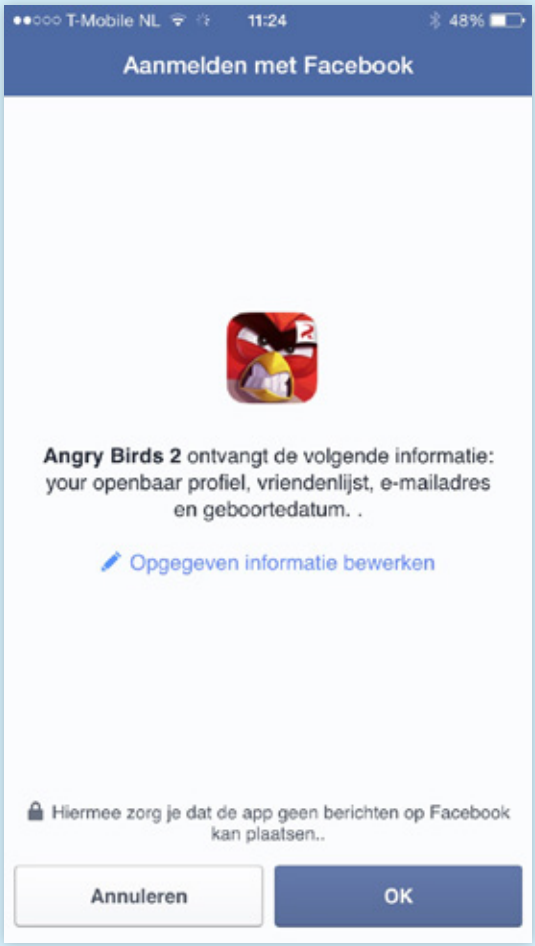
- Artikel 8 Wet bescherming persoonsgegevens
- Artikel 17 lid 3 Wet bescherming persoonsgegevens
- Artikel 19 lid 2 Wet bescherming persoonsgegevens
- Artikel 20 lid 2 Wet bescherming persoonsgegevens

12.3 Toelichting

Omdat het delen van gegevens 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 8b Wbp. Wanneer er een wettelijke plicht rust op de verantwoordelijke, dan kan 8c Wbp als grondslag dienen. In de meeste gevallen zal voor verstrekking aan derden echter toestemming nodig zijn van de betrokkene (8a Wbp).

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 gegevens doorgestuurd kunnen worden naar deze derden. Zorg dat u afspraken maakt met uw app bouwer over het gebruik van dit soort componenten en controleer welke gegevens worden uitgewisseld via plug-ins en API's.

12.4 Voorbeeld



Voorbeeld 1

Wanneer een gebruiker de Facebookknop in Angry Birds 2 gebruikt worden allerlei gegevens gedeeld tussen Rovio en Facebook. De gebruiker moet hiervoor zijn toestemming geven.

Voorbeeld 2

De Syntus app heeft duidelijk in zijn privacy policy aangegeven dat gegevens in principe niet aan derden worden doorgegeven. Indien gegevens wel aan derden worden gegeven, zorgt Syntus ervoor dat dit op een rechtmatige grondslag is gebaseerd: ofwel expliciete toestemming van de gebruiker (art. 8a Wbp) ofwel het voldoen aan een wettelijk voorschrift (art. 8c Wbp).

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.

13 Rechten van betrokkene

Als persoonsgegevens van een gebruiker worden verwerkt, heeft hij recht op inzage, recht op correctie en in sommige gevallen recht van verzet. Op basis van deze rechten kan hij zich verweren tegen onjuiste of incomplete persoonsgegevens. In dit hoofdstuk beschrijven we hoe u een inzageverzoek en een correctieverzoek goed kunt afhandelen. En hoe u een verzet tegen het verwerken van persoonsgegevens moet beoordelen en afhandelen. Een voorbeeld laat zien hoe een heldere inzageprocedure eruit kan zien.

13.1 Eis

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

13.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 35 Wet bescherming persoonsgegevens
- Artikel 36 Wet bescherming persoonsgegevens
- Artikel 40 Wet bescherming persoonsgegevens

13.3 Toelichting

De betrokkene heeft bepaalde rechten met betrekking tot de verwerking van zijn persoonsgegevens. Dit is om te borgen dat de betrokkene weet welke gegevens over hem verwerkt worden, hij zich kan verweren tegen onjuiste of incomplete gegevens en ervoor kan zorgen dat gegevens die niet meer relevant zijn, verwijderd worden.

Recht op inzage

De betrokkene heeft het recht op inzage in zijn persoonsgegevens. Een betrokkene 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) kan bij een verzoek om een ID worden gevraagd. Geef wel aan bij de betrokkene dat deze zijn pasfoto, BSN en MRZ (de onderste rij getallen en letters op een paspoort) moet doorstrepen, omdat deze gevoelige gegevens niet noodzakelijk zijn voor de identificatie.

Een inzageverzoek moet binnen vier weken schriftelijk worden beantwoord.

De beantwoording van het verzoek moet de volgende onderdelen bevatten:
- Een volledig overzicht van de verwerkte gegevens van de betrokkene
- Een omschrijving van:
  - het doel van de gegevensverwerking;
  - de categorieën van gegevens waarop de verwerking betrekking heeft;
  - de ontvangers of categorieën van ontvangers.
- Alle beschikbare informatie over de herkomst van de gegevens.

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

U moet de gegevens verstrekken in 'begrijpelijke vorm'. U moet dus kunnen duiden welke gegevens het betreft en hoe ze worden gebruikt. Wat 'begrijpelijk' is, is afhankelijk 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 voor de gebruiker.

Het is niet uit te sluiten dat een inzage in gegevens ook enig inzicht kan geven in gegevens die op anderen betrekking hebben. U moet als verantwoordelijke dan, op het moment dat u redelijkerwijs kan verwachten dat een derde bedenkingen zal hebben, deze derde op de hoogte stellen van het verzoek tot inzage.

Op het moment dat de inzage ook inzicht geeft in gegevens van derden, zal u als verantwoordelijke een belangenafweging moeten maken. U kunt eventueel een inzage weigeren met een beroep op art. 43 sub e Wbp (noodzakelijk in het belang van de bescherming van rechten en vrijheden van anderen).

Recht op correctie

Ook kan een betrokkene verzoeken de gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Dit verzoek moet binnen 4 weken schriftelijk worden beantwoord.
Een dergelijk verzoek hoeft alleen te worden ingewilligd als de gegevens feitelijk onjuist zijn, onvolledig of niet ter zake dienend zijn voor het doel van de verwerking of op andere wijze in strijd met een voorschrift van de Wbp of een andere wet zijn verwerkt.

Recht van verzet

Indien de verwerking is gebaseerd op de grondslag ‘noodzakelijk ter behartiging van het gerechtvaardigd belang van de verantwoordelijke’, heeft de betrokkene het recht bezwaar te maken tegen de gegevensverwerking in verband met bijzondere persoonlijke omstandigheden. Dit bezwaar moet worden beoordeeld en indien het bezwaar terecht is, dient de verwerking van de gegevens van de betrokkene te worden beëindigd. Kijk bij deze toetsing nogmaals naar hoe u zaken als proportionaliteit, subsidiariteit en privacybeschermende maatregelen heeft vormgegeven.

13.4 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.

14 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 bewerkersovereenkomsten.

14.1 Eis

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

14.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 13 Wet bescherming persoonsgegevens
- Artikel 14 Wet bescherming persoonsgegevens

14.3 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 gegevens 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.[5]

De AP heeft richtsnoeren voor de beveiliging van persoonsgegevens opgesteld die een kader bieden voor het goed beveiligen van persoonsgegevens.[6] De AP heeft echter geen standaard vastgesteld voor de beveiliging, daarvoor zijn de ISO-standaarden.

5 Zie: **http://www.iso.org/iso/home/standards/management-standards/iso27001.htm** en **https://www.pcisecuritystandards.org**

6 Zie: **http://wetten.overheid.nl/BWBR0033572/geldigheidsdatum_02-07-2015**

Bewerkersovereenkomst

Indien u gebruik maakt van een bewerker, moet u met deze partij een bewerkersovereenkomst afsluiten waarin u vastlegt dat de bewerker:

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

14.4 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 gegevens 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 gegevens 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%. 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 beveiligings-inbreuk moet worden gemeld bij de toezichthouder.

Beveiligingsbewustzijn
Een goede beveiliging valt en staat 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 er bij welke data? Zorg daarom dat u een helder autorisatiebeleid heeft.

Netwerkbeveiliging
Zorg ervoor dat uw netwerk beschermd is tegen aanvallers. Denk hierbij aan anti-virus software en firewalls. Bij meer risicovolle gegevens kunt u denken aan intrusion detection systemen (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.

15 Bewaren en vernietigen

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 bewaartermijnen ook in het privacy statement.

15.1 Eis

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

15.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 10 Wet bescherming persoonsgegevens

15.3 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 gegevens te bewaren, moeten de gegevens verwijderd worden of alle identificerende kenmerken worden verwijderd (anonimiseren). Vermeld ook de bewaartermijnen in uw privacy statement.

15.4 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

De privacy policy 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.

16 Gegevensexport

Persoonsgegevens mag u niet naar landen versturen waar geen goede privacywetgeving 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 is toestemming van de gebruiker nodig of een vergunning van de Autoriteit Persoons-gegevens, of kunt u gebruikmaken van 'standaard contractuele bepalingen'.

16.1 Eis

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

16.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 76 Wet bescherming persoonsgegevens

16.3 Toelichting

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

1. de landen binnen de Europese Economische Ruimte;
2. landen die volgens de Europese Commissie een adequaat niveau van bescherming bieden.

Ad 1)
De Europese Economische Ruimte bestaat uit de lidstaten van de Europese Unie plus IJsland, Noorwegen en Liechtenstein.

Ad 2)
Landen die ten tijde van de publicatie van deze referentiearchitectuur een adequaat niveau van bescherming bieden zijn: Andorra, Argentinië, Canada, Zwitserland, de Faeröer eilanden, Guernsey, Israël, the Isle of Man, Jersey, Uruguay en Nieuw Zeeland.

De Verenigde Staten kennen momenteel geen adequaat niveau van privacybescherming, doordat het Europees Hof van Justitie op 6 oktober 2015 de Safe Harbor- regels ongeldig heeft verklaard. Organisaties die zich aan deze regels hadden gecommitteerd werden geacht een adequaat niveau van privacybescherming te bieden. De VS en de EU zijn bezig met het uitwerken van de opvolger van de Safe Harbor-regels: het EU-US Privacy Shield.

Indien een land geen adequaat niveau van bescherming biedt en u wilt toch gegevens in dat land laten verwerken, dan moet u gebruikmaken van één van de uitzonderingen die artikel 77 Wbp biedt. De belangrijkste uitzonderingen zijn de toestemming van de betrokkene, of het hebben van een vergunning voor de export.

Een exportvergunning vraagt u aan bij de AP. U hoeft geen vergunning aan te vragen als u gebruikmaakt van zogenaamde 'standaard contractuele bepalingen'. Deze bepalingen in het contract met een andere verantwoordelijke of een bewerker zijn erop gericht om de privacy van de betrokkene te waarborgen. Als deze contractuele bepalingen zijn opgenomen, dan mogen de gegevens ook worden doorgestuurd.[7]

16.4 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://www.cbpweb.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu**

17 Meldplicht datalekken

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

17.1 Eis

De verantwoordelijke 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 verantwoordelijke stelt ook de betrokkene op de hoogte van bovengenoemde beveiligingsinbreuk indien deze waarschijnlijk ongunstige gevolgen heeft voor diens persoonlijke levenssfeer.

17.2 Wettelijke bepalingen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

- Artikel 34a Wet bescherming persoonsgegevens

17.3 Toelichting

Melding aan de Autoriteit Persoonsgegevens
U dient ervoor te zorgen dat u zo snel mogelijk en zo mogelijk binnen 72 uur een melding doet bij de Autoriteit Persoonsgegevens indien u een ernstig datalek heeft. 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.

U hoeft alleen een datalek te melden indien 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.
Indien u geen gebruik kunt maken van het webformulier, kunt u de melding ook per fax aan de AP sturen.

Melding aan de betrokkene
Als u een datalek moet melden aan de AP, moet u afwegen of dit datalek ook aan de betrokkene moet worden gemeld. U bent verplicht het datalek onverwijld te melden aan de betrokkene indien het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens 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 de betrokkene maatregelen nemen om zichzelf te beschermen tegen de gevolgen van het datalek. Daarom moet u zo snel mogelijk de betrokkene informeren, zodat deze zo snel mogelijk actie kan ondernemen om zichzelf te beschermen.

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

In de melding aan de betrokkene moet u in ieder geval het volgende 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 een beveiligingsincident aan de AP en eventueel ook aan de betrokkene moet worden gemeld. Deze beleidsregels zijn op de website van de AP terug te vinden.[8]

17.4 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 webformulier. Ook informeert SnellerThuis BV alle gebruikers over dit datalek en geeft daarbij aan dat de gebruiker zijn wachtwoord moet 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 inloggegegevens 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.

[8] Voor meer informatie zie: **https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf**

18 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 per hoofdstuk opgenomen.

1. Verantwoordelijkheid

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 1d Wet bescherming persoonsgegevens

Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Artikel 4 Wet bescherming persoonsgegevens

1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland.

2. Deze wet is van toepassing op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens.

3. Het is een verantwoordelijke als bedoeld in het tweede lid, verboden persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem han-

delt overeenkomstig de bepalingen van deze wet. Voor de toepassing van deze wet en de daarop berustende bepalingen, wordt hij aangemerkt als de verantwoordelijke.

Artikel 14 Wet bescherming persoonsgegevens

1. Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen, en ten aanzien van de melding van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt. De verantwoordelijke ziet toe op de naleving van die maatregelen.

2. De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.

3. De verantwoordelijke draagt zorg dat de bewerker:
   a. de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid;
   b. de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13, en
   c. de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplichting tot melding van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt.

4. Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b en c.

5. Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, de beveiligingsmaatregelen, bedoeld in artikel 13, en de verplichting tot melding van een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt, schriftelijk of in een andere, gelijkwaardige vorm vastgelegd.

2. Legitiem doel en grondslag

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 7 Wet bescherming persoonsgegevens

Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld.

Artikel 8 sub a en sub f Wet bescherming persoonsgegevens

Persoonsgegevens mogen slechts worden verwerkt indien:

a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

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.

3. Dataminimalisatie

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 11 lid 1 Wet bescherming persoonsgegevens

Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.

4. Doelbinding

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 7 Wet bescherming persoonsgegevens

Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld.

Artikel 9 lid 1 en 2 Wet bescherming persoonsgegevens

1. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

2. Bij de beoordeling of een verwerking onverenigbaar is als bedoeld in het eerste lid, houdt de verantwoordelijke in elk geval rekening met:
   a. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
   b. de aard van de betreffende gegevens;
   c. de gevolgen van de beoogde verwerking voor de betrokkene;
   d. de wijze waarop de gegevens zijn verkregen en
   e. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

Artikel 11 lid 1 Wet bescherming persoonsgegevens

Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.

5. Informatie en transparantie

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 33 Wet bescherming persoonsgegevens

1. Indien persoonsgegevens worden verkregen bij de betrokkene, deelt de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij de betrokkene daarvan reeds op de hoogte is.

2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, mede.

3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Artikel 34 Wet bescherming persoonsgegevens

1. Indien persoonsgegevens worden verkregen op een andere wijze dan bedoeld in artikel 33, deelt de verantwoordelijke de betrokkene de informatie mede, bedoeld in het tweede en derde lid, tenzij deze reeds daarvan op de hoogte is:
   a. op het moment van vastlegging van hem betreffende gegevens, of
   b. wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.

2. De verantwoordelijke deelt de betrokkene zijn identiteit en de doeleinden van de verwerking mede.

3. De verantwoordelijke verstrekt nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

4. Het eerste lid is niet van toepassing indien mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval legt de verantwoordelijke de herkomst van de gegevens vast.

5. Het eerste lid is evenmin van toepassing indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid.

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.

6. Delen van persoonsgegevens met derden

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 8 sub a en sub f Wet bescherming persoonsgegevens

Persoonsgegevens mogen slechts worden verwerkt indien:

a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Artikel 17 lid 3 Wet bescherming persoonsgegevens

1. Het verbod om persoonsgegevens betreffende iemands godsdienst of levensovertuiging te verwerken als bedoeld in artikel 16, is niet van toepassing indien de verwerking geschiedt door:
    a. kerkgenootschappen, zelfstandige onderdelen daarvan of andere genootschappen op geestelijke grondslag voor zover het gaat om gegevens van daartoe behorende personen;
    b. instellingen op godsdienstige of levensbeschouwelijke grondslag, voor zover dit gelet op het doel van de instelling en voor de verwezenlijking van haar grondslag noodzakelijk is, of
    c. andere instellingen voor zover dit noodzakelijk is met het oog op de geestelijke verzorging van de betrokkene, tenzij deze daartegen schriftelijk bezwaar heeft gemaakt.

2. In de gevallen als bedoeld in het eerste lid, onder a, is het verbod tevens niet van toepassing op persoonsgegevens betreffende godsdienst of levensovertuiging van de gezinsleden van de betrokkene voor zover:
   a. het betreffende genootschap met die gezinsleden uit hoofde van haar doelstelling regelmatige contacten onderhoudt en
   b. die gezinsleden daartegen geen schriftelijk bezwaar hebben gemaakt.

3. **In de gevallen als bedoeld in het eerste en tweede lid worden geen persoonsgegevens aan derden verstrekt zonder toestemming van de betrokkene.**

Artikel 19 lid 2 Wet bescherming persoonsgegevens

1. Het verbod om persoonsgegevens betreffende iemands politieke gezindheid te verwerken als bedoeld in artikel 16, is niet van toepassing indien de verwerking geschiedt:
   a. door instellingen op politieke grondslag betreffende hun leden of hun werknemers dan wel andere tot de instelling behorende personen, voor zover dit gelet op het doel van de instelling noodzakelijk is voor de verwezenlijking van haar grondslag, of
   b. met het oog op de eisen die met betrekking tot politieke gezindheid in redelijkheid kunnen worden gesteld in verband met de vervulling van functies in bestuursorganen en adviescolleges.

2. **In het geval als bedoeld in het eerste lid, onder a, worden geen persoonsgegevens aan derden verstrekt zonder toestemming van de betrokkene.**

Artikel 20 lid 2 Wet bescherming persoonsgegevens

1. Het verbod om persoonsgegevens betreffende iemands lidmaatschap van een vakbond te verwerken als bedoeld in artikel 16, is niet van toepassing indien de verwerking geschiedt door de betreffende vakbond of de vakcentrale waarvan die bond een onderdeel vormt, voor zover dat gelet op de doelstelling van de vakbond of centrale noodzakelijk is.

2. **In het geval als bedoeld in het eerste lid worden geen persoonsgegevens aan derden verstrekt zonder toestemming van de betrokkene.**

7. Rechten van de betrokkene

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 35 Wet bescherming persoonsgegevens

1. De betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt.

2. Indien zodanige gegevens worden verwerkt, bevat de mededeling een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van het doel of de doeleinden van de verwerking, de categorieën van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede de beschikbare informatie over de herkomst van de gegevens.

3. Voordat een verantwoordelijke een mededeling doet als bedoeld in het eerste lid, waartegen een derde naar verwachting bedenkingen zal hebben, stelt hij die derde in de gelegenheid zijn zienswijze naar voren te brengen indien de mededeling gegevens bevat die hem betreffen, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost.

4. Desgevraagd doet de verantwoordelijke mededelingen omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.

Artikel 36 Wet bescherming persoonsgegevens

1. Degene aan wie overeenkomstig artikel 35 kennis is gegeven van hem betreffende persoonsgegevens, kan de verantwoordelijke verzoeken deze te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.

2. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.

3. De verantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

4. Indien de persoonsgegevens zijn vastgelegd op een gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, dan treft hij de voorzieningen die nodig zijn om de gebruiker van de gegevens te informeren over de onmogelijkheid van verbetering, aanvulling, verwijdering of afscherming ondanks het feit dat er grond is voor aanpassing van de gegevens op grond van dit artikel.

5. Het bepaalde in het eerste tot en met vierde lid is niet van toepassing op bij de wet ingestelde openbare registers, indien in die wet een bijzondere procedure voor de verbetering, aanvulling, verwijdering of afscherming van gegevens is opgenomen.

Artikel 40 Wet bescherming persoonsgegevens

1. Indien gegevens het voorwerp zijn van verwerking op grond van artikel 8, onder e en f, kan de betrokkene daartegen bij de verantwoordelijke te allen tijde verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.

2. De verantwoordelijke beoordeelt binnen vier weken na ontvangst van het verzet of het verzet gerechtvaardigd is. Indien het verzet gerechtvaardigd is, beëindigt hij terstond de verwerking.

3. De verantwoordelijke kan voor het in behandeling nemen van een verzet een vergoeding van kosten verlangen, die niet hoger mag zijn dan een bij of krachtens algemene maatregel van bestuur vast te stellen bedrag. De vergoeding wordt teruggegeven in geval het verzet gegrond wordt bevonden.

4. Dit artikel is niet van toepassing op openbare registers die bij de wet zijn ingesteld.

8. Informatiebeveiliging

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 13 Wet bescherming persoonsgegevens

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 14 Wet bescherming persoonsgegevens

1. Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen, en ten aanzien van de melding van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt. De verantwoordelijke ziet toe op de naleving van die maatregelen.

2. De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.

3. De verantwoordelijke draagt zorg dat de bewerker:
   a. de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid;
   b. de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13, en
   c. de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van de verplichting tot melding van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt.

4. Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b en c.

5. Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, de beveiligingsmaatregelen, bedoeld in artikel 13, en de verplichting tot melding van een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt, schriftelijk of in een andere, gelijkwaardige vorm vastgelegd.

9. Bewaren en vernietigen

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 10 Wet bescherming persoonsgegevens

1. Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.

2. Persoonsgegevens mogen langer worden bewaard dan bepaald in het eerste lid voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

10. Gegevensexport

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 76 Wet bescherming persoonsgegevens

1. Persoonsgegevens die aan een verwerking worden onderworpen of die bestemd zijn om na hun doorgifte te worden verwerkt, worden slechts naar een land buiten de Europese Unie doorgegeven indien, onverminderd de naleving van de wet, dat land een passend beschermingsniveau waarborgt.

2. In afwijking van het eerste lid kunnen persoonsgegevens die aan een verwerking worden onderworpen of die zijn bestemd om na hun doorgifte te worden verwerkt naar een land buiten de Europese Unie worden doorgegeven, indien dat land partij is bij de op 2 mei 1992 te Oporto totstandgekomen Overeenkomst betreffende de Europese Economische Ruimte (Trb. 1992, 132), tenzij uit een besluit van de Commissie van de Europese Gemeenschappen of de Raad van de Europese Unie voortvloeit dat deze doorgifte is beperkt of verboden.

3. Het passend karakter van het beschermingsniveau wordt beoordeeld gelet op de omstandigheden die op de doorgifte van gegevens of op een categorie gegevensdoorgiften van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde of de doeleinden en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectoriële rechtsregels die in het betrokken derde land gelden, alsmede de regels van het beroepsleven en de veiligheidsmaatregelen die in die landen worden nageleefd.

11. Meldplicht datalekken

Deze eis is gebaseerd op de volgende wettelijke bepalingen:

Artikel 34a Wet bescherming persoonsgegevens

1. De verantwoordelijke stelt het College [red.: de Autoriteit Persoonsgegevens] onverwijld in kennis van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

2. De verantwoordelijke, bedoeld in het eerste lid, stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in het eerste lid, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

3. De kennisgeving aan het College en de betrokkene omvat in ieder geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

4. De kennisgeving aan het College omvat tevens een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

5. De kennisgeving aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.

6. Het tweede lid is niet van toepassing indien de verantwoordelijke passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens.

7. Indien de verantwoordelijke geen kennisgeving aan de betrokkene doet, kan het College, indien het van oordeel is dat inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, van de verantwoordelijke verlangen dat hij alsnog een kennisgeving doet.

8. De verantwoordelijke houdt een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.

9. Dit artikel is niet van toepassing indien de verantwoordelijke in zijn hoedanigheid als aanbieder van een openbare elektronische communicatiedienst een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet.

10. Het tweede en zevende lid zijn niet van toepassing op financiële ondernemingen als bedoeld in de Wet op het financieel toezicht.

11. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving.

Colofon

IMMA Privacy referentiearchitectuur is een uitgave van het ministerie van Infrastructuur en Milieu, programma Beter Benutten, maart 2016

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

Ontwerp en vormgeving
Lexenzo, Voorburg

Drukwerk
Sandedruk, Nootdorp

www.beterbenutten.nl/imma