YUCAN

Productinformatie

AVG-Control | Voor zelfstandigen zonder personeel (ZZP)

SECTOR

Bedrijfsleven

TYPE

Compliance management , Informatiebeveiliging , Informatiemanagement , Privacymanagement , Riskmanagement

BRON

AVG

PRODUCTINFORMATIE

AVG-Control | Voor zelfstandigen zonder personeel (ZZP)

SECTOR

Bedrijfsleven

TYPE

Compliance management , Informatiebeveiliging , Informatiemanagement , Privacymanagement , Riskmanagement

BRON

BESCHRIJVING

Uw eigen online management-omgeving waarin u alles rondom de AVG zelfstandig en blijvend organiseert. Inclusief Verwerkingsregister, DPIA's en management van uw verbeter- en beheersingsprocessen. Al uw verantwoordingsdocumenten altijd direct beschikbaar.

GESELECTEERDE MODULES

01. Modules: Evaluatie (looptijd 1 jaar)

PRIJS

€ 139,00 (excl. btw) incl. 25 gebruikers

INHOUDSOPGAVE

1. Informatie

AVG-Control in Yucan

U start uw eigen online management-omgeving inclusief AVG-Control.

Met AVG Control in Yucan krijgt u alles rondom de AVG kostenefficiënt en blijvend onder controle. Inhoudelijk èn procesmatig. AVG Control is namelijk een online management-omgeving die u in staat stelt om met of zonder consultancy of hulp van derden aan de strenge eisen van de AVG te voldoen.

AVG Control is tegelijk ook uw handleiding voor de AVG!U ziet altijd duidelijk waar u moet beginnen, met op ieder punt uitleg over wat u moet doen en wanneer u moet handelen. Zo heeft u uw volledige AVG-Dossier altijd en blijvend op orde!

Van Bewerkingsregister tot kant-en-klare checklists, DPIA's, inbreukregistraties (datalek), privacy-plannen en projectformats: U ziet direct wat u voor de wet (AVG) moet vastleggen en wordt overal waar nodig, door uitleg, voorbeelden en relevante wetgeving ondersteund. En wanneer maar nodig, zijn met één druk op de knop alle verantwoordingsdocumenten beschikbaar.

Start een gratis demo en laat u adviseren!

Start een gratis demo om te zien wat AVG-Control voor u kan betekenen.

AVG-Control biedt u veel en is zeer volledig. Neem daarom **geheel kosteloos** contact op met één van onze adviseurs om uw demo samen te doorlopen. Binnen 10 minuten heeft u een totaal beeld, u ziet direct hoe u alles rondom de AVG doelmatig, zelfstandig organiseert.

Tel: 020 - 5305053

Uw online management-omgeving inclusief

- Privacy-framework
- Proces-inventarisatie
- Organisatie DPIA's
- Proces DPIA's
- Bewerkingsregister
- Register datalekken
- Privacy beleid & protocollen
- Privacy jaarplan
- AVG-verantwoording
- Beheer & rapportage
- De PDCA rond.

Past dit AVG-Control product bij uw organisatie?

Dit AVG-Control product is geschikt voor kleinere bedrijven of zelfstandigen **zonder** personeel, waar verschillende verantwoordelijkheden door één enkele persoon (mogelijk met beperkte ICT of administratieve ondersteuning) worden gedaan en functies niet zijn gescheiden. Inventarisatie van processen is gegroepeerd op het niveau van bijvoorbeeld primaire processen en ondersteunende processen.

- Heeft u een grotere organisatie, werkt u zelfstandig **met** personeel of heeft u een organisatie waarin verantwoordelijkheden zijn verdeeld over afdelingen of er een duidelijker functiescheiding is? Of wilt u bij voorkeur alles verder opgeplitst analyseren en organiseren? Bekijk dan de andere AVG-Control producten.
- Bent u een school of onderwijsinstelling? Of een zorgaanbieder of zorginstelling? Bekijk de AVG-Control producten voor uw sector.

Bekijk de inhoud

Een deelweergave van uw AVG-Proces, behulpzame uitleg, procesinventarisatie, privacy framework, en wetgeving (AVG) heeft u direct in beeld.

De werking en inhoud van verwerkingsregister, DPIA's, behandellijst, verbeter- en privacy plannen en rapportagevormen ziet u in de demo in de module 'ontwikkelen'.

Bekijk de inhoud via de betreffende tab hierboven of start een demo om verder te kijken.

Werkwijze & looptijd kiezen

Kies een werkwijze door onder de tab 'Modules en proces' een combinatie van modules te kiezen. U kunt compact beginnen en altijd uitbreiden naar een team-aanpak. U ziet daar het gekozen proces en of deze het beste bij uw doelstellingen past. U leest in het kort wat u in de verschillende modules kunt doen en wat uw output is.

Let op!

- U kunt nu ook een **maandlicentie** nemen om eerst eens te kijken waar u staat en verbeterpunten vaststellen! Wilt u daarbij ook registraties doen en DPIA's uitvoeren?
- **> Kies dan voor een werkwijze met ontwikkelmodule.**
- En wilt u uw DPIA's en verwerkingsregister buiten Yucan uitvoeren en beheren? Maar wel werken met de checklist, procesinventarisatie en het privacy framework?
- > Kies dan voor een werkwijze **zonder** ontwikkelmodule. U kunt deze later altijd toevoegen.

Uw proces (PDCA) in AVG-Control ziet er als volgt uit:

Stap 1 Inventariseren & Beheren(evaluatiemodule)

U werkt in het privacy-framework. U inventariseert en brengt de processen waar persoonsgegevens worden gebruikt in kaart. Zo weet u zeker dat u niets over het hoofd ziet. Samen met de analyse in het Privacy Framework heeft u uw Organisatie DPIA in de basis op orde.

Stap 2 Analyseren, Vastleggen & Prioriteren (ontwikkelmodule)

Hier legt u alle bewerkingen vast die automatisch in het Bewerkingsregister komen. Daarbij checkt u o.a. of verwerking wetmatig is en direct ook of een DPIA vereist is. Voert u die DPIA ook uit dan brengt u eventuele verbeterpunten ook direct in beeld. AVG control genereert automatisch een overzichtelijke behandellijst.

Stap 3 Documenteren, Verbeteren & Plannen (ontwikkelmodule)

Hier documenteert u uw privacybeleid, datalekken, protocollen, handboeken en privacy (jaar)plannen. En met behulp van de handzame en flexibele formats in AVG Control werkt u hier al uw

verbeterprojecten uit.

Stap 4 Overzicht, bewerkingsregister & Verantwoording (ontwikkelmodule)

AVG Control is zo opgezet dat u continu een samenhangend overzicht heeft èn houdt van alle processen, bewerkingen, incidenten, beschrijvingen, verbeterprojecten & privacyplannen. En met één druk de knop heeft u al uw rapportages en verantwoordingsdocumenten altijd direct beschikbaar.

Rapportage en verantwoording AVG

Alles geintegreerd en direct beschikbaar voor de vereiste verantwoordingswijze van de toezichthouder (AP).

Met een druk op de knop heeft u op ieder gewenst moment de beschikking over allerhande keurig verzorgde rapportages (scherm en pdf). Van de uitkomsten uit uw inventarisatie tot volledige DPIA’s. Uw complete verwerkingsregister t/m behandellijsten, verbeterprojecten en privacyplannen.

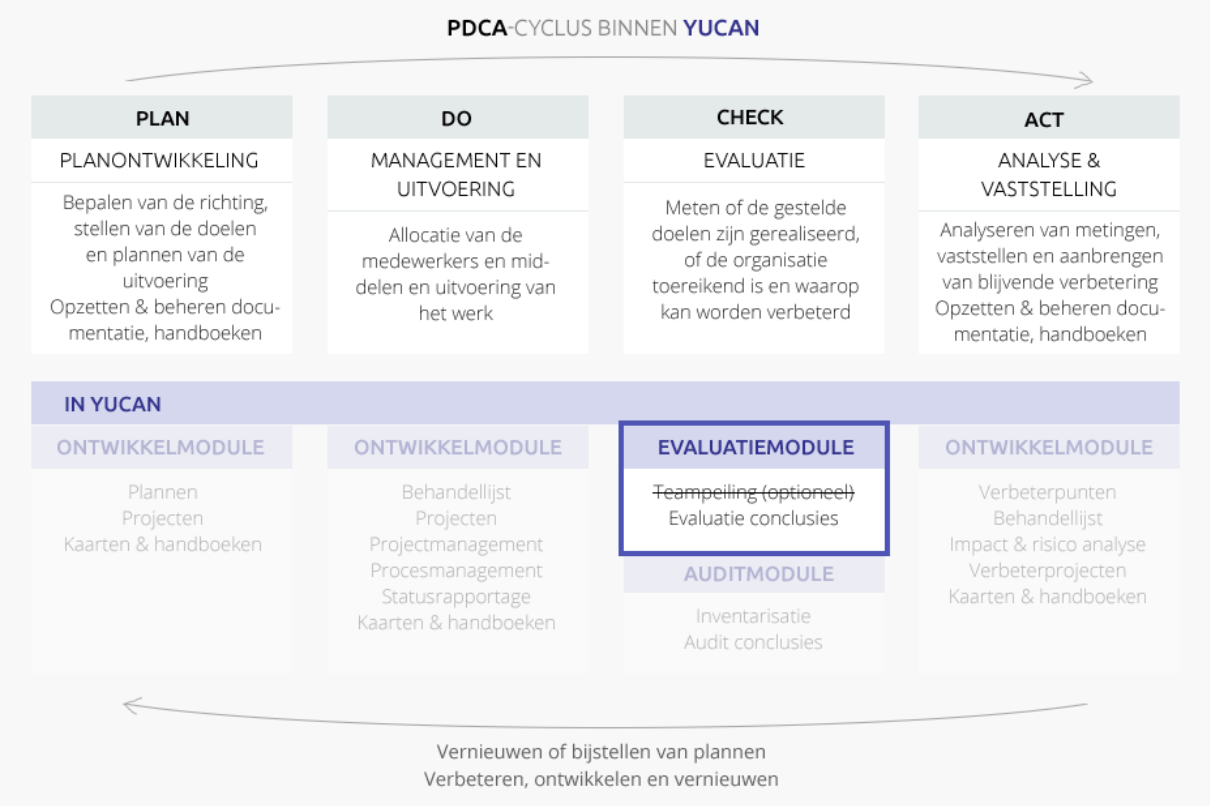
Binnen uw account werken met meerdere producten en werkomgevingen

Heeft u al een account? Binnen uw account kunt u voor het werken met iedere afzonderlijk product steeds een eigen werkruimte activeren. Dus ook voor uw AVG-Control. Zo heeft u alles goed georganiseerd.

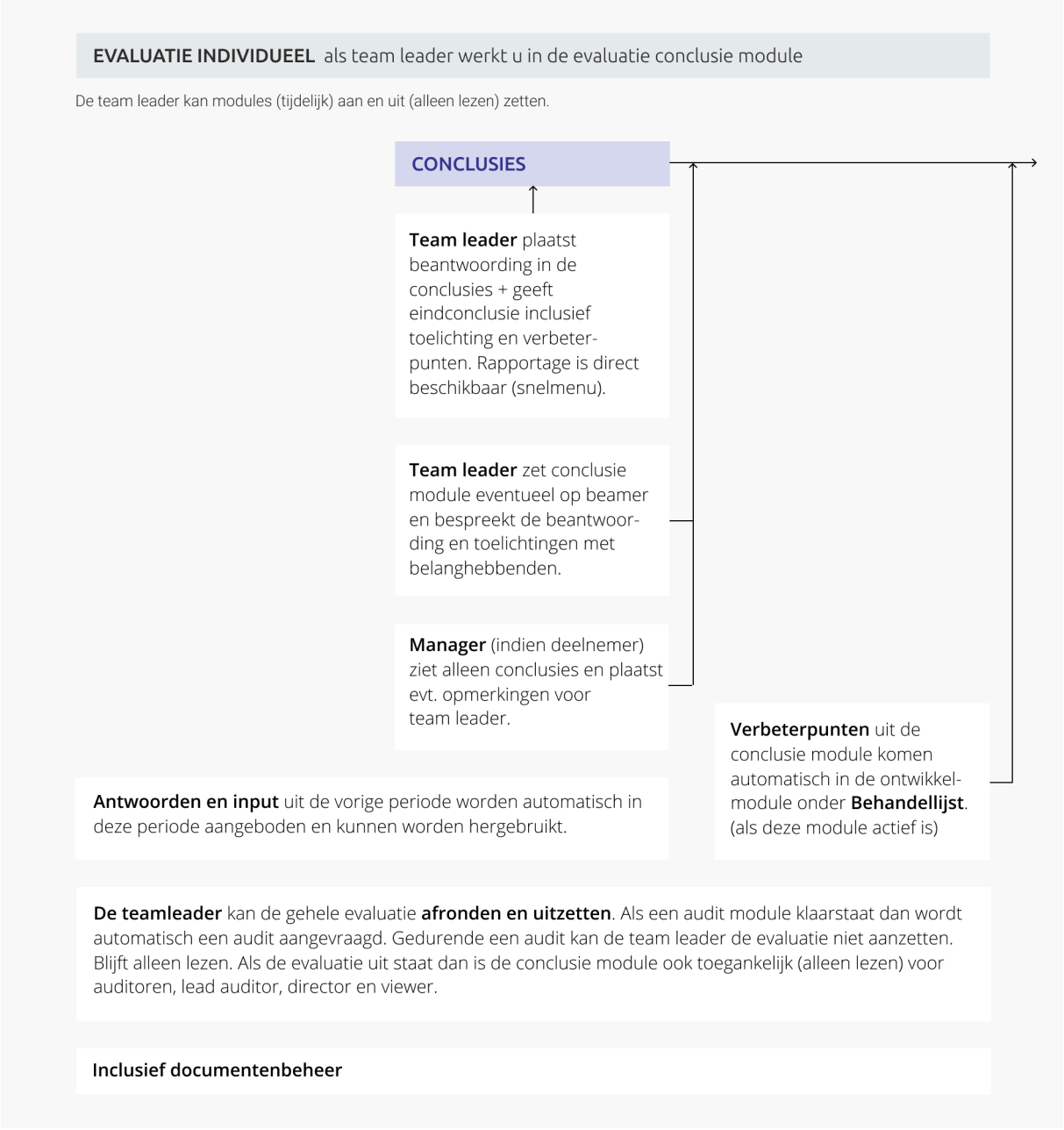
U kunt er voor kiezen binnen één werkruimte samen te werken o.b.v. een product. Ook kunt u voor ieder afzonderlijk deel van uw organisatie een eigen werkruimte met het betreffende product activeren. Per werkruimte of door meerdere werkruimten te activeren kunt u andere betrokkenen aanwijzen en het beheer en de opvolging in uw organisatie spreiden. U en uw collega's kunnen gelijktijdig bij meerdere werkruimten betrokken zijn terwijl de regie centraal kan blijven.

2. Modules en proces

Proces in beeld



Evaluatie individueel



Evaluatie - Conclusie

U evalueert de in het portfolio aangeboden onderwerpen. U beantwoordt de vragen, geeft eventueel toelichtingen en benoemd verbeterpunten. Zo nodig voegt u per onderwerp onderbouwende documenten (bewijsstukken) toe. Conclusies uit een eventuele eerdere periode of (teamevaluatie) input van deelnemers aan de peiling kunt u met een druk op de knop kopiëren. Door u benoemde verbeterpunten worden - indien de ontwikkelmodule wordt gebruikt - ook automatisch in uw behandellijst getoond.

U hebt de beschikking over uitgebreide rapportage van uw conclusies. Heeft u meerdere portfolio's? Dan kunt u de gegevens in rapporten combineren. Uw gegevens blijven bewaard en kunnen in een volgende periode eenvoudig worden hergebruikt.

3. Inhoud

AVG-Control - Voor kleine bedrijven zonder personeel (ZZP)

I. Proces en PDCA in beeld

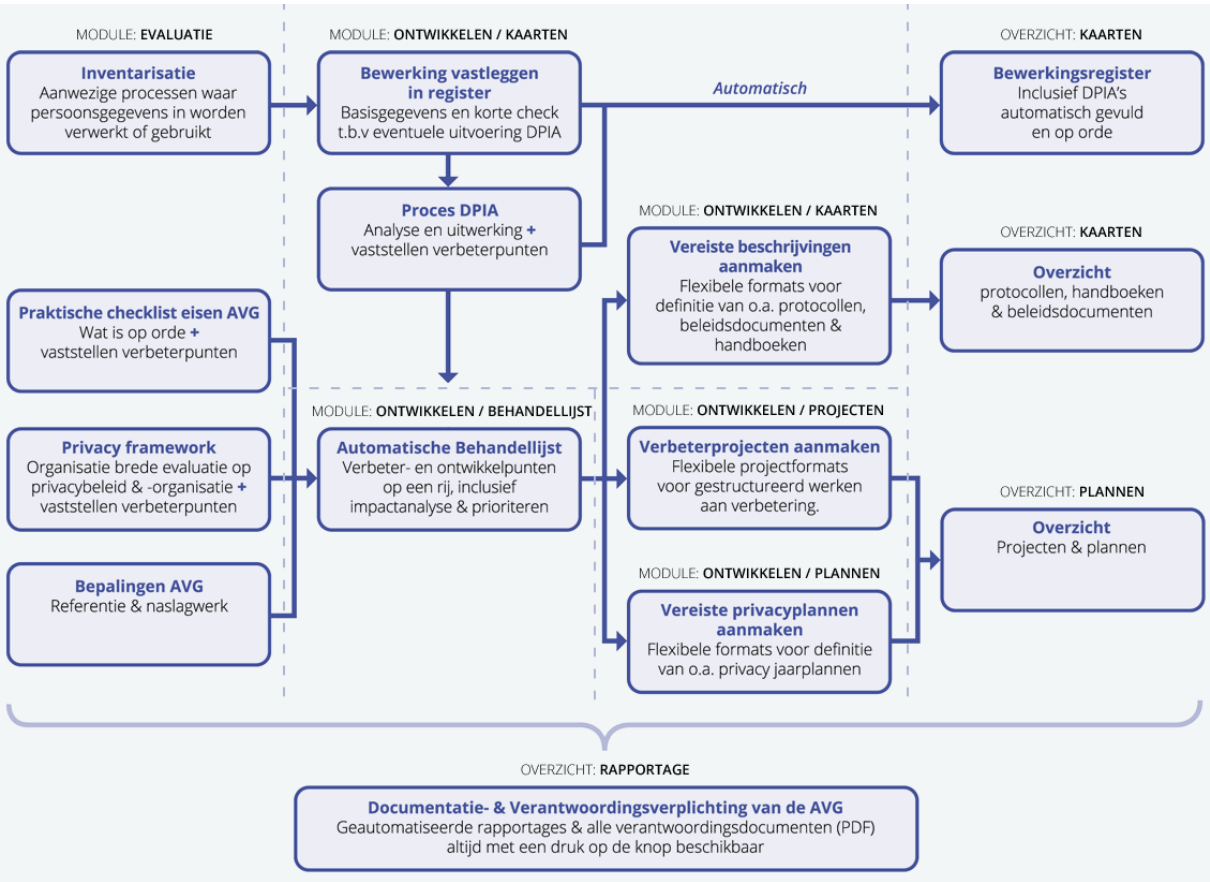
Proces en PDCA in beeld

AVG Control werkt intuïtief. U ziet altijd duidelijk waar u moet beginnen, wat u moet doen en wanneer u moet handelen. Van Bewerkingsregister tot organisatiebrede checklist (Privacy framework), DPIA's, privacy-plannen en projectformats: alles is helder vormgegeven en wordt overal waar nodig, door uitleg, voorbeelden en relevante wetgeving ondersteund. En wanneer maar nodig, zijn met één druk op de knop alle verantwoordingsdocumenten beschikbaar.

In 4 stappen blijven 'in control'

Via onderstaand schema ziet u direct welke stappen u waar in Yucan/AVG-Control doet.

U kunt alles op ieder moment benaderen en gebruiken. Uw ideale route is van links naar rechts.



Stap 1 Inventariseren & Beheren

In het privacy-framework evalueert u waar u staat. Met de proces inventarisatie brengt u de processen waar persoonsgegevens worden gebruikt in kaart. Zo weet u zeker dat u niets over het hoofd ziet. En zo heeft en houdt u uw Organisatie DPIA volledig op orde.

Stap 2 Analyseren, Vastleggen & Prioriteren

U legt alle bewerkingen vast die automatisch in het Bewerkingsregister komen. Daarbij checkt u meteen of een DPIA vereist is. Voert u die DPIA ook uit dan brengt u eventuele verbeterpunten ook direct in beeld. AVG control genereert automatisch een overzichtelijke behandellijst.

Stap 3 Documenteren, Verbeteren & Plannen

Hier documenteert u uw privacybeleid, protocollen, handboeken en privacy (jaar)plannen. En met behulp van de handzame en flexibele formats in AVG Control werkt u hier al uw verbeterprojecten uit.

Stap 4 Overzichten, bewerkingsregister & Verantwoording

AVG Control is zo opgezet dat u continu een samenhangend overzicht heeft èn houdt van alle processen, bewerkingen, beschrijvingen, verbeterprojecten & privacyplannen. En met één druk de knop heeft u al uw rapportages en verantwoordingsdocumenten altijd direct beschikbaar.

II. Privacy Framework

De onderwerpen, aspecten en toelichtingen in het privacy framework beslaan de relevante aandachtspunten voor privacymanagement in de organisatie. Het doorlopen van deze onderwerpen helpt u bij het inzichtelijk maken en houden van de status van het privacybeleid, de uitvoering daarvan en het voldoen aan wet- en regelgeving. Het geheel biedt een krachtig instrument om over het geheel van verplichtingen 'in control' te zijn en te voldoen aan de vereisten van de AVG.

1. Management & Beleid

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet voor u van toepassing zijn, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

1.1* Privacybeleid

U heeft een adequaat privacybeleid vastgesteld.

Toelichting

Een adequaat en bij u passend privacybeleid is wettelijk verplicht (AVG) en helpt u grip te krijgen en houden op privacy gerelateerde zaken en de bescherming daarvan. Inzicht in risico's, het formuleren van een visie en het vaststellen hoe u waarborgt dat gegevens rechtmatig, behoorlijk en transparant verwerkt, zijn de onderleggers voor een bestendige en gedragen implementatie en borging van adequate privacybescherming.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* U hebt een overkoepelend privacybeleid vastgesteld waaruit blijkt dat u kennis hebt en bewust bent van risico's en wetgeving ten aanzien van privacybescherming en waarin uw visie op privacybescherming is beschreven.					
b.* In het privacybeleid is beschreven hoe u waarborgt hoe u gegevens verwerkt en hoe u zich aan wet- en regelgeving houdt, waarin uitdrukkelijk doch niet uitsluitend wordt voldaan aan de beginselen van rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en verantwoordingsplicht zoals de AVG dat vereist.					
c.* Het privacybeleid is beschikbaar en begrijpelijk en omschrijft minimaal richtlijnen voor en wettelijke eisen, waaraan processen, bepalingen, werkafspraken en communicatie ten aanzien van privacy en privacy gerelateerde zaken en situaties moeten voldoen.					
d.* Het privacybeleid of minimaal de voor de betrokkenen relevante delen daarvan zijn beschikbaar en begrijpelijk voor betrokkenen (wiens persoonsgegevens worden verwerkt) en beschrijft de wijze waarop wordt gewaarborgd dat hun rechten worden beschermd en hen voldoende ruimte wordt geboden voor uitoefening daarvan.					
e.* Het privacybeleid bevat onderwerpen, procedures en frequenties voor adequate evaluatie van doelmatigheid en doeltreffendheid op het gebied van privacybescherming en de naleving van privacyregelgeving.					
f. Het privacybeleid is zodanig concreet dat de effectiviteit kan worden gemeten, gecontroleerd en privacybescherming gericht kan worden geoptimaliseerd.					
g.* Conclusie:					

1.2* Privacymanagement

1.3* Compliance & PDCA

2. U en de EG

2. Uw en de AVG

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet voor u van toepassing zijn, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

2.1* U bent proceseigenaar & uitvoerder

Als proceseigenaar en uitvoerder voldoet u aan de taakstelling en vereisten van het privacybeleid.

Toelichting

U bent proceseigenaar en uitvoerder en draagt verantwoording voor een proces en/of handeling waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin). U bent degene die binnen de dagelijkse gang van zaken grip moet houden op uw verantwoordelijkheid ten aanzien van privacy.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* U heeft kennis van het privacybeleid en weet waaraan u moeten voldoen.					
b.* U handelt conform het privacybeleid en houdt u aan wet- en regelgeving.					
c.* U bent op de hoogte van welke persoonsgegevens u wel en niet mag verwerken.					
d. U heeft voldoende kennis om zorg te dragen voor adequate uitvoering van het privacybeleid en het voldoen aan wet- en regelgeving.					
e. U heeft voldoende gelegenheid om uw kennis ten aanzien van privacy gerelateerde zaken en situaties actueel en toereikend te houden.					
f.* Conclusie:					

2.2* Functionaris gegevensbescherming (FG)

3. Externe partijen

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet voor u van toepassing zijn, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

3.1* Gegevensverantwoordelijken en Gegevensverwerkers (extern)

In relaties met of als gegevensverantwoordelijke en gegevensverwerker voldoet u aan wet- en regelgeving.

Toelichting

Om uitvoering te geven aan het privacybeleid en privacy adequaat te beschermen worden bij aanname of het uitbesteden van de verwerking van persoonsgegevens overeenkomsten afgesloten die voldoen aan wet- en regelgeving. U verzekert u er binnen uw mogelijkheden van dat de organisaties waar persoonsgegevens worden verwerkt of die persoonsgegevens voor u verwerken een adequaat privacybeleid voeren en zich houden aan wet- en regelgeving. De AVG vereist hierin een proactieve rol van u. Indien u vaststelt of gerede twijfel heeft of de derde partij zich aan wet- en regelgeving houdt dan dient u daar consequenties aan te verbinden. Deze kunnen bestaan uit het vereisen van passende maatregelen of afzien van samenwerking op het gebied van bewerking van persoonsgegevens.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* Met derde partijen (verwerkingsverantwoordelijken) waarvoor bewerkingen worden uitgevoerd en waartoe u zich als verwerker verhoudt zijn bewerkingsovereenkomsten afgesloten die voldoen aan wet- en regelgeving.					
b.* Met derde partijen (bewerkers) die bewerkingen uitvoeren en waartoe u zich als verwerkingsverantwoordelijke verhoudt zijn bewerkingsovereenkomsten afgesloten die voldoen aan wet- en regelgeving.					
c.* Bij het uitwisselen van persoonsgegevens in de relatie verwerkingsverantwoordelijke en verwerker houdt u zich aan wet- en regelgeving waarin uitdrukkelijk doch niet uitsluitend wordt voldaan aan de beginselen van rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en verantwoordingsplicht zoals de AVG dat vereist.					
d.* U - als verwerkingsverantwoordelijke - vereist aantoonbaar dat verwerkers en sub verwerkers voldoen aan wet en regelgeving en in het bijzonder de AVG.					
e.* U doet aantoonbaar navraag naar de aanwezigheid, uitvoering van en voldoen aan privacybeleid indien u als verwerkingsverantwoordelijke of verwerker een relatie met een derde aangaat.					
f.* U ziet af van ontvangst of verstrekking van persoonsgegevens indien blijkt dat deze derde partij onvoldoende privacybestendig is					

g.* U wisselt geen persoonsgegevens uit met derden indien op basis van feiten of omstandigheden ernstig getwijfeld moet worden aan de kwaliteit van het privacybeleid van die derden.					
h.* U voert bij een doorgifte van persoonsgegevens naar derde landen (landen buiten de EER) controle uit op het beschermingsniveau van persoonsgegevens bij het derde land.					
i.* Als U constateert dat het derde land niet beschikt over een passend beschermingsniveau, zorgt u dat er is voldaan aan een van de overige voorwaarden voor doorgifte van persoonsgegevens naar dat derde land.					
j.* Conclusie:					

3.2* Ontvangers en verstrekkers van gegevens

4. Middelen

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.
Indien onderwerpen of aspecten naar uw inzicht niet voor u van toepassing zijn, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

4.1* Financieel

U zet ten behoeve van de effectieve uitvoering van het privacybeleid voldoende financiele middelen in.

Toelichting

Er dienen voldoende financiële middelen beschikbaar te zijn en – bij voorkeur planmatig /in de begrotingscyclus - worden toegewezen voor uitvoering van het privacybeleid. Bij het vormgeven en beheren van processen dient functioneel, operationeel en financieel rekening te zijn gehouden met privacybescherming en de wettelijke vereisten (o.a. privacy by design & privacy by default). Verder vereist de AVG een adequate informatievoorziening over rechten van betrokkenen en ondersteuning bij het uitoefenen daarvan. Zowel de informatie en communicatie als technische en operationele invulling daarvan dienen structureel te zijn en vereisen financiële middelen.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* U stelt de voor adequate privacybescherming benodigde financiële middelen ter beschikking.					
b. De financiële middelen voor het inrichten en uitvoeren van privacymanagement zijn bekend, toereikend, beschikbaar en zijn of worden periodiek en/of planmatig toegewezen.					
c. De financiële middelen voor het privacybestendig maken van processen zijn bekend, toereikend, beschikbaar en zijn of worden periodiek en/of planmatig toegewezen.					
d. De financiële middelen voor zowel technische als operationele realisatie van de vereiste informatievoorziening over rechten van betrokkenen en de ondersteuning bij het uitoefenen daarvan zijn bekend, toereikend, beschikbaar en zijn of worden periodiek en/of planmatig toegewezen.					
e.* Conclusie:					

4.2* Gebouwen en faciliteiten

5. Privacy aspecten binnen operationele processen & procedures

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet voor u van toepassing zijn, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

De AVG stelt uitgebreide eisen ten aanzien van de inrichting en documentatie van processen. Naast de privacy-specifieke processen die de AVG vereist, dienen de operationele werkprocessen waarin persoonsgegevens worden verwerkt privacybestendig te zijn. Daarnaast dienen processen als inkoop, informatiebeveiliging, ICT en compliance ook te zijn gericht op het optimaliseren van uw privacybescherming als geheel.

5.1* Beheersing van privacy in werkprocessen en verwerkingen

De werkprocessen en verwerkingen binnen de organisatie zijn privacybestendig.

Toelichting

Het realiseren en borgen van een privacybestendige organisatie vindt in de basis plaats door de werkprocessen, waar persoonsgegevens worden verwerkt (verzamelen, beheren, gebruiken, verstrekken, in brede zin), ook ten aanzien van het beschermen van privacy te optimaliseren. Een adequate inrichting van processen waarbij in de ontwerpfase al rekening is gehouden met privacyaspecten helpt bij het voldoen aan wet- en regelgeving. Het brengt u doelmatiger 'in control' en minimaliseert uw inspanningen ten aanzien van privacymanagement.

Door uitvoering van de procesinventarisatie, het registreren van processen en bewerkingen in het bewerkingsregister – waarbij een korte basisanalyse op onderstaande punten plaatsvindt – en het eventueel uitvoeren van Proces-DPIA's aldaar, stelt u het onderstaande per werkproces vast.

Evaluatie op onderstaande punten betreft de samenvoeging van alle werkprocessen en heeft tot doel inzicht te verschaffen over het geheel. Deze onderliggende informatie per werkproces dient of is bedoeld beschikbaar te zijn in en via het verwerkingsregister.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* Werkprocessen (waarin persoonsgegevens worden verwerkt) zijn beschreven.					
b.* Werkprocessen hebben een procesverantwoordelijke (u).					
c.* Binnen het werkproces zijn passende technische en organisatorische maatregelen getroffen om de privacy te waarborgen en aan wet- en regelgeving te voldoen.					
d.* Bij het ontwerp of herontwerp van werkprocessen wordt adequaat rekening gehouden met privacy aspecten en wordt, zoveel als redelijkerwijs in verhouding staat tot de schaal en de risico's van het proces voor betrokkenen, gericht op privacy by design en privacy by default.					
e. Er zijn indicatoren beschikbaar die het mogelijk maken de risico bestendigheid van het werkproces te beoordelen.					
f.* Binnen de werkprocessen worden persoonsgegevens verwerkt op een wijze die ten aanzien van de betrokkene (degene van wie de persoonsgegevens zijn) rechtmatig, behoorlijk en transparant is (rechtmatigheid, behoorlijkheid en transparantie).					
g.* De doeleinden van de verwerking in het werkproces zijn welbepaald, uitdrukkelijk omschreven en gerechtvaardigd en worden vervolgens niet op een daarmee onverenigbare wijze verwerkt (verzamelen, beheren, gebruiken, verstrekken, in brede zin) (doelbinding).					
h.* Binnen de werkprocessen worden niet meer persoonsgegevens verwerkt dan noodzakelijk voor het bereiken van het doel van de respectieve processen (minimale gegevensverwerking en doelbinding).					

i.* Binnen de werkprocessen worden alleen die persoonsgegevens verwerkt die noodzakelijk zijn voor het bereiken van het doel van de respectieve processen (minimale gegevensverwerking en doelbinding)					
j.* Binnen het werkproces zijn alle redelijke maatregelen genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren (juistheid).					
k.* De binnen het werkproces te verwerken of verwerkte persoonsgegevens worden bewaard in een vorm die er in voorziet dat betrokkenen niet langer te identificeren zijn dan voor de doeleinden van de bewerking noodzakelijk is (opslagbeperking).					
l.* De binnen de werkprocessen verwerkte persoonsgegevens worden niet langer beschikbaar gehouden dan voor het doel van het proces noodzakelijk is (opslagbeperking).					
m.* De binnen de werkprocessen te verwerken persoonsgegevens zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (integriteit en vertrouwelijkheid).					
n.* De organisatie is verantwoordelijk voor naleving van de voornoemde punten / wettelijke vereisten en kan dit aantonen (verantwoordingsplicht).					
o. Conclusie:					

5.2* Inkoop

5.3* Informatiebeveiliging en -beleid

6. Privacy specifieke processen & procedures (AVG)

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet voor u van toepassing zijn, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

De AVG stelt uitgebreide eisen ten aanzien van de aanwezigheid, inrichting en documentatie van privacy specifieke processen. Gegevensverwerkingen dienen te zijn opgenomen in een bewerkingsregister; Analyseprocessen en beheerprocessen dienen vast te liggen (DPIA's) ; Waarborgende processen ten aanzien van transparantie naar en uitoefening van rechten door

betrokkenen (degene van wie de persoonsgegevens zijn) dienen te zijn vastgesteld en gedocumenteerd.

6.1* Organisatie-DPIA (Data Protection Impact Assessment op organisatieniveau)

6.2* Proces DPIA's (Data Protection Impact Assessment op procesniveau)

De proces-DPIA's worden adequaat ingezet en ondersteunen de uitvoering van het privacybeleid effectief.

Toelichting

Wanneer een soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (betrokkenen) dan vereist de AVG van u dat voorafgaand aan de verwerking een Proces-DPIA wordt uitgevoerd.

Een verhoogd risico kan bestaan door het gebruik van nieuwe technologieën, aard, context en doeleinden van de beoogde verwerking. Een Proces-DPIA is met name vereist voor verwerken die een of meer van onderstaande kenmerken in zich dragen:

- Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking , waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen.
- Grootschalige verwerking van bijzondere categorieën van persoonsgegevens (AVG; art 9, lid 1) of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten (AVG; Art. 10).
- Stelselmatige en grootschalige monitoring van openbare ruimten.

In de submodule 'Kaarten' onder 'ontwikkelen' vindt u kant en klare formats voor het uitvoeren van Proces-DPIA's.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* Proces-DPIA's worden voorafgaand aan de respectieve bewerking en bij aanpassing van die bewerking of verandering van het risico daarvan uitgevoerd.					
b.* Proces-DPIA's behandelen en beschrijven minimaal de onderdelen die volgens de AVG verplicht zijn.					
c.* Het uitvoeringsproces van Proces-DPIA's is systematisch en vastgelegd.					
d.* Voor het uitvoeren van een Proces-DPIA is een eindverantwoordelijke (u of een derde) aangewezen.					
e.* Indien u de proces-DPIA niet zelf uitvoert, heeft de eindverantwoordelijke voldoende informatie, bevoegdheden, rechten, plichten en bewegingsvrijheid om zijn of haar taken effectief en onafhankelijk te kunnen uitvoeren.					
f.* Een Proces-DPIA geeft u een adequaat beeld van het niveau van privacybescherming, privacyrisico's en in welke mate wordt voldaan aan wet en regelgeving.					
g.* Een Proces-DPIA geeft u een adequaat beeld op welke gebieden en aspecten, ten aanzien van het respectieve proces en/of de bewerkingen, maatregelen nodig zijn om aan de wettelijke vereisten en de bepalingen in het privacybeleid te voldoen.					
h.* Een Proces-DPIA geeft u een adequaat beeld van de ten behoeve van het respectieve proces te initiëren en reeds geïnitieerde verbeteracties en de status en deadlines daarvan.					
i.* Indien uit een Proces-DPIA blijkt dat de verwerking een hoog risico oplevert indien de verwerkingsverantwoordelijke geen maatregelen neemt, dan wordt de toezichthoudende					
j.* Conclusie:					

6.3* Verwerkingsregistratie en verwerkingsregister

Het bewerkingsregister wordt adequaat ingezet en ondersteunt de uitvoering van het privacybeleid effectief.

Toelichting

De AVG stelt verplicht dat organisaties de bewerkingen (verzamelen, beheren, gebruiken, verstrekken,

in brede zin) van persoonsgegevens vastleggen in het bewerkingsregister. Deze registraties moeten aan bepaalde eisen voldoen.

U heeft geen mensen in dienst. De AVG stelt dat, indien een organisatie minder dan 250 personen in dienst heeft, deze verplichting niet van toepassing is.

TENZIJ:

- *De verwerking die wordt verricht waarschijnlijk een risico inhoud voor de rechten en vrijheden van betrokkenen.*
- *De verwerking **niet** incidenteel is (**opgelet**: Verwerkingen zijn zelden incidenteel. Het bijhouden van persoonsgegevens in de salarisadministratie, het bijhouden van relatiegegevens of versturen van nieuwsbrieven is bijvoorbeeld niet incidenteel).*
- *De verwerking betreft bijzondere categorieën van persoonsgegevens (AVG: Art 9, lid 1)*
- *De verwerking persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten (AVG: Art. 10)*

Het voorgaande betekent in de praktijk dat vrijwel iedere organisatie een bewerkingsregister moet bijhouden.

Het bewerkingsregister bouwt en onderhoudt u eenvoudig en doelmatig in de submodule 'kaarten' onder 'ontwikkelen'. U doet daar direct een korte check en indien een proces-DPIA vereist blijkt, voegt u deze met een druk op de knop aan de bewerking toe.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* U beschikt over een register van alle verwerkingsactiviteiten.					
b.* Het verwerkingsregister bevat alle verplichte informatie.					
c.* Het verwerkingsregister is actueel.					
d.* U beschikt over een procedure voor het actueel houden van het verwerkingsregister.					
e.* Conclusie:					

6.4* Datalekken (inbreuk privacy)

6.5* Documentatie & Verantwoording

7. Transparantie, informatievoorziening en rechten van betrokkenen

De met een (*) gemarkeerde onderwerpen en aspecten zijn vereisten van de AVG.

Indien onderwerpen of aspecten naar uw inzicht niet voor u van toepassing zijn, dan is het raadzaam in ieder geval te overwegen of en zo ja; hoe deze van invloed zijn op het privacybeschermingsniveau en het voldoen aan wet- en regelgeving.

7.1* Informatievoorziening en informatieverzoeken met betrekking tot persoonsgegevens.

Uw informatievoorziening is effectief en voldoet aan wet- en regelgeving.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* U draagt er zorg voor en borgt dat informatie en communicatie, naar betrokkenen in verband met verwerkingen van persoonsgegevens in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal plaats vindt. Passend bij de doelgroep en met name indien het voor kinderen bestemd is.					
b.* U voorziet erin dat deze informatie schriftelijk of elektronisch beschikbaar wordt gemaakt en heeft een protocol en proces vastgesteld dat er in voorziet en borgt dat deze informatie, indien de betrokkende daarom verzoekt, ook mondeling kan worden / wordt meegedeeld op voorwaarde dat de identiteit van de betrokkene is bewezen.					
c.* U heeft een procedure en proces ingeregeld dat er in voorziet en borgt dat onverwijld, doch uiterlijk binnen een maand na ontvangst van het informatieverzoek met betrekking tot persoonsgegevens, informatie over het gevolg (opvolging of informatie zelf) aan betrokkene wordt verstrekt.					
d.* Voornoemde procedure voorziet erin dat, indien niet aan een informatieverzoek kan worden voldaan, de betrokkene onverwijld, doch uiterlijk binnen een maand na ontvangst, daarover en inclusief de redenen wordt geïnformeerd. De betrokkene wordt daarbij geïnformeerd over de mogelijkheid een klacht in te dienen bij de toezichthoudende autoriteit (AP) en beroep bij de rechter in te stellen.					
e. U bent bekend met de wettelijke beperkingen op deze bepaling en neemt deze hierbij in acht.					
f. Bij inregelen van het proces is, zoveel als redelijkerwijs mogelijk en rekening houdend met de beschikbare technologie en de uitvoeringskosten, gericht op ‘privacy by design’ en ‘privacy by default’.					
g.* Conclusie:					

7.2* Informatievoorziening indien de persoonsgegevens bij de betrokkene worden verzameld (direct)

7.3* Informatievoorziening indien de persoonsgegevens niet van de betrokkene zijn verkregen (indirect)

7.4* Verkrijgen van toestemming en het recht op intrekken van toestemming

U zorgt dat, wanneer dat vereist is, toestemming van betrokkene wordt verkregen, toetst de rechtmatigheid daarvan en legt die toestemming, conform wet- en regelgeving vast. U zorgt dat de betrokkene zijn recht om toestemming in te trekken effectief en conform wet- en regelgeving kan uitoefenen.

Toelichting

(AVG: Art 7) *Voorwaarden voor toestemming*

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

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

De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming doet geen afbreuk aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan. Voordat de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld.

Het intrekken van de toestemming is even eenvoudig als het geven ervan.

Toestemming dient vrijelijk te zijn gegeven. Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist (en/of gevraagd) is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.

(AVG Art. 8) *Voorwaarden voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij*

Wanneer uitdrukkelijke toestemming wordt verleent in verband met een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, is de verwerking van persoonsgegevens van een kind rechtmatig wanneer het kind ten minste 16 jaar is.

Wanneer het kind jonger is dan 16 jaar is zulke verwerking slechts rechtmatig indien en voor zover de toestemming of machtiging tot toestemming in dit verband wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt.

Met inachtneming van de beschikbare technologie doet de verwerkingsverantwoordelijke redelijke inspanningen om in dergelijke gevallen te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.

Het algemene overeenkomstenrecht (wetgeving), zoals de regels inzake de geldigheid, de totstandkoming of de gevolgen van overeenkomsten ten opzichte van kinderen, blijft van kracht.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* U beschikt over een protocol / procedure dat er in voorziet dat, wanneer vereist, toestemming wordt gevraagd, toestemming per betrokkene wordt vastgelegd en kan worden aangetoond, conform wet- en regelgeving.					
b.* U beschikt over een protocol / procedure die er in voorziet en borgt dat betrokkenen hun recht op het intrekken van toestemming zonder belemmering en onnodige vertraging, net zo eenvoudig als het geven van toestemming en conform wet- en regelgeving kunnen uitoefenen.					
c.* Het protocol / procedure voorziet er in dat u een redelijke inspanning doet om te achterhalen wat de leeftijd van de betrokkene is en daarbij de rechtmatigheid van de toestemming (met name m.b.t. kinderen) toetst.					
d. U bent bekend met de wettelijke beperkingen op deze bepaling en neemt deze in hierbij in acht.					
e. Bij inregelen van het proces is, zoveel als redelijkerwijs mogelijk en rekening houdend met de beschikbare technologie en de uitvoeringskosten, gericht op ‘privacy by design’ en ‘privacy by default’.					
f.* Conclusie:					

7.5* Recht van inzage van de betrokkene

U zorgt dat de betrokkene zijn recht van inzage effectief en conform wet- en regelgeving kan uitoefenen.

Toelichting

Betrokkenen hebben het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen.

Indien de betrokkene daartoe verzoekt dient de (verwerkingsverantwoordelijke) organisatie de betrokkene de bij wet- en regelgeving verplichte informatie te verstrekken. Indien de betrokkene om bijkomende kopieën verzoekt, kan de verwerkingsverantwoordelijke op basis van de administratieve kosten een redelijke vergoeding rekenen. Wanneer de betrokkene zijn verzoek elektronisch indient, en niet om een andere regeling verzoekt, wordt de informatie in een gangbare elektronische vorm verstrekt. Het verstrekken van kopieën doet geen afbreuk aan de rechten en vrijheden van anderen.

Persoonsgegevens waartoe een betrokkene het recht op inzage heeft:

1. *De verwerkingsdoeleinden;*
2. *De betrokken categorieën van persoonsgegevens;*

3. *Een overzicht van de persoonsgegevens die worden verwerkt.*
4. *De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;*
5. *Indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;*
6. *Dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;*
7. *Dat de betrokkene het recht heeft een klacht in te dienen bij een toezichthoudende autoriteit;*
8. *Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;*
9. *Het bestaan van geautomatiseerde besluitvorming, en of er sprake is van profilering en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.*
10. *Wanneer persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie, heeft de betrokkene het recht in kennis te worden gesteld van de passende waarborgen inzake de doorgifte.*

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* U beschikt over een protocol / procedure die er in voorziet en borgt dat betrokkenen hun recht van inzage zonder belemmering en onnodige vertraging en conform wet- en regelgeving kunnen uitoefenen.					
b. U bent bekend met de wettelijke beperkingen op deze bepaling en neemt deze hierbij in acht.					
c. Wanneer de betrokkene zijn verzoek tot inzage elektronisch indient, en niet om een andere regeling verzoekt, verstrekt u de informatie in een gangbare elektronische vorm.					
d.* Bij inregelen van het proces is, zoveel als redelijkerwijs mogelijk en rekening houdend met de beschikbare technologie en de uitvoeringskosten, gericht op ‘privacy by design’ en ‘privacy by default’.					
e.* Conclusie:					

7.6* Recht op rectificatie

U zorgt dat de betrokkene zijn recht op rectificatie effectief en conform wet- en regelgeving kan uitoefenen.

Toelichting

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke direct of zonder onredelijke vertraging rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. De betrokkene heeft er recht op dat onvolledige persoonsgegevens worden aangevuld zodat deze volledig zijn, doch niet meer dan voor de doeleinden van de verwerking noodzakelijk is. De betrokkene na daartoe onder meer een aanvullende verklaring verstrekken.

	VOLDOET NIET	VOLDOET BEPERKT	VOLDOET GROTENDEELS	VOLDOET GEHEEL	NIET VAN TOEPASSING
a.* U beschikt over een protocol / procedure die er in voorziet en borgt dat betrokkenen hun recht op rectificatie zonder belemmering en onnodige vertraging en conform wet- en regelgeving kunnen uitoefenen.					
b. U rectificeert onjuiste persoonsgegevens direct of zo snel als redelijkerwijs mogelijk is.					
c. U vult onvolledige persoonsgegevens aan voor zover passend bij de doeleinden van de verwerking en, indien daartoe een aanvullende verklaring benodigd is, na de ontvangst en eventuele verificatie van die verklaring.					
d.* U stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie van persoonsgegevens, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt. De verwerkingsverantwoordelijke verstrekt de betrokkene informatie over deze ontvangers indien de betrokkene hierom verzoekt.					
e.* U bent bekend met de wettelijke beperkingen op deze bepaling en neemt deze hierbij in acht.					
f.* Bij inregelen van het proces is, zoveel als redelijkerwijs mogelijk en rekening houdend met de beschikbare technologie en de uitvoeringskosten, gericht op ‘privacy by design’ en ‘privacy by default’.					
g.* Conclusie:					

7.7* Recht op gegevenswissing (“recht op vergetelheid”)

7.8* Recht op beperking van de verwerking

7.9* Recht op overdraagbaarheid van gegevens (dataportabiliteit)

7.10* Recht op bezwaar en weigering geautomatiseerde besluitvorming (o.a. profilering)

III. Proces-Inventarisatie

Aandachtsgebieden

De onderstaande aandachtsgebieden kunnen afdelingen zijn of activiteiten op het genoemde gebied.

Processen kunnen een enkele bewerking van persoonsgegevens bevatten of een aantal verschillende bewerkingen die in de samenhang van een proces of activiteit bestaan. Zie ook de gegeven

voorbeelden bij ieder aandachtsgebied.

(AVG: Artikel 4, lid 1) Persoonsgegevens: Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (AVG: De betrokkene):

Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens (denk aan woonadres, postcode en woonplaats), een online identificator (denk ook aan e-mailadres, inlognaam, gebruikersnaam) of één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

Leiding

Commercieel

Op het gebied van marketing & communicatie, klantenservice, inkoop en verkoop bestaan processen waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin, zowel digitaal als fysiek).

Toelichting

Bijvoorbeeld: versturen van mailingen, nieuwsbrieven, contactformulieren op uw website, online enquetes, online inschrijfformulieren, tracking van gebruikers van uw website, bezoekersstatistieken, bewaren en gebruiken van gegevens van klanten en prospects, analyse van doelgroepen, organisatie evenementen, beheer inkoopcontacten en wat u daarbij van hen vastlegt, verspreiding gegevens inkopers (denk ook aan online aankopen), opvolging klant contacten, klachtafhandeling, opvolging wettelijke vereisten t.a.v. transparantie naar en uitoefening van rechten door betrokkenen.

Als u deze activiteiten binnen de organisatie uitvoert dan bent u de gegevensverantwoordelijke. Heeft u deze activiteiten uitbesteed dan bepaalt u de doeleinden en middelen en blijft u de gegevensverantwoordelijke. De organisatie aan wie het hebt uitbesteed is de verwerker waarmee u een verwerkingsovereenkomst dient af te sluiten.

Inventariseer en benoem de processen en geef aan of - en zo ja - in welke rol de organisatie binnen dit aandachtsgebied persoonsgegevens verwerkt. U kunt onderscheid maken tussen gegevensverantwoordelijke (u bepaalt de doeleinden en middelen voor de verwerking), u bent gegevensverantwoordelijke maar hebt het proces of de verwerking uitbesteed, u bent de verwerker (u verwerkt de persoonsgegevens in opdracht van een gegevensverantwoordelijke en bepaalt de doeleinden en middelen niet) of sub-verwerker (u verwerkt persoonsgegevens in opdracht van een verwerker).

Uitvoering

Op het gebied van productie en dienstverlening oftewel; datgene wat de organisatie levert, onderhoud, planning, werkvoorbereiding, magazijn, distributie en transport bestaan processen waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin, zowel digitaal als fysiek).

Toelichting

Bijvoorbeeld: Adres- en contactgegevens voor de uitvoering van diensten of het leveren van producten, capaciteitsplanning waarbij leeftijd of gezondheidsfactoren een rol kunnen spelen, competenties van personen en daarmee beslissingen over hun inzetbaarheid, klachtafhandeling, samenwerkingen, opvolging wettelijke vereisten.

Als u deze activiteiten binnen de organisatie uitvoert dan bent u de gegevensverantwoordelijke. Heeft u deze activiteiten uitbesteed dan bepaalt u de doeleinden en middelen en blijft u de gegevensverantwoordelijke. De organisatie aan wie het hebt uitbesteed is de verwerker waarmee u een verwerkingsovereenkomst dient af te sluiten.

Inventariseer en benoem de processen en geef aan of - en zo ja - in welke rol de organisatie binnen dit aandachtsgebied persoonsgegevens verwerkt. U kunt onderscheid maken tussen gegevensverantwoordelijke (u bepaalt de doeleinden en middelen voor de verwerking), u bent gegevensverantwoordelijke maar hebt het proces of de verwerking uitbesteed, u bent de verwerker (u verwerkt de persoonsgegevens in opdracht van een gegevensverantwoordelijke en bepaalt de doeleinden en middelen niet) of sub-verwerker (u verwerkt persoonsgegevens in opdracht van een verwerker).

Ondersteunend

Op het gebied van kantoorondersteuning (office management), financiële diensten en administratie, salarisadministratie, personeelszaken, gebouwen en faciliteiten, ICT services, informatiemanagement, juridische zaken, kwaliteitsmanagement en compliance bestaan processen waarin persoonsgegevens worden verwerkt (verzamelen, bewaren, gebruiken, verstrekken in brede zin, zowel digitaal als fysiek).

Toelichting

Bijvoorbeeld: het verzorgen van een mailing, verwerking online enquetes en inschrijfformulieren, de personeel- en salarisadministratie, C.V's en motivatiebrieven in wervingsprocedures, functioneringsgesprekken, in- en uitdienstprocessen, inzet flexwerkers of ZZP'ers (zijn juridisch mogelijk gegevensverwerkers), gedrags- en competentiemetingen t.b.v. ontwikkeling medewerkers al dan niet uitgevoerd door HR of externen, organisatie evenementen, toegangsbeheer voor gebouwen en systemen, samenwerkingen, opvolging ziekmeldingen en ARBO gerelateerde processen, klachtafhandeling, opvolging wettelijke vereisten.

Als u deze activiteiten binnen de organisatie uitvoert dan bent u de gegevensverantwoordelijke. Heeft u deze activiteiten uitbesteed dan bepaalt u de doeleinden en middelen en blijft u de gegevensverantwoordelijke. De organisatie aan wie het hebt uitbesteed is de verwerker waarmee u een verwerkingsovereenkomst dient af te sluiten.

Inventariseer en benoem de processen en geef aan of - en zo ja - in welke rol de organisatie binnen dit aandachtsgebied persoonsgegevens verwerkt. U kunt onderscheid maken tussen gegevensverantwoordelijke (u bepaalt de doeleinden en middelen voor de verwerking), u bent gegevensverantwoordelijke maar hebt het proces of de verwerking uitbesteed, u bent de verwerker (u verwerkt de persoonsgegevens in opdracht van een gegevensverantwoordelijke en bepaalt de doeleinden en middelen niet) of sub-verwerker (u verwerkt persoonsgegevens in opdracht van een verwerker).

Kennis & ontwikkeling

Overig

IV. Status (concluderend)

Status (concluderend)

Beoordeel aan de hand van uw vaststellingen of en zo ja; in welke mate, de organisatie in control en privacybestendig is en of daarbij aan wet- en regelgeving (AVG) wordt voldaan.

V. Praktische vragen & uitleg

Bron: Autoriteit Persoonsgegevens 2018.

De hier aangeboden praktische uitleg is bedoeld behulpzaam te zijn. De verschillende onderwerpen uit de AVG die direct voor u van belang zijn worden handzaam en begrijpelijk uitgelegd. De beschrijvingen zijn handvatten en kunnen niet worden opgevat als wettelijke bepalingen. Wettelijke bepalingen vindt u verderop.

Voorbereiden: 10 onderwerpen en stappen

De onderstaande 10 onderwerpen en stappen geven u een globaal beeld van waar de introductie van de AVG voor u om zal gaan.

1. Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

Bedenk dat de AP uw organisatie sancties kan opleggen van maximaal 20 miljoen euro of 4% van uw wereldwijde omzet als u zich niet aan de nieuwe privacywetgeving houdt.

2. Rechten van betrokkenen

Onder de AVG krijgen betrokkenen (de mensen van wie u persoonsgegevens verwerkt) meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Personen kunnen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

3. Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt.

Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten is onderdeel van de verantwoordingsplicht.

U kunt het register ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

4. Data protection impact assessment (DPIA)

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico’s van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico’s te verkleinen.

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt straks uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start.

Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

5. Privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van privacy by design en privacy by default en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzameld dan noodzakelijk voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

6. Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

7. Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan.

Dit gaat verder dan de huidige protocolplicht uit de Wet bescherming persoonsgegevens, die alleen betrekking heeft op de gemelde datalekken.

De Europese privacytoezichthouders hebben in oktober 2017 guidelines gepubliceerd over de meldplicht datalekken onder de AVG. Deze guidelines zijn nog niet definitief, maar staan open voor publieke consultatie. Wanneer de guidelines definitief zijn, kunnen wij u volledig informeren over de meldplicht datalekken onder de AVG.

8. Verwerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een verwerker? (nu nog 'bewerker' genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

9. Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

10. Toestemming

Uw gegevensverwerking kan gebaseerd zijn op toestemming van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan.

Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

Wanneer mag u persoonsgegevens verwerken

Wat wordt verstaan onder verwerken?

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

De grondslagen: heeft u het recht om persoonsgegevens te verwerken?

U mag alleen '**gewone**' persoonsgegevens verwerken wanneer u aan ten minste 1 van de 6 AVG-grondslagen voldoet.

1. Toestemming
2. Noodzakelijk voor de uitvoering van een overeenkomst
3. Noodzakelijk voor het nakomen van een wettelijke verplichting
4. Noodzakelijk ter bescherming van vitale belangen
5. Noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag
6. Noodzakelijk voor de behartiging van de gerechtvaardigde belangen

De verwerking van bijzondere en strafrechtelijke persoonsgegevens is verboden. Tenzij u zich kunt beroepen op een specifieke wettelijke uitzondering én één van de grondslagen voor het verwerken van 'gewone' persoonsgegevens.

Wanneer u zich op welke van de grondslagen voor het verwerken van 'gewone' persoonsgegevens kunt beroepen leest u in de volgende paragrafen.

1. Grondslag: Toestemming

Bijvoorbeeld: u vraagt gebruikers van uw foto-app toestemming om locatiegegevens te verzamelen.

Locatiegegevens zijn persoonsgegevens. Eén van de voorwaarden voor rechtsgeldige toestemming voor gegevensverwerking is dat mensen de vrije keuze moeten hebben om toestemming te geven.

In dit voorbeeld moet iemand een foto-app dus ook kunnen gebruiken zonder deze toestemming te geven. Het verzamelen van locatiegegevens is immers niet direct noodzakelijk voor het maken en bewerken van foto's.

Wanneer mag u zich baseren op de grondslag toestemming?

U heeft alleen het recht om (gewone) persoonsgegevens te verwerken als u zich kunt baseren op 1 van de 6 grondslagen uit de AVG. Eén van die grondslagen is 'toestemming'. De AVG schrijft niet precies voor in welke vorm u toestemming moet vragen. Maar de manier waarop u toestemming vraagt moet wel voldoen aan een aantal specifieke eisen.

Rechstgeldige toestemming voldoet aan de volgende eisen:

- Vrijelijk gegeven: u mag iemand niet onder druk zetten om toestemming te geven. Bijvoorbeeld door iemand te benadelen als hij of zij geen toestemming geeft. Let daarbij op machtsverhoudingen: een werknemer kan een vraag van zijn werkgever bijvoorbeeld moeilijk weigeren.
- Ondubbelzinnig: er moet sprake zijn van een duidelijke actieve handeling. Bijvoorbeeld een (digitale) schriftelijke of een mondelinge verklaring. Het moet in elk geval volstrekt helder zijn dát er toestemming is verleend. U mag niet uit gaan van het principe 'wie zwijgt, stemt toe'. Het gebruik van voor-aangevinkte vakjes is dus niet toegestaan.
- Geïnformeerd: u moet mensen informeren over:
    - de identiteit van u als organisatie;
    - het doel van elke verwerking waarvoor u toestemming vraagt;
    - welke persoonsgegevens u verzamelt en gebruikt;
    - het recht dat zij hebben om de toestemming weer in te trekken. U moet de informatie in een toegankelijke vorm aanbieden. Ook moet deze begrijpelijk zijn zodat iemand een weloverwogen keuze kan maken. Dat betekent dat u duidelijke en eenvoudige taal moet gebruiken.
    - Specifiek: toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel. Indien u als organisatie bij de verwerking meerdere doeleinden heeft, dient u de betrokkene hierover te informeren en betrokkene voor elk doel afzonderlijk toestemming te vragen. Het doel mag niet gaandeweg veranderen.
    - Het moet voor mensen net zo makkelijk zijn om de toestemming weer in te trekken als dat het was om de toestemming te geven.
    - U moet kunnen aantonen dat u geldige toestemming heeft verkregen.

Voldoet de toestemming niet aan deze eisen? Dan is de toestemming niet geldig. U mag de persoonsgegevens dan niet verwerken.

Toestemming bij kinderen

De AVG geeft kinderen jonger dan 16 jaar extra bescherming. Want kinderen kunnen de risico's van een gegevensverwerking niet of minder goed inschatten. Daarom moeten zij toestemming hebben van de persoon die de ouderlijke verantwoordelijkheid draagt.

Verantwoordingsplicht

Wilt u zich baseren op de grondslag toestemming? Zorg er dan voor dat u kunt aantonen dat u die toestemming op de juiste manier heeft gevraagd en gekregen. Onder de AVG heeft u namelijk een verantwoordingsplicht.

2. Grondslag: Noodzakelijk voor de uitvoering van een overeenkomst

Bijvoorbeeld: u heeft de adresgegevens van klanten nodig om de bestelde producten bij hen thuis te bezorgen. Deze gegevens zijn noodzakelijk om de overeenkomst met uw klanten na te kunnen komen.

Zorg ervoor dat u goed kunt onderbouwen dat u zich op deze grondslag mag baseren. Zijn de persoonsgegevens echt noodzakelijk voor de naleving van de overeenkomst met ieder betrokken individu?

Wanneer mag u zich baseren op de grondslag uitvoering overeenkomst?

U heeft alleen het recht om persoonsgegevens te verwerken als u zich kunt baseren op minimaal 1 van de 6 AVG-grondslagen. Eén van die grondslagen is 'noodzakelijk voor de uitvoering van een overeenkomst'.

U mag zich op deze grondslag baseren als u een overeenkomst heeft met iemand en hiervoor het verwerken van persoonsgegevens noodzakelijk is. De overeenkomst zelf mag niet gericht zijn op het verwerken van persoonsgegevens, maar moet een ander doel hebben.

Soms heeft u toestemming nodig.

Let op dat u geen persoonsgegevens verwerkt die niet noodzakelijk zijn voor de uitvoering daarvan. Doet u dat wel? Dan moet u daarvoor rechtsgeldige toestemming of een andere grondslag hebben.

Voorbeeld: als u online een product verkoopt, moet u adresgegevens verwerken om het product bij iemand te kunnen bezorgen. Wilt u de persoonsgegevens daarnaast ook nog gebruiken om het koopgedrag van iemand te analyseren? Dan moet u hiervoor rechtsgeldige toestemming hebben van de betrokken persoon.

Verantwoordingsplicht

Zijn de persoonsgegevens echt noodzakelijk voor de naleving van de overeenkomst met ieder betrokken individu? Zorg ervoor dat u goed kunt onderbouwen dat u zich op deze grondslag mag baseren. Onder de AVG heeft u namelijk een verantwoordingsplicht.

3. Grondslag: Noodzakelijk voor het nakomen van een wettelijke verplichting

4. Grondslag: Noodzakelijk ter bescherming van vitale belangen

5. Grondslag: Noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag

6. Grondslag: Noodzakelijk voor de behartiging van de gerechtvaardigde belangen

Welke persoonsgegevens mag u verwerken

Wat wordt verstaan onder persoonsgegevens?

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Mag u bijzondere persoonsgegevens verwerken?

De verwerking van bijzondere persoonsgegevens is verboden

Tenzij u zich kunt beroepen op een wettelijke uitzondering én één van de grondslagen voor het verwerken van 'gewone' persoonsgegevens.

Er zijn wettelijke uitzonderingen voor verwerkingen van bijzondere persoonsgegevens die strikt noodzakelijk en vanzelfsprekend zijn. Zoals voor het verwerken van medische gegevens door huisartsen en ziekenhuizen. Of voor het verwerken van lidmaatschap van een vakbond of politieke partij door die organisaties zelf.

Er zijn 10 wettelijke uitzonderingen op het verbod op het verwerken van bijzondere persoonsgegevens:

1. Uitdrukkelijke toestemming. Iemand kan uitdrukkelijke toestemming geven voor de verwerking van zijn of haar bijzondere persoonsgegevens voor het doel of de doelen die u heeft aangegeven;
2. Verwerkingen die noodzakelijk zijn voor de uitvoering van verplichtingen en het uitoefenen van arbeidsrecht en het sociale zekerheidsrecht zoals geregeld in de nationale wet;
3. Verwerkingen die noodzakelijk zijn om de vitale belangen te beschermen;
4. Verwerkingen voor gerechtvaardigde activiteiten door een instantie zonder winstoogmerk. De instantie moet wel passende waarborgen hebben ingebouwd en het mag alleen gaan om gegevensverwerkingen van (voormalige) leden of personen die regelmatig contact met de instantie onderhouden;
5. Verwerkingen van persoonsgegevens die door de betrokken personen zelf openbaar zijn gemaakt;
6. Verwerkingen die noodzakelijk zijn voor rechtsvordering of rechtsbevoegdheden;
7. Verwerkingen met een zwaarwegend algemeen belang. Daarbij moet u de evenredigheid en de inhoud van het recht op bescherming respecteren. Ook moet u de maatregelen treffen zoals geregeld in een nationale wet;
8. Verwerkingen die noodzakelijk voor de doelen gezondheidszorg, sociale diensten en arbeidsongeschiktheid, zoals geregeld in een nationale wet;
9. Verwerkingen die noodzakelijk zijn voor de volksgezondheid, zoals geregeld in een nationale wet;
10. Verwerkingen die noodzakelijk zijn voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statische doeleinden.

Wat verstaat de AVG onder bijzondere persoonsgegevens?

Persoonsgegevens die door hun aard bijzonder gevoelig zijn, krijgen ook onder de Algemene verordening gegevensbescherming (AVG) extra bescherming. Nieuw onder de AVG is dat ook genetische gegevens en biometrische gegevens hieronder vallen als deze herleidbaar zijn tot een persoon.

- De volgende persoonsgegevens ziet de AVG als bijzondere persoonsgegevens:
- Persoonsgegevens waaruit ras of etnische afkomst blijkt;
- Persoonsgegevens waaruit politieke opvattingen blijken;
- Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken;
- Persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt;
- Gegevens over gezondheid;
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid;
- Genetische gegevens;
- Biometrische gegevens met het oog op de unieke identificatie van een persoon.

Genetische persoonsgegevens

Genetische persoonsgegevens geven unieke informatie over iemands fysiologie of gezondheid en/of over de gezondheid van familieleden. Dat maakt de informatie zo gevoelig.

In de praktijk gaat het hierbij vooral om informatie over erfelijkheid en genetische kenmerken die het

resultaat is van een biologisch monster. Bijvoorbeeld informatie uit analyse van het DNA.

Biometrische persoonsgegevens

Biometrische persoonsgegevens geven unieke informatie over iemands fysieke, fysiologische of gedragsgerelateerde kenmerken. Dat maakt het zo gevoelig.

In de praktijk gaat het hierbij vooral om biometrische persoonsgegevens die het resultaat zijn van een specifieke technische verwerking waardoor de gegevens tot een individu herleidbaar zijn. Zoals bij vingerafdrukgegevens.

Speciale regels voor strafrechtelijke persoonsgegevens

Let op: anders dan onder de Wet bescherming persoonsgegevens, zijn strafrechtelijke persoonsgegevens geen bijzondere persoonsgegevens. Voor strafrechtelijke persoonsgegevens gelden onder de AVG specifieke eisen.

Mag u strafrechtelijke persoonsgegevens verwerken?

Mag u onder de AVG persoonsgegevens van kinderen verwerken?

Rechten van betrokkenen

Onder de Algemene verordening gegevensbescherming (AVG) krijgen mensen meer mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Hun bestaande privacyrechten worden uitgebreid en er gelden 2 nieuwe rechten. Bent u klaar voor verzoeken van personen die hun rechten willen uitoefenen?

De AVG-privacyrechten

1. Het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen (NIEUW).
2. Het recht op vergetelheid. Het recht om ‘vergeten’ te worden (NIEUW).
3. Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die u van hen verwerkt in te zien.
4. Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die u verwerkt te wijzigen.
5. Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken.
6. Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.
7. Het recht om bezwaar te maken tegen de gegevensverwerking.

Ten slotte hebben mensen recht op duidelijke informatie over wat u met hun persoonsgegevens doet. Onder de AVG moet u aan een aantal specifieke eisen voldoen.

Bent u voorbereid?

U moet uw systemen, processen en interne organisatie op deze (nieuwe) rechten inrichten. Zodat u vanaf 25 mei 2018 op de juiste manier gehoor kunt geven aan verzoeken van mensen die hun rechten uitoefenen. Hieronder vindt u meer informatie over de verschillende rechten. En wanneer en hoe u daar gehoor aan moet geven.

Hoe bereidt u zich voor op de (nieuwe) privacyrechten van mensen?

Onder de Algemene verordening gegevensbescherming (AVG) worden de privacyrechten van personen versterkt en uitgebreid. U moet uw systemen, processen en interne organisatie op deze (nieuwe) rechten inrichten. Zodat u vanaf 25 mei 2018 op de juiste manier gehoor kunt geven aan verzoeken van betrokkenen.

Waar moet u op letten?

Om volgens de regels op een verzoek te reageren moet u het volgende weten en doen:

- Weet u en weten uw eventuele medewerkers welke privacyrechten er gelden en wanneer u wel of niet gehoor hoeft te geven aan een verzoek?
- Weet u en weten uw eventuele medewerkers hoe u aan de verzoeken gaat voldoen? Bijvoorbeeld: op welke manier u mensen inzage gaat geven, hun gegevens wist of gaat overdragen. Mogelijk moet u daarvoor technische en organisatorische maatregelen nemen;
- Wijst u mensen op de privacyrechten die zij hebben? Bijvoorbeeld via uw privacystatement?
- Informeert u mensen duidelijk over hóe zij een verzoek bij u kunnen indienen?
- Is het voor mensen makkelijk om een verzoek bij u te doen? Wanneer iemand elektronisch (bijvoorbeeld per e-mail) een verzoek doet, dan moet u de gevraagde informatie ook elektronisch geven.
- Kunt u zo snel mogelijk maar in ieder geval binnen 1 maand* reageren op een verzoek? Concreet betekent dit dat u binnen die termijn ofwel het verzoek moet hebben uitgevoerd en de verzoeker hierover hebben geïnformeerd, of hebben aangegeven waarom u geen gehoor geeft aan het verzoek.

In uitzonderlijke gevallen mag u binnen 3 maanden reageren op een verzoek. Bijvoorbeeld wanneer een verzoek heel complex is. Of wanneer het aantal ontvangen verzoeken van dezelfde persoon extreem hoog is. Maar ook dan geldt dat u wel binnen 1 maand moet laten weten dat u meer tijd nodig heeft om op het verzoek te reageren.

Kosten

U mag in principe géén kosten berekenen. Maar kunt u bewijzen dat een verzoek ongegrond of buitensporig is? Bijvoorbeeld omdat iemand heel veel verzoeken bij u indient? Dan mag u een redelijke administratieve vergoeding vragen. Of het verzoek weigeren.

1. Het recht op dataportabiliteit.

2. Het recht op vergetelheid (wissing van gegevens)

Wat houdt het recht op vergetelheid uit de AVG in?

In Artikel 17 van de Algemene verordening gegevensbescherming (AVG) is het zogeheten recht op vergetelheid opgenomen. Dit recht houdt in dat organisaties in een aantal gevallen persoonsgegevens moeten wissen als een betrokkene (diegene van wie de organisatie gegevens verwerkt) erom vraagt.

Voorwaarden recht op vergetelheid

Het recht op vergetelheid geldt niet altijd. Alleen in de volgende situaties is het recht op vergetelheid van toepassing:

- Niet meer nodig
- De organisatie heeft de persoonsgegevens niet meer nodig voor de doeleinden waarvoor de organisatie ze heeft verzameld of waarvoor de organisatie ze verwerkt.
- Intrekken toestemming
- De betrokkene heeft eerder (uitdrukkelijke) toestemming gegeven aan de organisatie voor het gebruik van zijn gegevens, maar trekt die toestemming nu in.
- Bezwaar
- De betrokkene maakt bezwaar tegen de verwerking. Er geldt op grond van artikel 21 van de AVG een absoluut recht van bezwaar tegen direct marketing. En een relatief recht van bezwaar als de rechten van de betrokkene zwaarder wegen dan het belang van de organisatie om de persoonsgegevens te verwerken.

- Onrechtmatige verwerking
- De organisatie verwerkt de persoonsgegevens onrechtmatig. Bijvoorbeeld omdat er geen wettelijke grondslag is voor de verwerking.
- Wettelijk bepaalde bewaartermijn
- De organisatie is wettelijk verplicht om de gegevens na bepaalde tijd te wissen.
- Kinderen
- De betrokkene is jonger dan 16 jaar en de persoonsgegevens zijn verzameld via een app of website ('dienst van de informatiemaatschappij').

Verschil met nu

Het recht op vergetelheid lijkt op het huidige recht op correctie en verwijdering (artikel 36 van de Wet bescherming persoonsgegevens). Maar het recht op vergetelheid is breder. Het recht is niet meer – zoals nu – beperkt tot het verwijderen van objectief onjuiste gegevens, onvolledige gegevens of niet ter zake doende gegevens.

Wanneer geldt het recht op vergetelheid uit de AVG niet?

De Algemene verordening gegevensbescherming (AVG) noemt een aantal omstandigheden waarin het recht op vergetelheid niet geldt:

- De verwerking is noodzakelijk om het recht op vrijheid van meningsuiting en informatie uit te oefenen. Daarmee doet de AVG recht aan het principe dat privacy en vrijheid van meningsuiting gelijkwaardige grondrechten zijn.
- De organisatie verwerkt de gegevens omdat er een wettelijke verplichting is om dat te doen.
- De organisatie verwerkt de gegevens om openbaar gezag of een (wettelijk vastgelegde) taak van algemeen belang uit te oefenen.
- De organisatie verwerkt de gegevens voor een taak van algemeen belang op het gebied van de volksgezondheid.
- De organisatie moet de gegevens in het algemeen belang archiveren.
- De gegevens zijn noodzakelijk voor een rechtsvordering.

Algemene uitzonderingen privacyrechten

Daarnaast is in artikel 23 van de AVG een aantal algemene uitzonderingen opgenomen op de rechten van betrokkenen. Dit artikel lijkt op het huidige artikel 43 van de Wet bescherming persoonsgegevens.

Het artikel biedt organisaties de mogelijkheid om in bijzondere omstandigheden geen gehoor te geven aan verzoeken van betrokkenen. Zij moeten dan voor dat verzoek een belangenafweging maken waaruit blijkt dat hun belangen (of de rechten en vrijheden van anderen) zwaarder wegen dan het privacyrecht van de betrokkene.

Het is bijvoorbeeld niet de bedoeling dat betrokkenen met een beroep op hun rechten sporen van crimineel gedrag wissen.

Wat moet ik als organisatie doen als ik een verzoek krijg om gegevens te wissen?

Zodra de Algemene verordening gegevensbescherming (AVG) geldt, hebben betrokkenen (degenen van wie u gegevens verwerkt) het recht op vergetelheid. Vraagt iemand u op grond van dit recht om zijn gegevens te wissen? Dan moet u dat onmiddellijk doen, uiterlijk binnen een maand. Alleen als het om een heel complex verzoek gaat, heeft u twee maanden extra de tijd. U moet dan wel binnen een maand aan de betrokkene laten weten dat het langer gaat duren.

Manier van reageren

Als een betrokkene het verzoek elektronisch indient, moet u ook elektronisch reageren. Tenzij de betrokkene u vraagt om op een andere manier te reageren.

Kosten

U mag in principe géén kosten berekenen. Maar kunt u bewijzen dat een verzoek ongegrond of buitensporig is (veelvuldig herhaalde verzoeken van één persoon)? Dan mag u een redelijke administratieve vergoeding vragen. Of het verzoek weigeren.

Derde partijen informeren

Heeft u de betreffende persoonsgegevens aan derde partijen verstrekt? Dan moet u die ontvangers informeren dat u deze persoonsgegevens heeft gewist. En uitleggen dat ook de ontvangers iedere kopie van of koppeling naar die persoonsgegevens moeten wissen.

Publiceert u bijvoorbeeld persoonsgegevens via een website? Dan moet u zoekmachines informeren. U kunt daarbij de webpagina opnieuw laten indexeren, zodat de gewiste persoonsgegevens niet meer verschijnen in de zoekresultaten.

Als een betrokkene erom vraagt, moet u ook vertellen welke ontvangers u op die manier heeft geïnformeerd (artikel 19 van de AVG).

Vallen back-ups ook onder het recht op vergetelheid?

Ja. U moet het recht op vergetelheid ook toepassen op digitale back-upbestanden. Vraagt iemand u om zijn gegevens te wissen? Dan moet u zijn persoonsgegevens dus ook zo snel mogelijk uit uw back-ups verwijderen.

Zodra de Algemene verordening gegevensbescherming (AVG) geldt, hebben mensen het recht op vergetelheid. Dit houdt in dat u in bepaalde gevallen verplicht bent om iemands gegevens te verwijderen als diegene hierom vraagt. Bijvoorbeeld als de gegevens niet meer nodig zijn of als die persoon zijn toestemming intrekt.

Eisen aan back-ups

Zo gaat u goed om met back-ups onder de AVG:

- Inventariseer van welke gegevens u back-ups moet bijhouden, bijvoorbeeld vanwege uw beveiligingsbeleid. Houd er rekening mee dat u alleen gegevens mag verwerken die noodzakelijk zijn voor het doel van uw verwerking (zie artikel 5 van de AVG). U moet ook kunnen aantonen dat deze gegevens noodzakelijk zijn. Dat is onderdeel van uw verantwoordingsplicht.
- Maak regelmatig back-ups en verwijder systematisch verouderde gegevens.
- Informeer mensen goed over welke aanvullende bewaartermijn noodzakelijk is voor back-ups van uw specifieke dienstverlening. Bijvoorbeeld: u bewaart persoonsgegevens van klanten 1 jaar in uw reguliere systemen, maar hanteert aanvullend een bewaartermijn van 3 maanden voor uw back-ups.
- Richt uw back-upsysteem zo in dat u verwijderverzoeken van betrokkenen ook kan doorvoeren in dit systeem.
- Is het noodzakelijk voor uw dienstverlening om back-ups te maken die moeilijk of niet overschrijfbaar zijn, zoals tapes? Dan kunt u de persoonsgegevens niet verwijderen uit de back-ups. Zorg dan wel dat u goed bijhoudt welke persoonsgegevens u had moeten verwijderen. Is het onverhoopt nodig om een back-up terug te zetten? Dan moet u deze gegevens alsnog verwijderen.

Uitzonderingen

Er zijn ook uitzonderingen op het recht op vergetelheid. U hoeft de betreffende persoonsgegevens bijvoorbeeld niet uit uw back-ups te verwijderen als u wettelijk verplicht bent om de gegevens een bepaalde tijd te bewaren. Of als u ze moet archiveren in het algemeen belang.

3. Het recht op inzage

Wat houdt het recht op inzage in?

De Algemene verordening gegevensbescherming (AVG) geeft mensen meer zeggenschap over hun persoonsgegevens. Ze hebben het recht om u te vragen welke gegevens u van hen heeft. Ze mogen u ook vragen deze gegevens in te zien. In de AVG (artikel 15) staat dit recht beschreven als ‘recht op inzage’.

Bij inzageverzoeken moet u ook laten weten:

- Waarom u bepaalde gegevens verwerkt.
- Welke soorten persoonsgegevens u verzamelt.
- Indien van toepassing: aan welke organisaties u de persoonsgegevens doorgeeft. Dit geldt ook voor gegevens die u doorgeeft aan organisaties in andere landen of aan internationale organisaties.
- Hoe lang u de persoonsgegevens bewaart. Als u dat niet precies kunt aangeven, moet u duidelijk kunnen maken welke criteria u hanteert om een bewaartermijn te bepalen.
- Welke privacyrechten mensen hebben: het recht om hun persoonsgegevens te laten wijzigen, aanvullen of wissen, om u te vragen om minder persoonsgegevens te verwerken en om bezwaar te maken als u hun persoonsgegevens verwerkt.
- Dat mensen het recht hebben om een klacht in te dienen bij de Autoriteit Persoonsgegevens.
- Indien van toepassing: van welke organisatie u persoonsgegevens heeft ontvangen als u deze niet zelf heeft verzameld bij de betrokken personen.
- Indien van toepassing: op basis van welke logica u een geautomatiseerd besluit over iemand neemt.

4. Het recht op rectificatie

5. Recht op beperking van de verwerking

6. Het recht van bezwaar

7. Het recht op informatie

Wat houdt het recht op informatie in?

Onder de Algemene verordening gegevensbescherming (AVG) heeft u een informatieplicht. Dat betekent dat u verplicht bent om nieuwe en bestaande klanten duidelijk te informeren over wat u met hun persoonsgegevens doet.

Is een privacyverklaring volgens de AVG verplicht?

In de praktijk is een online privacyverklaring de meest handige manier om hier aan te voldoen.

Hoe wijst u mensen op uw privacyverklaring?

In de AVG staat dat u de informatie over uw verwerkingen in principe schriftelijk moet geven. De beste manier om er zeker van te zijn dat uw informatie voor de meeste mensen goed vindbaar is, is het publiceren van een online privacyverklaring. Daarnaast mag u andere middelen inzetten. Zoals het tonen van pop-ups met een toelichting bij elke toestemmingsvraag.

Apparaten zonder beeldscherm*

Verkoopt u een apparaat zonder beeldscherm? Dan kunt u er voor kiezen om op de verpakking van het apparaat de URL van uw privacyverklaring op te nemen. Of om het apparaat de belangrijkste onderdelen van uw privacyverklaring te laten voorlezen. Het is in ieder geval belangrijk dat u mensen

vóór de aanschaf van het apparaat wijst op uw online privacyverklaring en waar zij die kunnen vinden.

Let op: verwerkt u persoonsgegevens maar heeft u geen (online) privacyverklaring? Dan moet u ervoor zorgen dat u de betrokken personen op een andere manier de vereiste informatie geeft.

Verantwoordingsplicht

Onder de AVG geldt de verantwoordingsplicht. Dat betekent dat u aan de Autoriteit Persoonsgegevens (AP) moet kunnen aantonen dat u aan de AVG voldoet. U moet onder meer kunnen laten zien dat u mensen goed heeft geïnformeerd over de verwerking van hun persoonsgegevens. U kunt hiervoor uw privacyverklaring gebruiken.

Privacyverklaring

Hoe stelt u een privacyverklaring op?

De AVG stelt een aantal specifieke eisen waar een privacyverklaring aan moet voldoen. Deze eisen gaan over de inhoud, de toegankelijkheid en de duidelijkheid van de informatie.

Welke informatie moet er in een privacyverklaring staan?

In het document moet u in ieder geval de volgende informatie geven:

- De identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van uw vertegenwoordiger in de EU;
- De contactgegevens van de FG als u die heeft.
- De doeleinden en rechtsgrond van de verwerking, en als u zich beroept op een gerechtvaardigd belang: op welk belang u zich beroept.
- De (categorieën van) ontvangers van de persoonsgegevens.
- Of u van plan bent de persoonsgegevens door te geven buiten de EU of een internationale organisatie en op welke juridische grond.
- De bewaartermijn van de gegevens.
- De rechten van de betrokkene, zoals het recht op inzage, correctie en verwijdering. Zie ook stap 10.
- Het recht van de betrokkene om de gegeven toestemming voor een bepaalde verwerking altijd in te kunnen trekken.
- Dat de betrokkene een klacht kan indienen bij de relevante privacytoezichthouder.
- Of en waarom de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn als de gegevens niet worden verstrekt.
- Of u gebruik maakt van geautomatiseerde besluitvorming, inclusief profilering, en hoe u besluiten neemt.
- Als de gegevens van een andere organisatie zijn verkregen: de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

Hoe zorgt u dat u privacyverklaring toegankelijk is?

In de AVG staat dat u de informatie over uw verwerkingen in principe schriftelijk moet geven. De beste manier om er zeker van te zijn dat uw informatie voor de meeste mensen goed vindbaar is, is het publiceren van een online privacyverklaring.

Daarnaast mag u andere middelen inzetten om de inhoud van uw privacybeleid toegankelijk te maken. Zoals het tonen van pop-ups met een toelichting bij elke toestemmingsvraag. Of het gebruik van iconen of een video.

Tip: om de informatie in een (online) privacyverklaring zo toegankelijk mogelijk te maken, kunt u de

verklaring in meerdere lagen opstellen. Bijvoorbeeld:

- In de eerste laag geeft u kort aan wie de verantwoordelijke organisatie is, hoe die te bereiken is en welke gegevensverwerkingen de meeste impact hebben op de betrokken personen.
- In de tweede en derde laag van de privacyverklaring kunt u meer in detail aangeven welke persoonsgegevens u voor welk doel verwerkt en hoe mensen hun rechten kunnen uitoefenen.

Duidelijke taal

De informatie over de gegevensverwerking moet beknopt, transparant en begrijpelijk zijn. Daarom moet u duidelijke en eenvoudige taal gebruiken.

Dat betekent onder meer: wees kort en bondig,vermijd vaktermen en verplaats u in de lezer.

Richt u zich tot kinderen onder de zestien jaar? Of weet u dat kinderen uw diensten veel gebruiken? Dan moet u de woordkeuze, toon en stijl van de informatie aanpassen. Zodat de kinderen weten dat deze informatie voor hen is bedoeld en ze de informatie kunnen begrijpen.

Verantwoordingsplicht

De Algemene verordening gegevensbescherming (AVG) legt meer verantwoordelijkheid bij u als organisatie om aan te tonen dat u aan de privacyregels voldoet. Door te voldoen aan uw verantwoordingsplicht (accountability) levert u een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

De nieuwe regels dwingen u om goed na te denken over hoe uw organisatie persoonsgegevens verwerkt en beschermt. De verantwoordingsplicht houdt in dat u moet kunnen aantonen dat uw verwerkingen aan de regels van de AVG voldoen.

U moet bijvoorbeeld kunnen aantonen dat een verwerking aan de belangrijkste beginselen van verwerking voldoet, zoals:

- rechtmatigheid;
- transparantie;
- doelbinding;
- juistheid.

Ook moet u kunnen laten zien dat u de juiste technische en organisatorische maatregelen hebt genomen om de persoonsgegevens te beschermen.

U bent verplicht verantwoording af te leggen over uw gegevensverwerkingen wanneer de Autoriteit Persoonsgegevens daar om vraagt. Zorg daarom dat u aan uw verantwoordingsplicht voldoet vanaf 25 mei 2018. Vanaf dan geldt de AVG.

Hoe voldoe ik aan de verantwoordingsplicht?

In de Algemene verordening gegevensbescherming (AVG) staan een aantal verplichte maatregelen genoemd waarmee u aan uw verantwoordingsplicht (accountability) voldoet. Naast de verplichte maatregelen kunt u ervoor kiezen om extra maatregelen te nemen.

Verplichte maatregelen

De verplichte maatregelen die de AVG concreet noemt zijn:

- het bijhouden van een register van verwerkingsactiviteiten;
- het uitvoeren van een data protection impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacyrisico;

- het bijhouden van een register van datalekken die zijn opgetreden;
- het aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer u voor een verwerking toestemming nodig heeft.
- wanneer onduidelijk is of u verplicht bent om een Functionaris voor gegevensbescherming aan te stellen, moet u goed kunnen onderbouwen waarom u ervoor gekozen hebt om al dan niet een FG aan te stellen.

Meer informatie over deze verplichtingen vindt u in het AVG-dossier van de autoriteit persoonsgegevens (AP)en in de AVG zelf.

Extra maatregelen

Naast de verplichte maatregelen kunt u ervoor kiezen om extra maatregelen te nemen waarmee u aantoont dat u voldoet aan de eisen van de AVG. Bijvoorbeeld:

- het aansluiten bij een gedragscode;
- het behalen van een bepaald certificaat;
- het hanteren van een specifiek ICT-beveiligingsbeleid;
- het afleggen van verantwoording over de verwerking van persoonsgegevens in uw jaarverslag of in een speciaal privacy-jaarverslag.

Hoewel deze maatregelen niet verplicht zijn, helpen zij u wel om aan de toezichthouder te laten zien dat u voldoet aan de eisen van de AVG. Daarom moedigen wij deze vrijwillige maatregelen aan.

Ben ik verplicht om een register van verwerkingsactiviteiten op te stellen?

Het opstellen van een register van verwerkingsactiviteiten is onder de AVG vaak een verplichte maatregel. In het register staat informatie over de persoonsgegevens die u verwerkt. Of u zo'n register moet opstellen, hangt af van de omvang van uw organisatie en het type gegevens dat u verwerkt.

Let op: In de praktijk is vrijwel iedere organisatie verplicht een verwerkingsregister bij te houden!

Organisaties met meer dan 250 medewerkers

Heeft uw organisatie meer dan 250 medewerkers? Dan bent u verplicht om een register van verwerkingsactiviteiten bij te houden.

Organisaties met minder dan 250 medewerkers

Heeft uw organisatie minder dan 250 medewerkers? Dan moet u over een register beschikken wanneer u persoonsgegevens verwerkt:

- waarvan de verwerking niet incidenteel is. In de praktijk zijn verwerkingen zelden incidenteel. Denk bijvoorbeeld aan de persoonsgegevens van medewerkers die u verwerkt. Of van uw klanten, cliënten, patiënten of inwoners en/of;
- die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt en/of;
- die vallen onder de categorie bijzondere persoonsgegevens. Zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

Bent u verplicht om een register van verwerkingsactiviteiten op te stellen? Dan moet u dit register kunnen verstrekken wanneer de Autoriteit Persoonsgegevens daar om vraagt.

Wat moet er in het register van verwerkingsactiviteiten staan?

Aantonen gegeven toestemming

Verwerkersovereenkomst

Wanneer moet u een verwerkersovereenkomst opstellen?

Als u andere partijen inschakelt om persoonsgegevens voor u te verwerken, moet u met deze organisaties een 'verwerkersovereenkomst' afsluiten. Met een verwerkersovereenkomst sluit u uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken.

U mag alleen verwerkers inschakelen die voldoende garanties bieden dat zij aan de wettelijke vereisten voldoen. Maar let op: als u de gegevensverwerking door een verwerker laat uitvoeren, dan bent u nog steeds verantwoordelijk voor de naleving van de Algemene verordening gegevensbescherming (AVG).

Wat moet er in een verwerkersovereenkomst staan?

In de overeenkomst legt u onder meer het volgende vast:

- Het onderwerp en de duur van de gegevensverwerking.
- De aard en het doel van de gegevensverwerking.
- Het soort persoonsgegevens.
- De categorieën van betrokkenen.
- De rechten en verplichtingen van de verwerkingsverantwoordelijke.

Wat moet er in een verwerkersovereenkomst staan?

Maakt u, zodra de Algemene verordening gegevensbescherming (AVG) geldt, gebruik van de diensten van een verwerker (nu nog ‘bewerker’ genoemd)? Dan zijn u en de verwerker verplicht om een aantal onderwerpen vast te leggen in een schriftelijke overeenkomst (zie artikel 28, lid 3 van de AVG).

U moet de volgende onderwerpen vastleggen:

Algemene beschrijving

- Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en uw rechten en verplichtingen als verwerkingsverantwoordelijke (nu nog ‘verantwoordelijke’ genoemd).

Instructies verwerking

- De verwerking vindt in principe uitsluitend plaats op basis van uw schriftelijke instructies. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken.

Geheimhoudingsplicht

- Personen in dienst van of werkzaam voor de verwerker hebben een geheimhoudingsplicht.

Beveiliging

- De verwerker treft passende technische en organisatorische maatregelen om de verwerking te beveiligen. Bijvoorbeeld pseudonimisering en versleuteling van persoonsgegevens, permanente informatiebeveiliging, herstel van beschikbaarheid en toegang tot gegevens bij incidenten, regelmatige beveiligingstesten.

Subverwerkers

- De verwerker schakelt geen subverwerker(s) in zonder uw voorafgaande schriftelijke toestemming. De verwerker legt aan een subverwerker in een subverwerkersovereenkomst dezelfde verplichtingen op als de verwerker richting u heeft.

- In de overeenkomst kunt u ook direct afspreken dat, en onder welke voorwaarden, de verwerker subverwerkers mag inschakelen.
- Komt de subverwerker zijn verplichtingen niet na? Dan blijft de verwerker volledig aansprakelijk richting u voor het nakomen van de verplichtingen van de subverwerker (zie artikel 28, lid 4 van de AVG).

Privacyrechten

- De verwerker helpt u om te voldoen aan uw plichten als betrokkenen hun privacyrechten uitoefenen (zoals het recht op inzage, correctie, vergetelheid en dataportabiliteit).

Andere verplichtingen

- De verwerker helpt u ook om andere verplichtingen na te komen. Zoals bij het melden van datalekken, het uitvoeren van een data protection impact assessment (DPIA) en bij een voorafgaande raadpleging.

Gegevens verwijderen

- Na afloop van de verwerkingsdiensten verwijdert de verwerker de gegevens. Of bezorgt hij deze aan u terug, als u dat wilt. Ook verwijdert hij kopieën. Tenzij de verwerker wettelijk verplicht is de gegevens te bewaren.

Audits

- De verwerker werkt mee aan uw audits of die van een derde partij. En stelt alle relevante informatie beschikbaar om te kunnen controleren of hij zich als verwerker houdt aan de hierboven genoemde verplichtingen (uit artikel 28 AVG).

Gegevensbeschermingsbeleid

Wanneer is een gegevensbeschermingsbeleid volgens de AVG verplicht?

U bent alleen verplicht om een gegevensbeschermingsbeleid op te stellen als dat in verhouding staat tot uw verwerkingsactiviteiten. Een gegevensbeschermingsbeleid wordt ook wel privacybeleid genoemd. Of u verplicht bent om zo'n privacybeleid op te stellen, hangt af van de concrete omstandigheden. Zoals de aard, de omvang, de context en het doel van de gegevensverwerking.

Ziekenhuizen, gemeenten, social mediabedrijven en handelsinformatiebureaus zullen daarom vaak verplicht zijn om een gegevensbeschermingsbeleid op te stellen. Ook kleine organisaties kunnen verplicht zijn een gegevensbeschermingsbeleid op te stellen.

Vrijwillig opstellen van een gegevensbeschermingsbeleid

Bent u niet verplicht om een gegevensbeschermingsbeleid op te stellen? Dan kan het toch nuttig zijn om dat wél te doen. Het helpt u namelijk om te zien of u voldoende maatregelen heeft genomen om de persoonsgegevens van uw klanten, patiënten, cliënten e.d. te beschermen. Daarnaast is het een manier waarmee u aan zowel uw doelgroep als de Autoriteit Persoonsgegevens kunt laten zien dat u voldoet aan de AVG.

Let op: een gegevensbeschermingsbeleid is iets anders dan een privacyverklaring. Alle organisaties die persoonsgegevens verwerken, moeten mensen heldere informatie geven over de persoonsgegevens die zij verwerken en voor welk(e) doel(en) zij deze gegevens verwerken. De meest aangewezen manier hiervoor is het opstellen van een online privacyverklaring.

Wat moet er volgens de AVG in een gegevensbeschermingsbeleid staan?

In de Algemene verordening gegevensbescherming (AVG) staat niet precies omschreven welke gegevens u in uw gegevensbeschermingsbeleid (ook wel privacybeleid genoemd) moet opnemen. Uit het beleid moet in ieder geval wèl blijken hoe u voldoet aan de AVG. Dat is onderdeel van uw verantwoordingsplicht.

Informatie gegevensbeschermingsbeleid

U kunt laten zien hoe u voldoet aan de AVG door onder andere deze informatie op te nemen:

- een omschrijving van de categorieën persoonsgegevens die u verwerkt;
- een beschrijving van de doeleinden waarvoor u persoonsgegevens verwerkt en wat de juridische grondslag daarvan is;
- hoe u voldoet aan de beginselen van verwerking van persoonsgegevens. Zoals de verplichting om niet meer gegevens te verwerken dan noodzakelijk;
- welke rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen. Zoals het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Maar ook het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens;
- welke organisatorische en technische maatregelen u genomen heeft om de persoonsgegevens te beveiligen;
- hoe lang u de persoonsgegevens bewaart.

Het opstellen van een gegevensbeschermings- of privacybeleid is niet altijd verplicht. Toch kan het nuttig zijn om zo'n beleid wel op te stellen.

Beveiligen van persoonsgegevens en verwerkingen

Gedragscodes

Datalekken

Of u een datalek moet melden aan de toezichthouder (AP) en de betrokkene die het betreft, is afhankelijk van het risico van de inbreuk voor de betrokkene en of er aan bepaalde voorwaarden is voldaan. De voorwaarden voor het melden aan de toezichthouder en de betrokkene verschillen onderling. Voor het melden staat een maximale wettelijke termijn en de melding moet bepaalde informatie bevatten.

Belangrijk en nieuw is dat u i**eder datalek moet registreren** en dat u zich daarover op afroep direct moet kunnen verantwoorden naar de toezichthouder. Het beschikbaar hebben van de informatie over ieder datalek maakt onderdeel uit van de verantwoordingsplicht.

Wanneer moet u een datalek (inbreuk) melden bij de toezichthouder (AP)?

Wanneer moet u een datalek (inbreuk) mededelen aan een betrokkene die het betreft?

Data protection impact assessment (DPIA)

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dit moment kunnen organisaties verplicht zijn een data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

In de Nederlandse vertaling van de AVG wordt de term data protection impact assessment (DPIA) gegevensbeschermingseffectbeoordeling genoemd.

Groot privacyrisico

Organisaties hoeven, zodra de AVG geldt, niet voor elke gegevensverwerking een DPIA uit te voeren. Een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Dat is in ieder geval zo als een organisatie:

1. systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
2. op grote schaal bijzondere persoonsgegevens verwerkt;
3. op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Buiten deze drie situaties geeft de AVG geen overzicht van verwerkingen met een hoog risico. De Europese privacytoezichthouders hebben criteria opgesteld om het risico te bepalen. Daarnaast publiceert de Autoriteit Persoonsgegevens (AP) op termijn een lijst van verwerkingen waarvoor een DPIA verplicht is.

Guidelines DPIA

De Europese privacytoezichthouders hebben in oktober 2017 de (definitieve) Guidelines on Data Protection Impact Assessment gepubliceerd die meer uitleg geven over de DPIA. Er is ook een officiële Nederlandse vertaling van de guidelines DPIA beschikbaar.

Huidige situatie

De Rijksoverheid is nu al verplicht om bij de ontwikkeling van nieuwe wetgeving rekening te houden met de resultaten van een DPIA, nu nog Privacy Impact Assessment (PIA) genoemd. Andere organisaties zijn nu nog niet maar vanaf 25 mei 2018 verplicht een (D)PIA uit te voeren.

Het is aan te raden om vrijwillig een (D)PIA te doen. Dit komt niet alleen de gegevensbescherming ten goede, maar ook voor de organisatie zelf levert een (D)PIA voordelen op.

In welke gevallen moet ik een DPIA uitvoeren?

Als verantwoordelijke moet u een data protection impact assessment (DPIA) uitvoeren wanneer uw gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert. Dit moet u zelf bepalen. De werkgroep van Europese privacytoezichthouders (WP29) heeft een lijst van 9* criteria opgesteld om u hierbij te helpen.

9 criteria om te toetsen of u een DPIA moet uitvoeren

Als vuistregel kunt u hanteren dat u een DPIA moet uitvoeren als uw verwerking aan 2 of meer van de onderstaande 9 criteria voldoet.

1. Beoordelen van mensen op basis van persoonskenmerken

Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.

Voorbeelden hiervan zijn een bank die de kredietwaardigheid van klanten bepaalt (creditscoring), een bedrijf dat DNA-testen aan consumenten levert om gezondheidsrisico's te testen en een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.

2. Geautomatiseerde beslissingen

Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden

uitgesloten of gediscrimineerd.

Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium. In de aankomende WP29-guidelines over profiling volgt hierover meer uitleg.

3. Stelselmatige en grootschalige monitoring

Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimten aan deze gegevensverwerking te onttrekken.

4. Gevoelige gegevens

Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG), zoals informatie over iemands politieke voorkeuren. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.

5. Grootschalige gegevensverwerkingen

De AVG geeft geen definitie van ‘grootschalige gegevensverwerkingen’. WP29 adviseert om met de volgende criteria te bepalen of hiervan sprake is:

- de hoeveelheid mensen van wie gegevens worden verwerkt;
- de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt;
- de tijdsduur van de gegevensverwerking;
- de geografische reikwijdte van de gegevensverwerking.

In de AVG staat niet precies uitgelegd wat ‘grootschalig’ inhoudt. Wel geven de Europese toezichthouders een aantal voorbeelden van verwerkingen die zij als grootschalig zien.

- Bijvoorbeeld een ziekenhuis dat patiëntgegevens verwerkt of een bank die klantgegevens verwerkt als onderdeel van de gebruikelijke werkzaamheden.
- Verwerking van bijzondere persoonsgegevens door individuele artsen of advocaten (‘eenpitters’), zien de AP en de andere Europese privacytoezichthouders niet als een grootschalige verwerking.

6. Gekoppelde databases

Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.

7. Gegevens over kwetsbare personen

Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.

8. Gebruik van nieuwe technologieën

De AVG is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico’s.

De persoonlijke en maatschappelijke gevolgen van het gebruik van een nieuwe technologie kunnen zelfs nog onbekend zijn. Een DPIA helpt de verantwoordelijke dan om de risico’s te begrijpen en te

verhelpen. Sommige ‘Internet of Things’-toepassingen bijvoorbeeld kunnen een grote impact hebben op het dagelijks leven en de privacy van mensen, waardoor hierbij een DPIA nodig is.

9. Blokkering van een recht, dienst of contract

Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen:

- een recht niet kunnen uitoefenen of;
- een dienst niet kunnen gebruiken of;
- een contract niet kunnen afsluiten.
- Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.

Verantwoordingsplicht

Let op: deze 9 criteria zijn een handreiking om in te schatten of u een DPIA moet uitvoeren.**Ook als u aan slechts één of geen van deze criteria voldoet, moet u goed kunnen onderbouwen waarom u ervoor kiest om geen DPIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht.**

*In de definitieve guidelines die zijn vastgesteld in oktober 2017, is het 10e criterium ‘Doorgifte van persoonsgegevens buiten de EU’ vervallen. Ook legt de wet voor bestaande verwerkingen nu een link naar het ‘voorafgaand onderzoek’ onder de huidige privacywetgeving.

Wanneer hoef ik geen DPIA uit te voeren?

U hoeft geen data protection impact assessment (PIA) uit te voeren wanneer uw gegevensverwerking:

- Waarschijnlijk geen hoog privacyrisico oplevert.
- Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd.
- Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een DPIA is uitgevoerd. Tenzij de privacytoezichthouder oordeelt dat er toch een DPIA nodig is.
- Op een lijst staat van verwerkingen waarvoor een DPIA niet verplicht is. De AVG geeft de privacytoezichthouder de mogelijkheid om zo’n lijst op te stellen, maar dit is niet verplicht.

Moet ik alsnog een DPIA uitvoeren voor een bestaande verwerking?

Ja, soms moet u alsnog een data protection impact assessment (DPIA) uitvoeren voor een bestaande verwerking. Dat is als er iets verandert aan het risico van de gegevensverwerking. En de gegevensverwerking vervolgens (na de verandering) een hoog privacyrisico oplevert.

Geen DPIA nodig

U hoeft dus niet alsnog een DPIA uit te voeren als een van de volgende 3 situaties van toepassing is:

- uw gegevensverwerking levert waarschijnlijk géén hoog privacyrisico op; of
- u heeft voor deze verwerking al eens een voorafgaand onderzoek door de AP laten uitvoeren en de verwerking is in de tussentijd niet veranderd; of
- de risico's van de verwerking zijn niet veranderd.
- Verwerking verandert

Uw verwerking verandert bijvoorbeeld als u een nieuwe technologie gaat gebruiken. Of als u persoonsgegevens voor een ander doel gaat gebruiken. In deze situaties verandert uw gegevensverwerking feitelijk in een nieuwe gegevensverwerking. En dan kan een DPIA verplicht zijn.

Risico verandert

Verandert het privacyrisico van uw verwerking? Dan kunt u ook verplicht zijn alsnog een DPIA uit te

voeren. Risico's kunnen bijvoorbeeld veranderen omdat een onderdeel van het verwerkingsproces wijzigt. De technologische ontwikkelingen gaan snel, waardoor nieuwe kwetsbaarheden kunnen ontstaan.

Omgeving verandert

Tot slot kunt u alsnog verplicht zijn een DPIA uit te voeren omdat de organisatie- of maatschappelijke context verandert. Bijvoorbeeld omdat de gevolgen van bepaalde geautomatiseerde beslissingen belangrijker zijn geworden of omdat er nieuwe categorieën mensen kwetsbaar worden voor discriminatie.

Periodieke DPIA

Vanwege de hierboven genoemde veranderingen is het sowieso aan te raden om periodiek een DPIA uit te voeren. Ook als de gegevensverwerking zelf niet is veranderd. Bijvoorbeeld een keer per 3 jaar.

Op welk moment moet ik een DPIA uitvoeren

Start met het data protection impact assessment (DPIA) zo vroeg als praktisch gezien mogelijk is in de ontwerpfase van de gegevensverwerking. Ook als nog niet alle details van de verwerking bekend zijn. Door vroeg te beginnen, is het voor u makkelijker om aan de wettelijk vereiste principes van privacy by design en privacy by default te voldoen.

Continu proces

Let op: dat u de DPIA misschien gaandeweg moet aanpassen, is geen argument om de DPIA uit te stellen of achterwege te laten. Een DPIA uitvoeren is geen eenmalige opdracht, maar een continu proces. U zult altijd moeten (blijven) monitoren of uw gegevensverwerking wijzigt en of u daarom de DPIA moet bijstellen.

Wie moet een DPIA uitvoeren?

Op welke manier moet ik een DPIA uitvoeren?

Moet ik de DPIA publiceren?

Wanneer is een voorafgaande raadpleging nodig?

Functionaris voor de gegevensbescherming (FG)

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dit moment kunnen organisaties verplicht zijn een functionaris voor de gegevensbescherming (FG) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Op grond van artikel 37 van de AVG is een FG in drie situaties verplicht.

1. **Overheden en publieke organisaties** Ten eerste zijn overheidsinstanties en publieke organisaties altijd verplicht om een FG aan te stellen, ongeacht het type gegevens dat ze verwerken. Het kan gaan om de rijksoverheid, gemeenten en provincies, maar ook om bijvoorbeeld zorg- en onderwijsinstellingen. Voor rechtbanken geldt de verplichte aanstelling van een FG niet.
2. **Observatie** Ten tweede geldt de verplichting om een FG aan te stellen voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen. Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via wearables. Relevant hierbij zijn onder meer het aantal mensen dat een organisatie volgt, de hoeveelheid gegevens die deze organisatie verwerkt en hoe lang de

organisatie mensen volgt.

3. **Bijzondere persoonsgegevens** Ten derde zijn organisaties verplicht een FG te benoemen als ze op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden.

Andere situaties

EU-lidstaten kunnen ook andere situaties benoemen waarin een FG verplicht is. Het is nog niet bekend of dit in Nederland gaat gebeuren. Wanneer onduidelijk is of u verplicht bent om een FG aan te stellen, moet u goed kunnen onderbouwen waarom u ervoor gekozen hebt om dat wel of niet te doen.

Guidelines FG

De Europese privacytoezichthouders hebben in april 2017 de (definitieve) Guidelines on Data Protection Officers gepubliceerd die meer uitleg geven over de FG. Er is ook een officiële Nederlandse vertaling van de guidelines FG beschikbaar.

VI. AVG - Wet- en regelgeving

Algemene Verordening Gegevensbescherming (AVG)

VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016

betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

(Voor de EER relevante tekst)

Weergegeven delen van de AVG:

Hoofdstuk 1 t/m Hoofdstuk 5, zijnde Artikel 1 t/m Artikel 50.

Hoofdstuk 1: Algemene bepalingen

Art. 1: Onderwerp en doelstellingen

1. Bij deze verordening worden regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens.
2. Deze verordening beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens.
3. Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens.

Art. 2: Materieel toepassingsgebied

1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
2. Deze verordening is niet van toepassing op de verwerking van persoonsgegevens:

- a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;

- b) door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen;

- c) door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit;
- d)door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

1. Op de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie is Verordening (EG) nr. 45/2001 van toepassing. Verordening (EG) nr. 45/2001 en andere rechtshandelingen van de Unie die van toepassing zijn op een dergelijke verwerking van persoonsgegevens worden overeenkomstig artikel 98 aan de beginselen en regels van de onderhavige verordening aangepast.
2. Deze verordening laat de toepassing van Richtlijn 2000/31/EG, en met name van de regels in de artikelen 12 tot en met 15 van die richtlijn betreffende de aansprakelijkheid van als tussenpersoon optredende dienstverleners onverlet.

Art. 3 Territoriaal toepassingsgebied

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

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

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

Art. 4 Definities

1) „persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

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

3) „beperken van de verwerking": het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken;

4) „profilering": elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden

geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

5) „pseudonimisering": het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

6) „bestand": elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

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

8) „verwerker": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

9) „ontvanger": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk 4.5.2016 L 119/33 Publicatieblad van de Europese Unie NL persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidsta telijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;

10) „derde": een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;

11) „toestemming" van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

12) „inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

13) „genetische gegevens": persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;

14) „biometrische gegevens": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;

15) „gegevens over gezondheid": persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

16) „hoofdvestiging":
a) met betrekking tot een verwerkingsverantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslissingen over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd;

b) met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten;

17) „vertegenwoordiger": een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;

18) „onderneming": een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;

19) „concern": een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend;

20) „bindende bedrijfsvoorschriften": beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meerderde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen;

21) „toezichthoudende autoriteit": een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie;

22) „betrokken toezichthoudende autoriteit": een toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens omdat:

a) de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd;
b) de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of
d) bij die toezichthoudende autoriteit een klacht is ingediend;
e)
23) „grensoverschrijdende verwerking":

a) verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; 24) „relevant en gemotiveerd bezwaar": een bezwaar tegen een ontwerpbesluit over het bestaan van een inbreuk op deze verordening of over de vraag of de voorgenomen maatregel met betrekking tot de verwerkingsverantwoordelijke of de verwerker strookt met deze verordening, waarin duidelijk de omvang wordt aangetoond van de risico's die het ontwerpbesluit inhoudt voor de grondrechten en de fundamentele vrijheden van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie;25) „dienst van de informatiemaatschappij": een dienst als

gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad (1);

26) „internationale organisatie": een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.

Hoofdstuk 2: Beginselen

Art. 5 Beginselen inzake verwerking van persoonsgegevens

1. Persoonsgegevens moeten:

a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie");
b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding");
c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking");
d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren („juistheid"); (1) Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PB L 241 van 17.9.2015, blz. 1).
e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen („opslagbeperking");
f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").

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

Art. 6 Rechtmatigheid van de verwerking

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

a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

2. De lidstaten kunnen specifiekere bepalingen handhaven of invoeren ter aanpassing van de manier waarop de regels van deze verordening met betrekking tot de verwerking met het oog op de naleving van lid 1, punten c) en e), worden toegepast; hiertoe kunnen zij een nadere omschrijving geven van specifieke voorschriften voor de verwerking en andere maatregelen om een rechtmatige en behoorlijke verwerking te waarborgen, ook voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX.

1. De rechtsgrond voor de in lid 1, punten c) en e), bedoelde verwerking moet worden vastgesteld bij:
a) Unierecht; of
b) lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is.
Het doel van de verwerking wordt in die rechtsgrond vastgesteld of is met betrekking tot de in lid 1, punt e), bedoelde verwerking noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslag perioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, zoals die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX. Het Unierecht of het lidstatelijke recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.

4. Wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld niet berust op toestemming van de betrokkene of op een Unierechtelijke bepaling of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, lid 1, bedoelde doelstellingen houdt de verwerkingsverantwoordelijke bij de beoordeling van de vraag of de verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld onder meer rekening met:

a) ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld, en de doeleinden van de voorgenomen verdere verwerking;
b) het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft;
c) de aard van de persoonsgegevens, met name of bijzondere categorieën van persoonsgegevens worden verwerkt, overeenkomstig artikel 9, en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt, overeenkomstig artikel 10;
d) de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen;
e) het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

Art. 7 Voorwaarden voor toestemming

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

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

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

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

Art. 8 Voorwaarden voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij

1. Wanneer artikel 6, lid 1, punt a), van toepassing is in verband met een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, is de verwerking van persoonsgegevens van een kind rechtmatig wanneer het kind ten minste 16 jaar is. Wanneer het kind jonger is dan 16 jaar is zulke verwerking slechts rechtmatig indien en voor zover de toestemming of machtiging tot toestemming in dit verband wordt verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. De lidstaten kunnen dienaangaande bij wet voorzien in een lagere leeftijd, op voorwaarde dat die leeftijd niet onder 13 jaar ligt.

2. Met inachtneming van de beschikbare technologie doet de verwerkingsverantwoordelijke redelijke inspanningen om in dergelijke gevallen te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.

3. Lid 1 laat het algemene overeenkomstenrecht van de lidstaten, zoals de regels inzake de geldigheid, de totstandkoming of de gevolgen van overeenkomsten ten opzichte van kinderen, onverlet.

Art. 9 Verwerking van bijzondere categorieën van persoonsgegevens

Art. 10 Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

Art. 11 Verwerking waarvoor identificatie niet is vereist

Hoofdstuk 3: Rechten van de betrokkene

Afd. 1 Transparantie en regelingen

Art. 12 Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene

1. De verwerkingsverantwoordelijke neemt passende maatregelen opdat de betrokkene de in de artikelen 13 en 14 bedoelde informatie en de in de artikelen 15 tot en met 22 en artikel 34 bedoelde communicatie in verband met de verwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is. De informatie wordt schriftelijk of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen, verstrekt. Indien de betrokkene daarom verzoekt, kan de informatie mondeling worden meegedeeld, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is.

2. De verwerkingsverantwoordelijke faciliteert de uitoefening van de rechten van de betrokkene uit hoofde van de artikelen 15 tot en met 22. In de in artikel 11, lid 2, bedoelde gevallen mag de verwerkingsverantwoordelijke niet weigeren gevolg te geven aan het verzoek van de betrokkene om diens rechten uit hoofde van de artikelen 15 tot en met 22 uit te oefenen, tenzij de verwerkingsverantwoordelijke aantoont dat hij niet in staat is de betrokkene te identificeren.

3. De verwerkingsverantwoordelijke verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek krachtens de artikelen 15 tot en met 22 informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

4. Wanneer de verwerkingsverantwoordelijke geen gevolg geeft aan het verzoek van de betrokkene, deelt hij deze laatste onverwijld en uiterlijk binnen één maand na ontvangst van het verzoek mee waarom het verzoek zonder gevolg is gebleven, en informeert hij hem over de mogelijkheid om klacht in te dienen bij een toezichthoudende autoriteit en beroep bij de rechter in te stellen.

5. Het verstrekken van de in de artikelen 13 en 14 bedoelde informatie, en het verstrekken van de communicatie en het treffen van de maatregelen bedoeld in de artikelen 15 tot en met 22 en artikel 34 geschieden kosteloos. Wanneer verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag de verwerkingsverantwoordelijke ofwel:
a) een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie en het treffen van de gevraagde maatregelen gepaard gaan; ofwel
b) weigeren gevolg te geven aan het verzoek.
Het is aan de verwerkingsverantwoordelijke om de kennelijk ongegronde of buitensporige aard van het verzoek aan te tonen.

6. Onverminderd artikel 11 kan de verwerkingsverantwoordelijke, wanneer hij redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het verzoek indient als bedoeld in de artikelen 15 tot en met 21, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

7. De krachtens de artikelen 13 en 14 aan betrokkenen te verstrekken informatie mag worden verstrekt met gebruikmaking van gestandaardiseerde iconen, om de betrokkene een nuttig overzicht, in een goed zichtbare, begrijpelijke en duidelijk leesbare vorm, van de voorgenomen verwerking te bieden. Wanneer de iconen elektronisch worden weergegeven, zijn ze machine leesbaar.

8. De Commissie is bevoegd overeenkomstig artikel 92 gedelegeerde handelingen vast te stellen om te bepalen welke informatie de iconen dienen weer te geven en via welke procedures de gestandaardiseerde iconen tot stand dienen te komen.

Afd. 2 Informatie en toegang tot persoonsgegevens

Art. 13 Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden

verzameld

Art. 14 Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen

Art. 15 Recht van inzage van de betrokkene

1. De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens en van de volgende informatie:
a) de verwerkingsdoeleinden;
b) de betrokken categorieën van persoonsgegevens;
c) de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
d) indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
e) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
f) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
g) wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
h) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

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

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

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

Afd. 3 Rectificatie en wissing van gegevens

Art. 16 Recht op rectificatie

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

Art. 17 Recht op gegevenswissing („recht op vergetelheid”)

1. De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende

gevallen van toepassing is:
a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt; 4.5.2016 L 119/43 Publicatieblad van de Europese Unie NL
b) de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), berust, in, en er is geen andere rechtsgrond voor de verwerking;
c) de betrokkene maakt overeenkomstig artikel 21, lid 1, bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking, of de betrokkene maakt bezwaar tegen de verwerking overeenkomstig artikel 21, lid 2;
d) de persoonsgegevens zijn onrechtmatig verwerkt;
e) de persoonsgegevens moeten worden gewist om te voldoen aan een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
f) de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij als bedoeld in artikel 8, lid 1.

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

3. De leden 1 en 2 zijn niet van toepassing voor zover verwerking nodig is:
a) voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
b) voor het nakomen van een in een het Unierecht of het lidstatelijke recht neergelegde wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;
c) om redenen van algemeen belang op het gebied van volksgezondheid overeenkomstig artikel 9, lid 2, punten h) en i), en artikel 9, lid 3;
d) met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, voor zover het in lid 1 bedoelde recht de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen;
e)voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Art. 18 Recht op beperking van de verwerking

1. De betrokkene heeft het recht van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen indien een van de volgende elementen van toepassing is:
a) de juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te controleren;
b) de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
c) de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
d) de betrokkene heeft overeenkomstig artikel 21, lid 1, bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

2. Wanneer de verwerking op grond van lid 1 is beperkt, worden persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerkt met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.

3. Een betrokkene die overeenkomstig lid 1 een beperking van de verwerking heeft verkregen, wordt door de verwerkingsverantwoordelijke op de hoogte gebracht voordat de beperking van de verwerking wordt opgeheven.

Art. 19 Kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking

Art. 20 Recht op overdraagbaarheid van gegevens

Afd. 4 Recht van bezwaar en geautomatiseerde individuele besluitvorming

Art. 21 Recht van bezwaar

Art. 22 Geautomatiseerde individuele besluitvorming, waaronder profilering

Afd. 5 Beperkingen

Art. 23 Beperkingen

Hoofdstuk 4: Verwerkingsverantwoordelijke en verwerker

Afd. 1 Algemene verplichtingen

Art. 24 Verantwoordelijkheid van de verwerkingsverantwoordelijke

1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.
3. Het aansluiten bij goedgekeurde gedragscodes als bedoeld in artikel 40 of goedgekeurde certificeringsmechanismen als bedoeld in artikel 42 kan worden gebruikt als element om aan te tonen dat de verplichtingen van de verwerkingsverantwoordelijke zijn nagekomen.

Art. 25 Gegevensbescherming door ontwerp en door standaardinstellingen

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

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

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

Art. 26 Gezamenlijke verwerkingsverantwoordelijken

1. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de in de artikelen 13 en 14 bedoelde informatie te verstrekken, door middel van een onderlinge regeling, tenzij en voor zover de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijken zijn vastgesteld bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijken van toepassing is. In de regeling kan een contactpunt voor betrokkenen worden aangewezen.

2. Uit de in lid 1 bedoelde regeling blijkt duidelijk welke rol de gezamenlijke verwerkingsverantwoordelijken respectievelijk vervullen, en wat hun respectieve verhouding met de betrokkenen is. De wezenlijke inhoud van de regeling wordt aan de betrokkene beschikbaar gesteld.

3. Ongeacht de voorwaarden van de in lid 1 bedoelde regeling, kan de betrokkene zijn rechten uit hoofde van deze verordening met betrekking tot en jegens iedere verwerkingsverantwoordelijke uitoefenen.

Art. 27 Vertegenwoordigers van niet in de Unie gevestigde verwerkingsverantwoordelijken of verwerkers

Art. 28 Verwerker

Art. 29 Verwerking onder gezag van de verwerkingsverantwoordelijke of de verwerker

Art. 30 Register van de verwerkingsactiviteiten

Art. 31 Medewerking met de toezichthoudende autoriteit

Afd. 2 Persoonsgegevensbeveiliging

Art. 32 Beveiliging van de verwerking

Art. 33 Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

Art. 34 Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene

Art. 35 Gegevensbeschermingseffectbeoordeling

Hoofdstuk 5: Doorgiften van persoonsgegevens aan derde landen of internationale organisaties