AVG

Algemene Verordening Gegevensbescherming

Praktisch naslagwerk en tips

Uitgavedatum: januari 2018

gevolgen van het handelen op grond van informatie uit dit document. Aan de informatie in dit document kunnen op geen enkele wijze rechten of aanspraken ontleend worden.

Inhoudsopgave

Inleiding 6

1. Houd een register van verwerkingsactiviteiten bij 7
2. Bepaal de noodzaak van een Functionaris voor Gegevensbescherming (FG) 7
3. Leg de verwerkingsgrond vast 8
4. Bepaal het risico van de verwerking 9
5. Doe aan privacy by design/default 9
6. Herzie de privacyverklaring 9
7. Check de beveiliging 9
8. Maak schriftelijke afspraken met verwerkende externen 10
9. Richt een procedure datalekken in 10
10. Stel procedures op voor rechtenuitoefening door betrokkenen 12

Bijlage 1 – Definities 13
Bijlage 2 – Eisen Verwerkingsregisters 15
Bijlage 3 – Rechtmatige verwerkingsgronden persoonsgegevens 17
Bijlage 4 – Wettelijke uitzonderingen verwerking bijzondere persoonsgegevens 18
Bijlage 5 – Data protection impact assessment (DPIA) 20
Bijlage 6 – Eisen privacyverklaring 21
Bijlage 7 – Voorbeeld instructies gegevensbeveiliging voor medewerkers 22
Bijlage 8 – Voorbeeld afhandeling recht op inzage 23
Bijlage 9 – Voorbeeld afhandeling recht op rectificatie 24
Bijlage 10 – Voorbeeld afhandeling recht op gegevenswissing 25
Bijlage 11 – Voorbeeld afhandeling recht op beperking van de verwerking 26
Bijlage 12 – Voorbeeld afhandeling recht op overdraagbaarheid van gegevens 27
Bijlage 13 – Voorbeeld afhandeling recht op bezwaar – specifieke situatie 29
Bijlage 14 – Voorbeeld afhandeling recht op bezwaar – direct marketing 30

Nieuwe privacywetgeving vanaf 25 mei 2018
De AVG in een notendop

Op basis hiervan mag je persoonsgegevens verzamelen
De grondslag

- Toestemming van de gebruiker
- Vitale belangen
- Wettelijke verplichting
- Overeenkomst
- Algemeen belang
- Gerechtvaardigd belang

Het begint aan de tekentafel
Zorgvuldigheid

- Functionaris gegevens-bescherming
- Privacy by design
- Impact assessment

Technische en organisatorische maatregelen
Verplichtingen

- Register met alle verwerkingen
- Gegevens-beschermingsbeleid
- (Digitale) beveiliging

Mensen moeten controle kunnen uitoefenen
Rechten van de betrokkenen

- Recht om in te zien
- Recht om te wijzigen
- Recht om vergeten te worden
- Recht om gegevens over te dragen
- Recht op informatie

De AVG geldt vanaf 25 mei 2018

Gegevens zijn beschermd!

U heeft een goed privacyverhaal

- Voor uw doelgroep
- Voor de Autoriteit Persoonsgegevens

Inleiding

Met de overgang van de Wet bescherming persoonsgegevens (Wbp) naar de Algemene Verordening Gegevensbescherming (AVG) per 25 mei 2018 veranderen de regels rondom de verwerking van persoonsgegevens. Organisaties moeten dan zelf goed kunnen aantonen dat zij voldoen aan de privacyregels. De privacyrechten van personen en de bevoegdheden van de toezichthouder, de Autoriteit Persoonsgegevens (AP), worden uitgebreid. En tenslotte worden de boetes hoger.

Gezien de intensieve verwerking van persoonsgegevens en de maatschappelijke functie is het belangrijk dat u goed op de hoogte bent van de nieuwe eisen en dat u deze toepast. Doel van dit document is om uw organisatie te helpen bij de praktische toepassing van de nieuwe en reeds bestaande privacyregels. Tevens verwijzen wij u naar goede hulpmiddelen waarmee uw organisatie op een goede en efficiënte manier aan de AVG-verplichtingen kan voldoen.

In de hoofdstukken 1 t/m 5 behandelen we een aantal praktische maatregelen. Belangrijke definities zijn opgenomen in bijlage 1. De overige bijlagen geven meer achtergrondinformatie over de diverse onderdelen van de wet of de toepassing ervan.

1. Houd een register van verwerkingsactiviteiten bij

De AVG legt alle organisaties een verantwoordingsplicht op. Dit houdt in dat een organisatie met documenten moet kunnen aantonen dat de juiste organisatorische en technische maatregelen zijn genomen om aan de AVG te voldoen.

In de AVG staan een aantal verplichte maatregelen genoemd waarmee een organisatie aan zijn verantwoordingsplicht kan voldoen. Een van die verplichtingen is het 'register van verwerkingsactiviteiten'. Of uw organisatie verplicht is zo'n Verwerkingsregister op te stellen, hangt af van de omvang van uw organisatie en het type gegevens dat wordt verwerkt.

Heeft uw organisatie meer dan 250 medewerkers? Dan is uw organisatie verplicht om een Verwerkingsregister bij te houden.

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

- die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie uw organisatie persoonsgegevens verwerkt en/of;
- waarvan de verwerking niet incidenteel is en/of;
- die vallen onder de categorie bijzondere persoonsgegevens, zie bijlage 1. Zoals gegevens over godsdienst, gezondheid en politieke voorkeur of strafrechtelijke gegevens.

De verwerking van persoonsgegevens zal bij dierenartspraktijken niet incidenteel zijn, waardoor een Verwerkingsregister verplicht is.

De eisen aan een Verwerkingsregister zijn afhankelijk van de rol die de organisatie speelt bij de gegevensverwerking. Is uw organisatie de verwerkingsverantwoordelijke of de verwerker. Uw rol bepaalt welke stappen uw organisatie verder moet nemen. Als u zelf het doel van en de middelen voor gegevensverwerking bepaalt, dan bent u de verwerkingsverantwoordelijke. Vermoedelijk zal dit vaak het geval zijn bij een dierenartspraktijk.

Bijlage 2 bevat een overzicht van de wettelijke eisen aan het Verwerkingsregister van zowel de verwerkingsverantwoordelijke als de verwerker.

Er zijn diverse hulpmiddelen beschikbaar om het inrichten van een Verwerkingsregister makkelijker te maken. Een van deze hulpmiddelen is bijvoorbeeld PrivacyBlox (zie: https://privacyblox.nl). Met PrivacyBlox kunt u eenvoudig het verplichte verwerkingsregister opzetten. Met behulp van een interactieve vragenlijst wordt de relevante informatie verzameld. Hierdoor weet u welke verwerkingen plaatsvinden, welke aandachtspunten er zijn en welke actie nodig is.

2. Bepaal de noodzaak van een Functionaris voor Gegevensbescherming (FG)

Een FG is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. In de volgende gevallen, is een FG verplicht (deze gevallen zijn niet van toepassing op de dierenartspraktijk, maar dit zou in de toekomst kunnen wijzigen als er aanvullende situaties benoemd zouden worden):

1. Overheden en publieke organisaties
   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.
2. Observatie

Organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen, zijn verplicht een FG aan te stellen. Het kan hierbij bijvoorbeeld gaan om profiling van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via wearables.

3. Bijzondere persoonsgegevens
   Organisaties die op grote schaal bijzondere persoonsgegevens verwerken en waar dit een kernactiviteit is, zijn verplicht een FG te benoemen.

   De FG kan een personeelslid zijn, of een persoon die de taken op grond van een dienstverleningsovereenkomst verricht. Om belangenverstrengeling te voorkomen, mag de FG binnen de organisatie niet ook een functie hebben waarin hij het doel en de middelen van een gegevensverwerking bepaalt.

   Deel de contactgegevens van de FG mee aan de toezichthoudende autoriteit. De FG wordt daar opgenomen in een register.

   Een FG is een deskundige op het gebied van de gegevensbescherming en vervult ten minste de volgende **taken**:

   a. informeren en adviseren van de mensen binnen de organisatie over de verplichtingen die voortvloeien uit de AVG.
   b. toezien op naleving van deze verordening en van het gegevensbeschermingsbeleid van de organisatie.
   c. toewijzen van verantwoordelijkheden.
   d. bewustmaken en opleiden van het personeel betrokken bij de verwerking en de audits.
   e. advies verstrekken met betrekking tot de DPIA en toezien op de uitvoering van de DPIA.
   f. samenwerken met de toezichthoudende autoriteit.
   g. optreden als contactpunt voor de AP.

   De FG moet toegang krijgen tot persoonsgegevens en verwerkingsactiviteiten. Aan hem/haar moeten de benodigde middelen ter beschikking worden gesteld voor het vervullen van de FG-taken en het in stand houden van zijn/haar deskundigheid.

   De FG mag geen instructies ontvangen over de uitvoering van zijn/haar FG-taken. De FG wordt door de organisatie niet ontslagen of gestraft voor de uitvoering van zijn/haar FG-taken. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende van de organisatie. Verder is de FG bij wet tot geheimhouding of vertrouwelijkheid gehouden.

   De FG kan naast de FG-taken andere taken en plichten binnen de organisatie vervullen. De organisatie moet ervoor zorgen dat deze verschillende taken en plichten niet tot een belangenconflict leiden.

3. Leg de verwerkingsgrond vast

Uw organisatie mag alleen persoonsgegevens verwerken als daarvoor een rechtmatige grond is. Voorbeelden van rechtmatige gronden zijn: toestemming van de persoon zelf; gegevens nodig om de gesloten overeenkomst uit te kunnen voeren of wettelijk verplichting.

Verwerking van *bijzondere* persoonsgegevens, is op grond van de AVG verboden, tenzij sprake is van een wettelijke uitzondering. In de wet is speciaal voor verenigingen en stichtingen op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied een uitzondering gemaakt.

Een overzicht van de diverse rechtmatige verwerkingsgronden en de wettelijke uitzonderingen voor de verwerking van bijzondere persoonsgegevens is te vinden in respectievelijk **bijlage 3** en **bijlage 4**.

Leg als verwerkingsverantwoordelijke vast wat de verwerkingsgrond is van de persoonsgegevens die uw organisatie verwerkt. Een goede plek om dit vast te leggen is het Verwerkingsregister.

4. Bepaal het risico van de verwerking

Bepaal of de gegevensverwerking een hoog privacy-risico oplevert voor de personen van wie de gegevens worden verwerkt. Als er sprake is van risicovolle verwerking, voer dan een data protection impact assesment (DPIA) uit. Meer informatie over de DPIA is opgenomen in **bijlage 5**.

5. Doe aan privacy by design/default

De processen en systemen van uw organisatie moeten van de grond af rekening houden met de privacybescherming van personen. Dit betekent dat het ontwerp en de standaardinstellingen zo privacy vriendelijk mogelijk moeten worden ingesteld. Ga na waar binnen de organisatie verbeteringen mogelijk zijn.

Ook hier zijn diverse hulpmiddelen beschikbaar. Zo heeft de AP een handleiding voor het privacy vriendelijk instellen van Google Analytics.

6. Herzie de privacyverklaring

Het is de taak van de verwerkingsverantwoordelijke, op basis van zijn informatieplicht, om de betrokkenen te laten begrijpen wat er met hun persoonsgegevens gebeurt. Vaak wordt dit beschreven in een privacyverklaring. De AVG eist ten opzichte van de voorgaande wet over meer aspecten van de verwerking een uitleg. Tevens stelt de AVG dat de privacyverklaring in duidelijke eenvoudige taal is opgesteld en goed toegankelijk/vindbaar is. Herzie waar nodig de inhoud en de publicatieplek van uw huidige privacyverklaring. **Bijlage 6** bevat een overzicht van de onderwerpen over de verwerking van persoonsgegevens die aan betrokkenen in ieder duidelijk gemaakt moeten worden.

Middels JuriDox (zie: https://juridox.nl/) is het mogelijk om een privacyverklaring op maat te maken. Door een aantal eenvoudige vragen te beantwoorden stelt u een privacyverklaring op die voldoet aan uw situatie én aan de eisen van de AVG.

7. Check de beveiliging

De beveiliging van persoonsgegevens moet passend zijn. Hoe risicovoller de verwerking, hoe hoger de beveiliging moet zijn.

Zowel de verwerkingsverantwoordelijke als de verwerker moeten technische en organisatorische maatregelen nemen om een passend beveiligingsniveau te waarborgen.

Beperk binnen de organisatie zoveel mogelijk de toegang tot persoonsgegevens en de bewaarperiodes.

Zorg dat medewerkers op een verantwoorde manier omgaan met persoonsgegevens. Hanteer daarvoor een geheimhoudingsverklaring en duidelijke werkinstructies. **Bijlage 7** bevat een voorbeeld van dergelijke instructies. Zorg dat medewerkers de inhoud van de geheimhoudingsverklaring en de instructies goed begrijpen, ernaar handelen en het hebben ondertekend. Herhaal de inhoud van beide documenten regelmatig.

8. Maak schriftelijke afspraken met verwerkende externen

Verwerker en verwerkingsverantwoordelijke zijn verplicht om over zaken rondom de verwerking van persoonsgegevens schriftelijke afspraken te maken. Deze afspraken kunnen in een aparte Verwerkersovereenkomst (een modelovereenkomst wordt spoedig op de website van de KNMvD ter beschikking gesteld) worden vastgelegd, maar ook onderdeel uitmaken van een andere overeenkomst zoals de leveringsvoorwaarden of de Service Level Agreement (SLA). Houd de afspraken rondom de verwerking van persoonsgegevens actueel. Over de volgende aspecten moeten schriftelijke afspraken worden gemaakt:

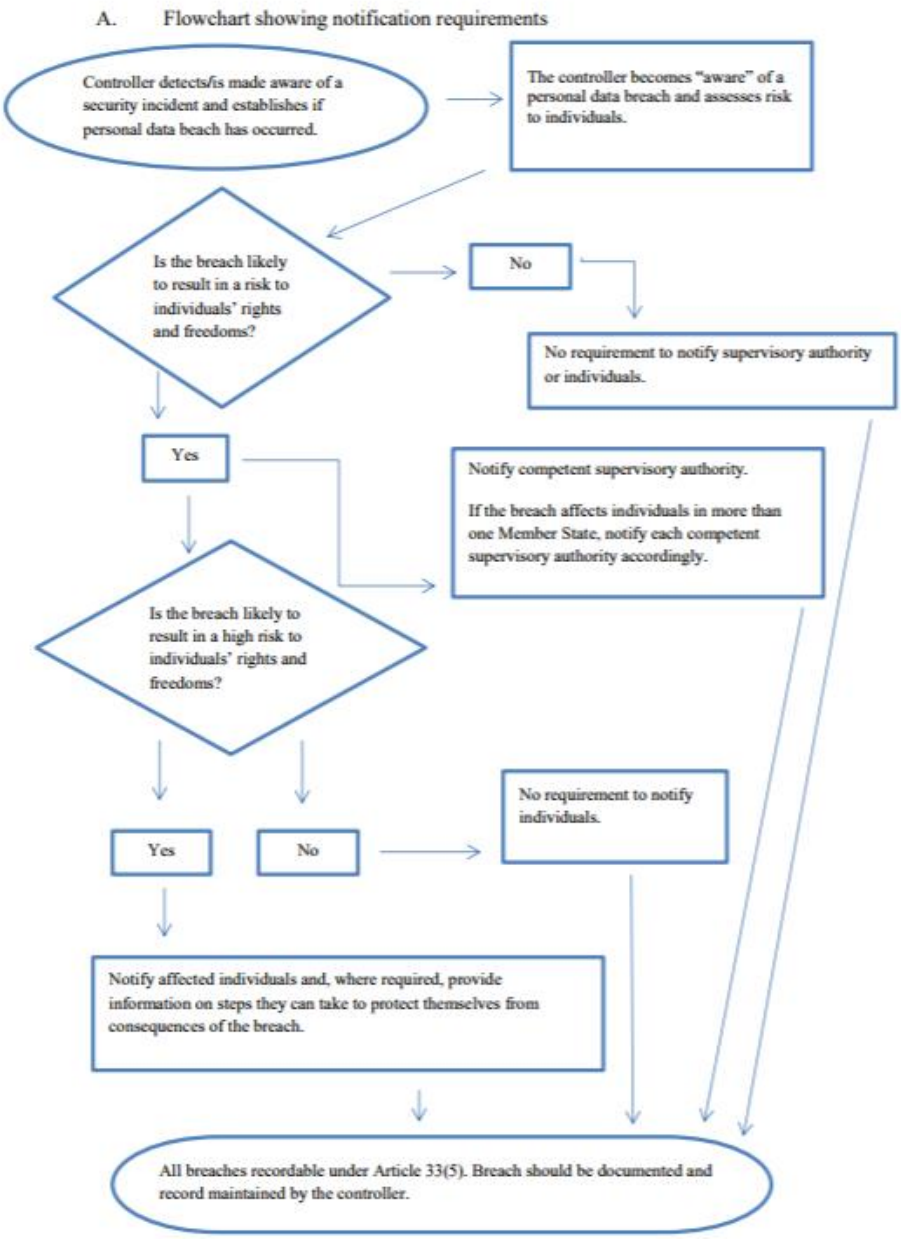
- Algemene beschrijving
  Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en verplichtingen van de verwerkingsverantwoordelijke.
- Verwerkingsinstructies
  Hoe worden verwerkingsinstructies gegeven en voor welke doeleinden mogen de gegevens worden gebruikt?
- Geheimhoudingsplicht
  Welke geheimhouding is voor wie vereist?
- Beveiliging
  Welke passende beveiligingsmaatregelen worden genomen?
- Subverwerkers
  Hoe worden eventuele subverwerkers ingeschakeld?
- Privacyrechten
  Op welke wijze helpt de verwerker de verwerkingsverantwoordelijke om aan zijn plichten te voldoen als betrokkenen hun privacyrechten uitoefenen?
- Andere verplichtingen
  Op welke wijze helpt de verwerker de verwerkingsverantwoordelijke ook om andere verplichtingen na te komen, zoals bij het melden van datalekken, het uitvoeren van een DPIA en bij een voorafgaande raadpleging.
- Gegevens verwijderen
  Welke handelswijze wordt gehanteerd na afloop van de verwerkingsdiensten?
- Audits
  Hoe wordt naleving van deze overeenkomst gecontroleerd?

9. Richt een procedure datalekken in

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat elke organisatie direct een melding moet doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. In sommige gevallen moet het datalek ook gemeld worden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Nieuwe richtlijnen voor het melden van datalekken zijn in de maak.

Zorg dat u beschikt over een duidelijke procedure over hoe te handelen als in uw organisatie een beveiligingslek is geconstateerd. Een procedure datalekken is afhankelijk van de rol van de organisatie: verwerker of verwerkingsverantwoordelijke.

In de nieuwe Engelstalige concept meldingsrichtlijnen zien de afwegingen die de verwerkingsverantwoordelijke moet maken bij het constateren van een beveiligingslek er als volgt uit:



In de verwerkersovereenkomst maken de verwerkingsverantwoordelijke en de verwerker afspraken over meldingen vanuit de verwerker aan de verwerkingsverantwoordelijke. Verwerkers hebben geen zelfstandige meldingsplicht aan de AP en/of betrokkenen.

PrivacyBlox biedt ook hulp op het gebied van datalekken. Zo stelt u eenvoudig een calamiteitenplan op voor het omgaan met mogelijke datalekken. Tevens adviseert PrivacyBlox u als er een datalek wordt vermoed. Door een interactieve vragenlijst te doorlopen wordt snel duidelijk of er daadwerkelijk een datalek heeft plaatsgevonden en welke vervolgstappen er nodig zijn.

10. Stel procedures op voor rechtenuitoefening door betrokkenen

Personen hebben op basis van de AVG de volgende rechten rondom hun persoonsgegevens:

- Recht op inzage
- Recht op rectificatie
- Recht op gegevenswissing (recht op vergetelheid)
- Recht op beperking van de verwerking
- Recht op overdraagbaarheid van gegevens (dataportabiliteit)
- Recht op bezwaar
- Recht op niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit

Zorg dat u als organisatie voorbereid bent op verzoeken van betrokken om hun gegevens in te zien, te rectificeren, te wissen, te beperken of over te dragen. Stel ook een procedure op voor hoe om te gaan met bezwaren die worden ingediend.

De afhandeling van het verzoek is afhankelijk van het type verzoek. Bepaal daarom eerst goed of het gaat om een verzoek om inzage, of ook om rectificatie, aanvulling, verwijdering of een beperking van de verwerking? Betrokkenen kunnen soms andere termen gebruiken, dus wees hier alert op.

In bijlage 8 t/m 14 zijn handvatten voor de afhandeling van verzoeken gebaseerd op de eerste zes genoemde rechten opgenomen. Bij de afhandeling van bezwaren wordt onderscheid gemaakt tussen bezwaren wegens bijzondere persoonlijke omstandigheden/wegens een specifieke situatie en bezwaren bij direct marketing.

Bijlage 1 – Definities

Betrokkenen
De betrokkene is degene van wie de organisatie persoonsgegevens verwerkt. Dit is dus degene op wie de persoonsgegevens betrekking hebben.

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.

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.

Bijzondere persoonsgegevens
Gegevens over iemands:
- gezondheid, inclusief genetische en biometrische gegevens gericht op unieke identificatie van een persoon
- ras of etnische afkomst
- seksueel gedrag of seksuele gerichtheid
- religieuze of levensbeschouwelijke overtuigingen
- lidmaatschap van een vakbond
- politieke opvattingen
- strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

Een foto van een persoon is alleen een bijzonder persoonsgegeven wanneer de foto met behulp van bepaalde technische middelen wordt verwerkt en zo unieke identificatie van een persoon mogelijk maakt.

Soms kan er ook sprake zijn van indirecte bijzondere persoonsgegevens. Dit is het geval wanneer de aanwezigheid van een gevoelig gegeven kan worden afgeleid. Denk hierbij aan de administratie van een kerkgenootschap of een politieke partij.

Volgens de Wpb is het burgerservicenummer (BSN-nummer) ook een bijzonder persoonsgegeven, in de AVG niet. In de nog vast te stellen Uitvoeringswet AVG gaan wel speciale eisen aan de verwerking van het BSN-nummer gesteld worden. Vooralsnog is het standpunt dat een dierenartspraktijk geen grondslag heeft om een BSN-nummer te verwerken. Ook niet voor incassoprocedures.

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

Verwerkingsverantwoordelijke
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Bijlage 2 – Eisen Verwerkingsregisters

Verwerkingsregister verwerkingsverantwoordelijke

Het Verwerkingsregister van de verwerkingsverantwoordelijke moet in ieder geval de volgende gegevens per verwerkingsactiviteit bevatten:

- Naam en contactgegevens van
  - uw organisatie, of de vertegenwoordiger van uw organisatie;
  - eventuele andere organisaties met wie u gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld;
  - de Functionaris voor de gegevensbescherming als u die heeft aangesteld;
  - eventuele andere internationale organisaties waar u persoonsgegevens mee deelt.
- Verwerkingsdoeleinden
  Beschrijf waarom het persoonsgegeven of de set van persoonsgegevens wordt verwerkt. Persoonsgegevens mogen namelijk alleen verzameld worden voor, zoals de wet het stelt, een 'welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel'. Voorbeelden van verwerkingsdoeleinden zijn het beantwoorden van vragen en klachten van klanten en uitbetaling van salaris.
- De categorieën betrokkenen
  Beschrijf de categorieën van de personen van wie u gegevens verwerkt, bijvoorbeeld: leden, relaties, potentiële leden, medewerkers van leden en relaties, eigen personeelsleden, uitzendkrachten, klanten, website-bezoekers, leveranciers, mensen die zich hebben aangemeld voor een nieuwsbrief etc.
- De categorieën van persoonsgegevens
  Bijvoorbeeld: NAW-gegevens, IP-adressen, bankrekeningnummer, online bestelgeschiedenis of polisnummers. Bepaal of onder deze verwerkte persoonsgegevens zich ook bijzondere persoonsgegevens bevinden en markeer deze. Voor bijzondere gegevens gelden namelijk afwijkende regels en eisen.
- De (voorgenomen) categorieën van ontvangers van de persoonsgegevens
  Beschrijf de (voorgenomen) categorieën van ontvangers van de persoonsgegevens zoals de Belastingdienst of een reclamebureau.
- Uitvoer 3e landen
  Vermeld het derde land of de internationale organisatie waaraan de persoonsgegevens verstrekt (zullen) worden en waar nodig documentatie omtrent de genomen passende waarborgen voor de bescherming van persoonsgegevens in dit derde land.

  Van uitvoer naar een 3e land is sprake wanneer gegevens worden verwerkt buiten de Europese Unie, Noorwegen, Liechtenstein en IJsland. Is er sprake van uitvoer naar 3e landen, onderzoek dan of er voldoende wettelijke waarborgen zijn die uitvoer toestaan.
- Bewaartermijnen
  De beoogde bewaartermijnen voor de verschillende categorieën van gegevens.
- Beveiliging
  Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Verwerkingsregister verwerker

Bij de verwerker is het register georganiseerd per verantwoordelijke. Verwerkers registreren per verantwoordelijke voor wie zij werken:

- Naam en contactgegevens van de hoofdverwerker(s) of verwerkingsverantwoordelijke(n)
  De naam en contactgegevens van de verwerker(s) of verwerkingsverantwoordelijke(n) voor rekening waarvan de verwerker (eventueel als sub-verwerker) handelt. Meestal komt dit neer op de lijst met klanten van de verwerker.
- Naam en contactgegevens van de vertegenwoordiger
  De naam en contactgegevens van de vertegenwoordiger van de verwerkingsverantwoordelijke of de verwerker waarvoor de (sub-)verwerker handelt.
- Naam en contactgegevens van de Functionaris voor de Gegevensbescherming (FG)
  In het geval geen FG genoemd is, moet hier worden uitgelegd waarom er geen FG nodig is.
- Categorieën van verwerkingen
  De categorieën van verwerkingen die voor rekening van verwerkingsverantwoordelijken uitgevoerd zijn. Bijvoorbeeld: personeelsadministratie of bezoekersregistratie.
- Uitvoer 3e landen
  Vermelding van doorgifte aan een derde land of internationale organisatie en vermelding van dit derde land of internationale organisatie en waar nodig documentatie omtrent de genomen passende waarborgen voor de bescherming van persoonsgegevens in dit derde land.
- Beveiliging
  Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Bijlage 3 – Rechtmatige verwerkingsgronden persoonsgegevens

De verwerking van persoonsgegevens (bijzondere persoonsgegevens uitgezonderd) is rechtmatig als ten minste aan een van de onderstaande voorwaarden is voldaan:

1. Toestemming
   De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
2. Noodzakelijk uitvoering overeenkomst
   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.
3. Wettelijke verplichting/publieke taak
   De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
4. Bescherming vitale belangen
   De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.
5. Algemeen belang/gezaguitoefening
   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.
6. Gerechtvaardigd belang
   De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen, de grondrechten en/of de fundamentele vrijheden van de betrokkene zwaarder wegen dan die gerechtvaardigde belangen. Met name wanneer de betrokkene een kind is, kan dit het geval zijn. Wees zeer terughoudend met het hanteren van deze grondslag.

Bijlage 4 – Wettelijke uitzonderingen verwerking bijzondere persoonsgegevens

Verwerking van bijzondere persoonsgegevens (uitgezonderd de strafrechtelijke) is onder de AVG verboden, tenzij sprake is van een van de volgende wettelijke uitzonderingen:

1. Uitdrukkelijke toestemming
   De betrokkene heeft uitdrukkelijk toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden.
2. Noodzakelijk uitvoering verplichtingen en uitoefening specifieke rechten
   De verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht.
3. Bescherming vitale belangen
   De verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokkene of van een andere natuurlijke persoon indien de betrokkene fysiek of juridisch niet in staat is zijn toestemming te geven.
4. Verwerking door stichting en vereniging op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied
   De verwerking wordt verricht door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie of op personen die in verband met haar doeleinden regelmatig contact met haar onderhouden, en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt.
5. Kennelijk openbaar gemaakt door betrokkene
   De verwerking heeft betrekking op persoonsgegevens die door de betrokkene openbaar zijn gemaakt. De werking moet ook in lijn zijn met het doel van de openbaarmaking door de betrokkene.
6. Noodzakelijk voor rechtsvordering/rechtshandhaving
   De verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering of wanneer gerechtsprekende instanties handelen in het kader van hun rechtsbevoegdheid.
7. Zwaarwegend algemeen belang
   De verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.
8. Noodzakelijk voor (arbeids)geneeskunde en sociale diensten
   De verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en wanneer die gegevens worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die krachtens Unierecht of lidstatelijk recht

of krachtens door nationale bevoegde instanties vastgestelde regels aan het beroepsgeheim is gebonden, of door een andere persoon die eveneens krachtens Unierecht of lidstatelijk recht of krachtens door nationale bevoegde instanties vastgestelde regels tot geheimhouding is gehouden.

9. Noodzakelijk voor algemeen belang volksgezondheid
   De verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim.
10. Noodzakelijk voor archivering in het algemeen belang
    De verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig AVG artikel 89, lid 1, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.

De lidstaten kunnen bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren. Tot op heden (januari 2017) heeft Nederland nog geen aanvullende voorwaarden ingevoerd.

Bijlage 5 – Data protection impact assessment (DPIA)

Een organisatie is verplicht tot het uitvoeren van een data protection impact assessment (DPIA) als gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de personen van wie gegevens verwerkt worden. Van zo een risicovolle verwerking is volgens de AVG in ieder geval sprake als u:

- systematisch en uitvoerig persoonlijke kenmerken evalueert, waaronder profiling*;
- op grote schaal bijzondere persoonsgegevens verwerkt;
  (bij de grootschaligheidsbeoordeling wordt gekeken naar het aantal mensen van wie u gegevens verwerkt, de hoeveelheid gegevens die u verwerkt, de duur van de gegevensverwerking en de geografische reikwijdte van de verwerking)
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Valt de verwerking niet onder de drie bovengenoemde criteria dan, zal de organisatie zelf een beoordeling moeten maken of een DPIA noodzakelijk is. Kijk hierbij naar de aard, omvang, context en het doel van de (voorgenomen) verwerking.

De werkgroep van Europese privacy-toezichthouders (WP 29) heeft een tiental criteria opgesteld om zelf een DPIA-afweging te maken. Vuistregel hierbij is: voldoet de verwerking aan twee of meer van deze criteria, dan is een DPIA nodig:

1. Beoordelen van mensen op basis van persoonskenmerken
2. Geautomatiseerde beslissingen
3. Stelselmatige en grootschalige monitoring
4. Gevoelige gegevens
5. Grootschalige gegevensverwerkingen
6. Gekoppelde databases
7. Gegevens over kwetsbare personen
8. Gebruik van nieuwe technologieën
9. Doorgifte van persoonsgegevens buiten de EU
10. Blokkering van een recht, dienst of contract

Daarnaast publiceert de AP op termijn een lijst van verwerkingen waarvoor een DPIA verplicht is.

Op de website van de AP zijn richtlijnen voor de uitvoering van een DPIA te vinden.

* Profiling: 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.

Bijlage 6 – Eisen privacyverklaring

De verwerkingsverantwoordelijke moet de betrokkene in duidelijke en eenvoudige taal, bijvoorbeeld in een privacyverklaring, in ieder geval het volgende laten weten:

- Identiteit van de verwerkingsverantwoordelijke
  Vermeld wie u bent.
- Contactgegevens
  Hoe kan de betrokkene contact opnemen met de verwerkingsverantwoordelijke? En indien van toepassing: wat zijn de contactgegevens van de Functionaris voor de Gegevensbescherming?
- Welke persoonsgegevens
  Geef aan welke persoonsgegevens worden verwerkt.
- Doeleinden en rechtsgrond van de verwerking
  Waarom worden persoonsgegevens verzameld en waarom mag dat? (doelomschrijving, rechtsgrond en onderbouwing daarvan)
- Wie ontvangen de gegevens?
  Aan wie gaat u de persoonsgegevens verder nog verstrekken?
- Wel of geen verplichting om gegevens te verstrekken
  Is de betrokkene verplicht om de gevraagde persoonsgegevens te verstrekken of niet? En wat zijn de gevolgen als hij/zij de persoonsgegevens niet verstrekt?
- Rechten van de betrokkenen
  Wijs de betrokkene op zijn rechten. Geef aan hoe de betrokkene kan vragen om inzage, rectificatie, overdraging, beperking of het wissen van persoonsgegevens (right to be forgotten). En hoe kan de betrokkene bezwaar maken?
- Intrekken toestemming
  Hoe kan een betrokkene een verleende toestemming intrekken?
- Bewaartermijn
  Hoe lang worden persoonsgegevens bewaard? Of indien dat niet mogelijk is, de criteria ter bepaling van de bewaartermijn.
- Verwerking derde landen
  Als de persoonsgegevens buiten de EU, Noorwegen, Liechtenstein en IJsland verwerkt gaan worden, welke waarborgen zijn er dan getroffen zodat de persoonsgegevens in dat derde land conform de AVG verwerkt worden?
- Vermelding geautomatiseerde gegevensverzameling
  Vermeld of er geautomatiseerde besluitvorming (bijvoorbeeld profiling) plaatsvindt. En zo ja, welke logica wordt daarvoor gebruikt?
- Cookies
  Geef duidelijk aan of u gebruik maakt van cookies.
- Klacht indienen
  Vermeld hoe de betrokkene een klacht over de privacy kan indienen bij de AP.

Bijlage 7 – Voorbeeld instructies gegevensbeveiliging voor medewerkers

Door het nemen van de juiste beveiligingsmaatregelen en het in acht nemen van de juiste beveiligingsprocedures willen we voorkomen dat onbevoegden toegang krijgen tot onze bedrijfssystemen, onze vertrouwelijke informatie en de persoonsgegevens die wij beheren. Neem daarom gegevensbeveiliging serieus en volg onderstaande instructies en werkwijzen zorgvuldig op. Onderteken na het doornemen en akkoord dit formulier en lever deze in bij [naam/functionaris].

Werk gerelateerde gegevensverwerking mag alleen worden uitgevoerd met door de werkgever ter beschikking gestelde gegevensdragers, tenzij anders overeengekomen met de directie.

Computers, laptops en tablets

1. Beveilig de toegang tot je computers, laptops en tablets met een sterk en uniek wachtwoord.
2. Stel multifactor authenticatie in.
3. Stel de schermbeveiliging in op maximaal 5 minuten.
4. Installeer in afstemming met de systeembeheerder betrouwbare antivirus-software en houd deze up-to-date.
5. Stel in afstemming met de systeembeheerder een firewall in en houd deze up-to-date.
6. Ga alleen online via een beveiligde verbinding.
7. Stel de automatische update-functie in om besturingssystemen en andere software up-to-date te houden.
8. Download alleen na toestemming van de systeembeheerder nieuwe software en apps.

Losse externe dataopslagapparatuur

Voorbeelden van externe dataopslagapparatuur zijn USB-sticks, externe harde schijven, geheugenkaartjes en cd's/dvd's/blu-ray-discs.

1. Beveilig de toegang tot de losse dataopslagapparatuur met een sterk en uniek wachtwoord.
2. Beveilig de toegang tot de individuele documenten op de losse dataopslagapparatuur met een sterk en uniek wachtwoord.
3. Verwijder na gebruik gegevens van de losse dataopslagapparatuur.

Smartphone

1. Beveilig de toegang tot je telefoon met een pincode van minimaal 4 cijfers.
2. Stel in dat je telefoon automatisch wordt geleegd na 10 verkeerde pincode pogingen.
3. Stel 'zoek mijn iPhone/Android' in en test of dit werkt.
4. Download alleen apps uit de officiële appstores: App-store, Google Play en Windows-store.

Fysieke documenten

1. Voorzie documenten met vertrouwelijke informatie of persoonsgegevens van een duidelijk predicaat 'vertrouwelijk'.
2. Berg fysieke documenten met vertrouwelijke informatie of persoonsgegevens op in een afsluitbare opslagruimte en zorg dat alleen bevoegden toegang hebben tot deze fysieke documenten.

Ondergetekende verklaart dat hij/zij de bovengenoemde instructies hanteert.

Handtekening:
Naam:
Datum:

Bijlage 8 – Voorbeeld afhandeling recht op inzage

1. Bepaal wie het verzoek behandeld

Beleg in de organisatie wie een inzageverzoek behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.

2. Voer een identiteitscontrole uit

Leg vast hoe de identiteit van de aanvrager wordt gecontroleerd. Stel in dat deze controle altijd wordt uitgevoerd voordat het verzoek verder in behandeling genomen wordt. Deze check moet zwaarder zijn naarmate het om meer gevoelige of zelfs bijzondere gegevens gaat. Voorkomen moet worden dat er een 'fake'-inzageverzoek gedaan wordt om zo gegevens te verzamelen.

3. Bepaal welke gegevens verstrekt moeten worden

De betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitsel te krijgen over:

- of de organisatie zijn/haar persoonsgegevens gebruikt, en zo ja:
- om welke gegevens het gaat;
- wat het doel is van de verwerking;
- aan wie de organisatie de gegevens eventueel heeft verstrekt (bij uitvoer 3e landen: welke waarborgen);
- wat de herkomst is van de gegevens, als deze bekend is;
- het bestaan van geautomatiseerde besluitvorming, profilering en eventueel, informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen;
- bewaartermijnen.

De AVG stelt verder dat de betrokkene bij de beantwoording ook gelijk geïnformeerd moet worden over het recht op rectificatie, wissen of beperking van de verwerking en over het feit dat de verzoeker een bezwaar of klacht kan indienen.

Indien er gegevens van derde personen in de te verstrekken gegevens opgenomen zijn, moet met het (privacy-)belang van die derde rekening gehouden worden. Die gegevens moeten dus of verwijderd worden, of pas na toestemming van die derde verstrekt worden. Denk bijvoorbeeld aan (interne) aantekeningen van een medewerker in een dossier van een lid. Die mogen niet zomaar verstrekt worden.

4. Verstrek de gegevens aan de betrokkene

De verwerkingsverantwoordelijke is verplicht binnen 4 weken schriftelijk of per e-mail te reageren op het inzageverzoek. De AVG stelt geen eisen aan de manier waarop inzage wordt gegeven, maar schrijft wel voor dat de organisatie de verzoeker een kopie verstrekt van de persoonsgegevens die worden verwerkt.

Onder de AVG moet een kopie van de verwerkte persoonsgegevens kosteloos worden verstrekt en mag alleen voor bijkomende kopieën op basis van de administratieve kosten een redelijke vergoeding in rekening worden gebracht.

Een inzageverzoek kan geweigerd worden indien dat noodzakelijk is voor de veiligheid van de staat, de voorkoming, opsporing en vervolging van strafbare feiten, belangrijke economische en financiële belangen van de staat, het toezicht op de naleving van wettelijke voorschriften en de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Bijlage 9 – Voorbeeld afhandeling recht op rectificatie

1. Bepaal wie het verzoek behandeld
Beleg in de organisatie wie een rectificatieverzoek behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.

2. Voer een identiteitscontrole uit
Leg vast hoe de identiteit van de aanvrager wordt gecontroleerd. Stel in dat deze controle altijd wordt uitgevoerd voordat het verzoek verder in behandeling genomen wordt. Deze check moet zwaarder zijn naarmate het om meer gevoelige of zelfs bijzondere gegevens gaat. Voorkomen moet worden dat er een 'fake'-rectificatieverzoek gedaan wordt om zo gegevens te wijzigen.

3. Beoordeel en verwerk het verzoek
Beoordeel of en hoe aan het verzoek om rectificatie kan worden voldaan. Rectificatie en aanvulling moeten direct geschieden.

Het recht op rectificatie houdt ook het recht op aanvulling in van ontbrekende gegevens of zelfs het toevoegen van een verklaring van de betrokkene aan de gegevens. Dit kan bijvoorbeeld van belang zijn bij een HR-dossier, indien een betrokkene het niet eens is met een negatieve aantekening, berisping of beoordeling. In dat geval moet zijn andersluidende verklaring toegevoegd worden aan het dossier.

Is het technisch gezien niet mogelijk om gegevens te rectificeren? Bijvoorbeeld doordat deze zijn opgeslagen op een cd-rom? Dan kan de organisatie een bestand met aanvullingen en verbeteringen aanleggen.

4. Informeer de betrokkene
Informeer de betrokkene schriftelijk of per e-mail binnen 4 weken na ontvangst van het verzoek of het verzoek is ingewilligd, hoe dat is gedaan en zo niet, motiveer waarom niet.

5. Informeer ontvangers over de rectificatie
Informeer ontvangers van de persoonsgegevens over de rectificatie en zorg dat ook zij de gegevens aanpassen. Hiervan kan worden afgezien wanneer de ontvangers onmogelijk kunnen worden opgespoord of wanneer het informeren een onevenredige inspanning is.

Bijlage 10 – Voorbeeld afhandeling recht op gegevenswissing

1. Bepaal wie het verzoek behandeld
Beleg in de organisatie wie een gegevenswissingsverzoek behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.

2. Voer een identiteitscontrole uit
Leg vast hoe de identiteit van de aanvrager wordt gecontroleerd. Stel in dat deze controle altijd wordt uitgevoerd voordat het verzoek verder in behandeling genomen wordt. Deze check moet zwaarder zijn naarmate het om meer gevoelige of zelfs bijzondere gegevens gaat. Voorkomen moet worden dat er een 'fake'-wissingsverzoek gedaan wordt om zo gegevens te verwijderen.

3. Beoordeel en verwerk het verzoek
Beoordeel of en hoe aan het verzoek om te wissen kan worden voldaan. Het wissen moet zonder onredelijke vertraging worden gedaan als er geen verwerkingsgrond of geen doelbinding meer is voor de verwerking.

4. Informeer de betrokkene
Informeer de betrokkene schriftelijk of per e-mail binnen 4 weken na ontvangst van het verzoek of het verzoek is ingewilligd, hoe dat is gedaan en zo niet, motiveer waarom niet.

5. Informeer ontvangers over de wissing
Informeer ontvangers van de persoonsgegevens over de wissing en zorg dat ook zij de gegevens wissen. Hiervan kan worden afgezien wanneer de ontvangers onmogelijk kunnen worden opgespoord of wanneer het informeren een onevenredige inspanning is.

Als de gegevens openbaar gemaakt waren, moet de verwerkingsverantwoordelijke zijn best doen ervoor te zorgen dat koppelingen naar derden of kopieën bij derden ook verwijderd worden.

Bijlage 11 – Voorbeeld afhandeling recht op beperking van de verwerking

1. Bepaal wie het verzoek behandeld
Beleg in de organisatie wie een beperkingsverzoek behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.

2. Voer een identiteitscontrole uit
Leg vast hoe de identiteit van de aanvrager wordt gecontroleerd. Stel in dat deze controle altijd wordt uitgevoerd voordat het verzoek verder in behandeling genomen wordt. Deze check moet zwaarder zijn naarmate het om meer gevoelige of zelfs bijzondere gegevens gaat. Voorkomen moet worden dat er een 'fake'-beperkingsverzoek gedaan wordt om zo de verwerking te beïnvloeden.

3. Beoordeel en verwerk het verzoek
Beoordeel of en hoe aan het verzoek om beperking kan worden voldaan. Beperking van de verwerking kan veel vormen aannemen bijvoorbeeld dat gegevens niet gewist, niet verspreid of niet gecombineerd mogen worden.

Zorg ervoor dat bij lopende verzoeken bestaande gegevens 'bevroren' worden, zodat ze niet veranderd kunnen worden en niet meer voor iedereen toegankelijk zijn, maar alleen voor specifieke personen.

4. Informeer de betrokkene
Informeer de betrokkene schriftelijk of per e-mail binnen 4 weken na ontvangst van het verzoek of het verzoek is ingewilligd, hoe dat is gedaan en zo niet, motiveer waarom niet.

5. Informeer ontvangers over de beperking
Informeer ontvangers van de persoonsgegevens over de beperking en zorg dat ook zij de gegevens beperken. Hiervan kan worden afgezien wanneer de ontvangers onmogelijk kunnen worden opgespoord of wanneer het informeren een onevenredige inspanning is.

Bijlage 12 – Voorbeeld afhandeling recht op overdraagbaarheid van gegevens

Het recht op overdraagbaarheid van gegevens, dataportabiliteit, is het recht om gegevens te mogen meenemen naar een andere aanbieder. Dit houdt in dat gegevens verzonden moeten worden aan de betrokkene zelf of aan de nieuwe aanbieder.

1. Bepaal wie het verzoek behandeld

Beleg in de organisatie wie een dataportabiliteitsverzoek behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.

2. Voer een identiteitscontrole uit

Leg vast hoe de identiteit van de aanvrager wordt gecontroleerd. Stel in dat deze controle altijd wordt uitgevoerd voordat het verzoek verder in behandeling genomen wordt. Deze check moet zwaarder zijn naarmate het om meer gevoelige of zelfs bijzondere gegevens gaat. Voorkomen moet worden dat er een 'fake'-dataportabiliteitsverzoek gedaan wordt om gegevens te verkrijgen.

3. Beoordeel en verwerk het verzoek

Beoordeel of en hoe aan het verzoek om dataportabiliteit kan worden voldaan.

Data opvragen kan in de volgende gevallen:

- Het gaat om geautomatiseerde verwerkingen (geen papier)
- De verwerking berust op de verwerkingsgrond 'toestemming' of 'uitvoering van een overeenkomst'

De verwerkingsverantwoordelijke moet alle persoonsgegevens beschikbaar stellen die de betrokkene aan hem heeft verstrekt. Het gaat hierbij om gegevens die klanten actief en bewust hebben verstrekt, zoals de accountgegevens (e-mailadres, gebruikersnaam, leeftijd etc.) die zij op een online formulier hebben ingevuld, maar ook om de gegevens die klanten hebben 'verstrekt' door de dienst of het apparaat van de verwerkingsverantwoordelijke te gebruiken. Bijvoorbeeld de zoekgeschiedenis of locatiegegevens van de betrokken of andere (ruwe) data.

Door de verwerkingsverantwoordelijke zelf gegenereerde data (zoals analyses of profiling-gegevens) hoeven niet te worden verstrekt. Leg die gekozen afbakening tussen verstrekte (ruwe)data en zelf gegeneerde data in deze procedure vast.

De verwerkingsverantwoordelijke moet niet alleen de feitelijke inhoud leveren, maar ook zoveel mogelijk relevante metagegevens meeleveren zoals tijdstip, afzender, geadresseerde etc. Hierdoor blijft de betekenis van de overgedragen informatie zo goed mogelijk bewaard.

De verwerkingsverantwoordelijke mag in principe geen kosten rekenen voor het overdragen van deze gegevens. Alleen in uitzonderlijke gevallen als u kunt aantonen dat een verzoek duidelijk ongegrond is of excessief (bijvoorbeeld als u heel veel verzoeken van één persoon krijgt), kunt u geld vragen of het verzoek weigeren.

4. Verstrek de gegevens aan de betrokkene

De verwerkingsverantwoordelijke moet de gevraagde persoonsgegevens zo snel mogelijk beschikbaar stellen, in ieder geval binnen een maand. Bij complexe verzoeken heeft de verwerkingsverantwoordelijke maximaal drie maanden de tijd, maar dan moet de reden voor deze vertraging wel binnen een maand aan de betrokkene gemeld worden.

Een weigering van een verzoek moet binnen een maand aan de betrokkene zijn gemeld met daarbij aangegeven waarom het verzoek is geweigerd. Wijs de betrokken in de afwijzing op het feit dat hij/zij een klacht kan indienen bij de Autoriteit Persoonsgegevens of juridische hulp kan zoeken.

Gegevens moeten verstrekt worden in een gestructureerd, gebruikelijk, machine-leesbaar formaat. Het doel van dataportabiliteit is dat de betrokkene er zelf of bij een nieuwe provider mee verder kan. Aanlevering mag dus niet in een ‘eigen formaat’ dat niet te converteren is naar gebruikelijke standaarden. Het is nog niet duidelijk wat precies de gebruikelijke standaarden zijn.

Bijlage 13 – Voorbeeld afhandeling recht op bezwaar – specifieke situatie

1. Bepaal wie het bezwaar behandeld
Beleg in de organisatie wie een bezwaar wegens een specifieke situatie behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.

2. Voer een identiteitscontrole uit
Leg vast hoe de identiteit van de bezwaarmaker wordt gecontroleerd.

3. Beoordeel het bezwaar
Weeg af of het bezwaar redenen bevat om de verwerking van persoonsgegevens van de betrokkene te wijzigen. De verwerkingsgrond speelt een grote rol bij deze beoordeling.

4. Informeer de betrokkene
Informeer de betrokkene schriftelijk of per e-mail binnen 4 weken na ontvangst van het bezwaar of het bezwaar is ingewilligd, hoe dat is gedaan en zo niet, motiveer waarom niet.

Bijlage 14 – Voorbeeld afhandeling recht op bezwaar – direct marketing

1. Bepaal wie het bezwaar behandeld
Beleg in de organisatie wie een bezwaar tegen direct marketing behandelt. Leg dit vast in de procedure of in het register van de verwerkingsactiviteiten.

2. Voer een identiteitscontrole uit
Leg vast hoe de identiteit van de bezwaarmaker wordt gecontroleerd.

3. Beoordeel het bezwaar
Wanneer persoonsgegevens ten behoeve van direct marketing verwerkt worden, heeft de betrokkene te allen tijde het recht bezwaar te maken tegen de verwerking van zijn persoonsgegevens voor dergelijke marketing, met inbegrip van profiling die betrekking heeft op direct marketing.

Dit recht is absoluut. De verwerkingsverantwoordelijke moet altijd stoppen met de verwerking. Er is geen ruimte voor een belangenafweging. Dit is de opt-out regeling. Deze opt-out mogelijkheid moet uiterlijk op het moment van het eerste contact met de betrokkene uitdrukkelijk onder de aandacht van de betrokkene gebracht worden en duidelijk en gescheiden van enige andere informatie weergegeven.

4. Informeer de bezwaarmaker
Informeer de bezwaarmaker schriftelijk of per e-mail binnen 4 weken na ontvangst hoe het bezwaar is ingewilligd.