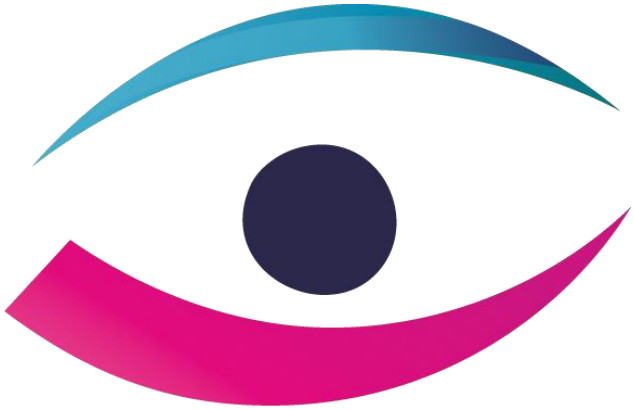
Checklist Privacy | AVG



AANGEBODEN DOOR:

MOS bv

EEN CO-CREATIE VAN:

Monique Hennekens van **Hekkelman Advocaten** en

Siegfried Frencken van **Rapasso**

2 maart 2018

Over deze checklist

Privacy is een grondrecht. De privacyregelgeving is er daarom op gericht om individuen te beschermen. Vanaf 25 mei 2018 wordt de Wet bescherming persoonsgegevens (Wbp) vervangen door de Algemene Verordening Gegevensbescherming (AVG). De grootste wijziging die de AVG meebrengt is de verantwoordingsplicht. Iedere organisatie of zelfstandige professional zal aan de hand van documenten moeten kunnen aantonen dat zij voldoet aan de privacybeginselen uit de AVG.

De 'Checklist AVG' is een hulpmiddel om *AVG proof* te worden en is met name bestemd voor zelfstandige professionals. Deze checklist is bedoeld als leidraad voor het oppakken van de belangrijkste verplichtingen uit de AVG. In de tekst zijn diverse verwijzingen en hyperlinks opgenomen naar achtergrondinformatie. Bovendien treft u een aantal voorbeelddocumenten aan die gebruikt kunnen worden als model. Tevens treft u hier een 'TO-DO list AVG' aan met een opsomming van de checks die hieronder nader zijn toegelicht.

Deze checklist is opgedeeld in een aantal hoofdstukken:

Verwerking van persoonsgegevens
De privacywetgeving geldt voor iedere *verwerking* van *persoonsgegevens* voor niet huishoudelijk gebruik. De begrippen *persoonsgegeven* en *verwerking* worden zeer ruim uitgelegd door de toezichthouders, waaronder de Nederlandse toezichthouder, de Autoriteit Persoonsgegevens. De *verwerking* van persoonsgegevens is iedere handeling die betrekking heeft op persoonsgegevens. Het hoeft geen actieve handeling te zijn. Het inzien, bewaren, verstrekken of uitsluitend opslaan of vernietigen van persoonsgegevens zijn allemaal verwerkingen. Een *persoonsgegeven* is ieder gegeven dat herleidbaar is tot een natuurlijk persoon (de *betrokkene*). Denk aan contactgegevens, foto's, camerabeelden, sportprestaties, telefoonopnames en IP adressen.

Iedere professional verwerkt dagelijks persoonsgegevens. Denk aan de klantenadministratie of de financiële administratie en via de website. De privacywetgeving speelt daarom een belangrijke rol in die dagelijkse werkzaamheden.

Verwerkingsverantwoordelijke en verwerker
De AVG en ook de overige privacywetgeving maakt een onderscheid tussen twee rollen, namelijk de *verwerkingsverantwoordelijke* (in de Wbp verantwoordelijke genoemd) en de *verwerker* (in de Wbp bewerker genoemd). De verwerkingsverantwoordelijke bepaalt het doel en de middelen van de gegevensverwerking en zal moeten voldoen aan alle vereisten van de privacywetgeving. De *verwerker* is degene die persoonsgegevens verwerkt *ten behoeve van* een verwerkingsverantwoordelijke. Een verwerker heeft geen eigen doel voor de verwerking van de persoonsgegevens buiten het uitvoeren van de dienstverlening voor de verwerkingsverantwoordelijke.

Voorbeeld
De professional is verwerkingsverantwoordelijke ten aanzien van haar klantenadministratie. Het is namelijk de professional die bepaalt welke gegevens van de klanten worden verwerkt en hoe dat wordt gedaan. Als de professional daarbij gebruik maakt van een administratiesysteem die wordt onderhouden door een IT leverancier, dan is die IT leverancier een verwerker van de professional. De IT leverancier is op haar beurt verwerkingsverantwoordelijke voor haar eigen personeelsadministratie.

Zie voor een overzicht van alle wettelijke definities uit de AVG hier.

De verwerkingsverantwoordelijke zal aan de volledige privacywetgeving moeten voldoen én blijft verantwoordelijk voor de juiste omgang met de persoonsgegevens in de gehele keten, dus ook als bepaalde verwerkingen worden uitbesteed aan een verwerker. Een verwerker heeft op grond van de privacywetgeving veel minder verplichtingen.

1. Inventarisatie van persoonsgegevens

Het is niet mogelijk om te voldoen aan de AVG als niet bekend is welke persoonsgegevens worden verwerkt en op welke wijze. Er zal daarom in kaart moeten worden gebracht welke gegevensstromen er binnen de organisatie zijn en welke persoonsgegevens daarbij worden verwerkt.

Welke gegevensstromen zijn er?

Denk aan:
- de klantenadministratie
- de personeelsadministratie of administratie van ingeschakelde personen
- debiteuren- en crediteurenadministratie
- online communicatiemiddelen (zoals e-mails, website, online platformen, sociale media, apps)
- toegangscontrole, telefoongegevens (incl. opnames), camerabeelden
- mobiele apparaten, zoals tablets en smartphones

Welke persoonsgegevens worden er per gegevensstroom verwerkt?

Denk aan:
- contactgegevens (NAW, e-mailadres, telefoonnummers)
- financiële gegevens
- BSN
- pasfoto's of ander beeldmateriaal van personen
- gezondheidsgegevens

Daarnaast is het voor de naleving van de AVG van belang om de volgende vragen te documenteren:

In welke systemen worden de persoonsgegevens opgeslagen en beheerd?

- Opslag op interne of externe servers
- Koppelingen en uitwisseling tussen systemen

✓ **Wie heeft toegang tot de persoonsgegevens per systeem/administratie**

- Intern en extern
- Is vastgesteld wie dat bepaalt?

✓ **Welke externe partijen hebben toegang tot de gegevens of slaan deze op?**

- Wat zijn de afspraken met externe partijen (zoals opdrachtgevers, leveranciers, ingeschakelde derden)

✓ **Hoelang worden de persoonsgegevens bewaard?**

- Persoonsgegevens mogen ingevolge artikel 5 AVG niet langer bewaard worden dan noodzakelijk voor de doelen waarvoor zij worden verwerkt
- Concrete bewaartermijnen zijn af te leiden uit wettelijke bewaarplichten, zoals de administratieplicht en de fiscale bewaarplicht. Op de website van de AP staat meer informatie over bewaartermijnen.
- Ook zal moeten worden ingeregeld dat de persoonsgegevens bij het verstrijken van de bewaartermijnen worden verwijderd.

2. Bepalen van uw privacyrechtelijke rol

Om te kunnen beoordelen aan welke verplichtingen van de AVG voldaan moet worden zal bepaald moeten worden wat de rol is van de organisatie of professional voor de verwerkingen van persoonsgegevens. Zie ook de begrippen in de inleiding.

✓ **Bepaal per gegevensstroom welke wettelijke rol u heeft ten opzichte van de gegevensverwerking**

- Bepaalt u het doel van de verwerking? Dan bent u verwerkingsverantwoordelijke.
- Verwerkt u de gegevens *uitsluitend* ten behoeve van een opdrachtgever? Dan bent u verwerker.
- Ook als u in opdracht van een opdrachtgever werkt, maar wel zelf bepaalt welke persoonsgegevens u verwerkt en hoe. Dan bent u ook verwerkingsverantwoordelijke.

Deze checklist is gericht op de verplichtingen voor de verwerkingsverantwoordelijke. Een verwerker heeft minder verplichtingen en zal ook een ander register moeten opstellen en bijhouden.

3. Opstellen register van verwerkingsactiviteiten

De verwerkingsverantwoordelijke zal op grond van artikel 30 lid 1 AVG een register van verwerkingsactiviteiten moeten opstellen en bijhouden. Dit is een onderdeel van de verantwoordingsplicht van de AVG. Het gaat om de registratie van alle structurele verwerkingen, zoals genoemd onder 1. De gegevens die in het register moeten worden opgenomen zijn:

✓ **Contactgegevens van de organisatie of professional en eventueel van de Functionaris voor de gegevensbescherming (FG)**

✓ **Groep(en) personen waar de gegevens betrekking op hebben (betrokkenen)**

- Denk aan klanten of opdrachtgevers, maar ook specifieke groepen die kwetsbaar kunnen zijn, zoals kinderen of zieken.

✓ **Categorieën van persoonsgegevens**

- Welke concrete gegevens worden verwerkt (contactgegevens, pasfoto, etc.).

✓ **De doeleinden waarvoor de persoonsgegevens worden verwerkt**

- Opgenomen moet worden waarom de concrete persoonsgegevens worden verwerkt.

✓ **Categorieën van ontvangers**

- Aan wie worden de persoonsgegevens verstrekt (intern en extern).

✓ **Doorgifte van persoonsgegevens naar landen buiten de EU**

- Met informatie over het land of de internationale organisatie en de wijze waarop voldaan wordt aan de wettelijke regels voor doorgifte.

✓ **De beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist (bewaartermijnen)**

- Als een wettelijke bewaartermijn geldt, zoals fiscale bewaartermijnen, dan kan die worden opgenomen.

✓ **Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen**

- Hier kunnen concrete maatregelen worden genoemd of verwezen worden naar een beveiligingsbeleid.

Voor het opstellen van het register kan gebruik gemaakt worden van dit sjabloon[1] (Excelbestand). In dit sjabloon zijn een aantal velden meer opgenomen dan strikt vereist op grond van de AVG, zoals hiervoor opgesomd. Dat kan helpen om een beter overzicht te krijgen van de risico's en beter te kunnen voldoen aan de verantwoordingsplicht.

---

4. Wordt voldaan aan de privacybeginselen

De basisbeginselen wijzigen onder de AVG niet. Ze staan opgesomd in artikel 5 AVG. Het grote verschil is dat de verwerkingsverantwoordelijke moet kunnen aantonen dat wordt voldaan aan deze beginselen. Controleer daarom voor de verwerkingen waarvoor u verwerkingsverantwoordelijke bent of aan deze beginselen wordt voldaan. Hét uitgangspunt is dataminimalisatie, namelijk dat niet meer persoonsgegevens mogen worden verwerkt dan **noodzakelijk** is om het doel van de verwerking te kunnen bereiken.

Download hier de checklist basisbeginselen privacyregelgeving. Deze geeft een beknopte toelichting op de belangrijkste beginselen die voor iedere verwerking van persoonsgegevens gelden.

✓ **Controle op de rechtmatigheid van de verwerking**

- Voor iedere gegevensstroom zal een wettelijke grondslag uit artikel 6 AVG moeten bestaan, zoals de uitvoering van een overeenkomst met de betrokkene, een wettelijke verplichting, een gerechtvaardigd belang of uitdrukkelijke toestemming
  - Let op met toestemming! Artikel 7 AVG en artikel 8 AVG kennen strenge eisen voor toestemming. Zie de checklist basisbeginselen privacyregelgeving.

[1] Beveiligingsinstellingen op uw computer kunnen voorkomen dat dit Exceldocument kan worden gedownload. Dit sjabloon wordt meegeleverd bij deze checklist.

Controle op verbod verwerking bijzondere persoonsgegevens

- In artikel 9 en artikel 10 AVG is een verbod opgenomen op de verwerking van bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens over:
  - ras of etnische afkomst
  - politieke opvattingen
  - religieuze of levensbeschouwelijke overtuigingen
  - lidmaatschap vakbond
  - genetische en biometrische gegevens met het oog op identificatie
  - gezondheid
  - seksueel gedrag of seksuele gerichtheid
  - strafrechtelijke veroordelingen of strafbare feiten

- In Nederland wordt het BSN ook als een bijzonder persoonsgegeven beschouwd. Deze staat niet in de AVG, maar wel in de UAVG (Uitvoeringswet op de AVG). In artikel 46 UAVG[2] is opgenomen dat het BSN slechts mag worden gebruikt als dat bij wet is bepaald en dan ook uitsluitend ter uitvoering van die wet, dan wel voor de doeleinden die bij die wet zijn bepaald.

Welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel

- Gecontroleerd moet worden of alle persoonsgegevens die per gegevensstroom worden verwerkt noodzakelijk zijn om de omschreven doelen te bereiken en niet voor andere doelen worden gebruikt (doelbinding). Als meer gegevens worden verwerkt dan noodzakelijk zullen die gegevens verwijderd moeten worden (dataminimalisatie).

Controle op juistheid van gegevens…

- …en aanpassen van de gegevens als deze niet meer kloppen (bijvoorbeeld als een adreswijziging wordt doorgegeven).

Proportionaliteit en subsidiariteit

- Het beginsel van *proportionaliteit* betekent dat de inbreuk op de privacy van de betrokkene evenredig moet zijn aan het doel dat wordt beoogd met de verwerking. Om dat te beoordelen zal een belangenafweging nodig zijn tussen de privacybelangen van de betrokkene en het belang van de verwerkingsverantwoordelijke bij de verwerking van een *specifiek* persoonsgegeven.
- Het s*ubsidiariteitsbeginsel* houdt in dat het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere - voor de betrokkene minder nadelige wijze - kan worden bereikt.

[2] Ten tijde van het opstellen van dit stappenplan is de UAVG nog een wetsvoorstel.

Als het alleen *handig* of *makkelijk* is om bepaalde gegevens te verwerken, dan is die verwerking zeer waarschijnlijk in strijd met het noodzakelijkheidsvereiste.

Is de verwerking bekend bij betrokkenen?

- Transparantie is een belangrijk privacybeginsel. De betrokkene zal moeten worden geïnformeerd over de wijze van verwerking van zijn of haar persoonsgegevens. Zie de volgende stap in deze checklist.

Hoe worden de gegevens bewaard

- Nieuw in de AVG is dat in artikel 5 lid 1 sub e AVG expliciet wordt vermeld dat persoonsgegevens alleen mogen worden bewaard in een vorm dat de betrokkene niet langer is te identificeren dan voor het bereiken van de doeleinden noodzakelijk is. Dit is bijvoorbeeld van belang voor het maken van analyses en rapportages. Als geen identificatie van de persoon nodig is, zullen de gegevens bijvoorbeeld gepseudonimiseerd moeten worden. Dat betekent dat de persoonsgegevens zo worden verwerkt dat deze niet direct herleidbaar zijn naar een persoon.

Pseudonimiseren kan door de namen en andere direct herleidbare gegevens te verwijderen of te vervangen door willekeurige tekens.

5. Opstellen privacyverklaring

De AVG stelt concrete eisen aan de wijze waarop betrokkenen moeten worden geïnformeerd. Artikel 12 AVG verplicht de verwerkingsverantwoordelijke om betrokkenen op een duidelijke en gemakkelijk toegankelijke te informeren. De wijze waarop mag zelf bepaald worden. Wel moet de informatie in principe voorafgaand aan de verwerking worden verstrekt. Een privacyverklaring op de website is een praktische manier om betrokkenen te informeren. In andere communicatie kan dan naar die privacyverklaring worden verwezen.

In artikel 13 en artikel 14 AVG staat welke informatie aan betrokkenen verstrekt moet worden.

Het gaat om:

- de identiteit en contactgegevens van de verwerkingsverantwoordelijke
- de identiteit en contactgegevens van de FG (indien van toepassing)
- categorieën van persoonsgegevens

- de verschillende doeleinden waarvoor de gegevens worden verwerkt
- de grondslagen op basis waarvan de persoonsgegevens worden verwerkt
- aanvullende informatie in geval van de grondslagen toestemming en gerechtvaardigd belang
- categorieën van externe ontvangers van de persoonsgegevens
- doorgifte van persoonsgegevens buiten de Europese Economische Ruimte (indien van toepassing) met de getroffen maatregelen
- bewaartermijnen of bewaarcriteria
- rechten van de betrokkenen, waaronder de klachtmogelijkheid bij de Autoriteit Persoonsgegevens
- de bron waar de persoonsgegevens vandaan komen en of de verstrekking van persoonsgegevens verplicht is en wat de gevolgen zijn als de gegevens niet worden verstrekt
- of persoonsgegevens worden gebruikt voor profilering en zo ja, op welke wijze
- zelf gewenste aanvullende informatie, bijvoorbeeld over de beveiliging van de persoonsgegevens of dat afspraken zijn gemaakt met de externe ontvangers die de persoonsgegevens verkrijgen.

Met een goede privacyverklaring kunt u laten zien dat u serieus bezig bent met privacy. Wel moet de concrete omgang met de persoonsgegevens niet afwijken van hoe het in de privacyverklaring staat!

Bij het opstellen van een privacyverklaring kan gebruik gemaakt worden van dit model privacyverklaring[3]. Het is een model, dus deze zal moeten aangepast worden aan de concrete, eigen situatie. Er staan opmerkingen in de kantlijn om het invullen van het model te vergemakkelijken.

---

6. Maak afspraken met externe partijen

Op de verwerkingsverantwoordelijke rusten alle wettelijke verplichtingen. Op een verwerker rusten veel minder wettelijke verplichtingen. Deze dient zich met name te houden aan de schriftelijke instructies van de verwerkingsverantwoordelijke en mag de persoonsgegevens niet voor eigen doeleinden gebruiken.

Bij het inschakelen van een verwerker zal op grond van artikel 28 AVG een verwerkersovereenkomst gesloten moeten worden. In de verwerkersovereenkomst moeten onder meer afspraken te worden vastgelegd over de omgang met persoonsgegevens, de beveiliging en de meldplicht datalekken.

[3] Beveiligingsinstellingen op uw computer zouden kunnen voorkomen dat dit Worddocument kan worden gedownload. Dit modeldocument wordt meegeleverd bij deze checklist.

In deze "checklist verwerkersovereenkomst" staan alle onderdelen toegelicht die in een verwerkersovereenkomst dienen te staan. Dit "model verwerkersovereenkomst"[4] kan gebruikt worden als sjabloon voor het opstellen van een verwerkersovereenkomst. In de kantlijn staan opmerkingen om te helpen bij het nader invullen van het model.

Als met een partij persoonsgegevens worden uitgewisseld die de persoonsgegevens ook gebruikt voor eigen doeleinden, dan zijn beide partijen verwerkingsverantwoordelijken.

✓ **Wanneer sprake is van meerdere verwerkingsverantwoordelijken vereist artikel 26 AVG dat afspraken worden gemaakt over onder meer de verdeling van de onderlinge verantwoordelijkheden ten aanzien van de verwerkingen.**

✓ **Ook moet tussen partijen duidelijk worden afgesproken wie de betrokkenen informeert over de verwerkingen en over de uitwisseling van hun gegevens tussen partijen. Daarnaast moet worden afgesproken hoe wordt omgegaan met verzoeken van betrokkenen.**

Op grond van de AVG kan de betrokkene bij iedere partij terecht. Partijen zijn hoofdelijk aansprakelijk als de betrokkene schade zou hebben door het handelen van één van beide partijen. Dat neemt niet weg dat onderling de verantwoordelijkheid kan worden afgebakend.

7. Zorg voor een op het risico afgestemde beveiliging

Om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking, moet iedere verwerkingsverantwoordelijke én verwerker passende technische en organisatorische maatregelen treffen. Wat passend is hangt af van de *risico's* die een betrokkene loopt indien zijn gegevens verloren gaan of op straat komen te liggen. Zo is het risico voor een betrokkene is een stuk kleiner als zijn e-mailadres op straat ligt dan wanneer een kopie van zijn paspoort op straat komt te liggen.

[4] Beveiligingsinstellingen op uw computer zouden kunnen voorkomen dat dit Worddocument kan worden gedownload. Deze checklist en modeldocument wordt meegeleverd bij deze checklist.

✓ **Maak een risico-analyse en stem de beveiligingsmaatregelen daarop af**

- Een hoger risico vereist zwaardere beveiligingsmaatregelen. Er moeten niet alleen technische maatregelen, zoals een firewall of versleuteling, maar ook organisatorische maatregelen, zoals fysieke toegangsbeveiliging of een clean desk policy, worden getroffen.
- De Autoriteit Persoonsgegevens heeft Richtsnoeren beveiliging van persoonsgegevens gepubliceerd met een toelichting over hoe bepaald kan worden welke beveiligingsmaatregelen getroffen moeten worden.

✓ **Data Protection Impact Assessment (DPIA)**

- De gegevensbeschermingseffectbeoordeling (DPIA) uit artikel 35 AVG is een instrument om de risico's voor een betrokkene bij een verwerking van zijn persoonsgegevens te beoordelen. Voor verwerkingen die waarschijnlijk een hoog risico meebrengen voor de rechten en vrijheden van natuurlijke personen is het uitvoeren van een DPIA verplicht.
- In de Richtsnoeren voor gegevensbeschermingseffectbeoordelingen van de Europese privacy toezichthouders staat meer informatie over de DPIA.
- Zie voor een methode voor het uitvoeren van een DPIA het Model gegevensbeschermingseffectbeoordeling rijksdienst of de Handreiking PIA van Norea.

✓ **Privacy by design en privacy by default**

- Al bij het ontwerpen of bedenken van nieuwe producten en diensten zal ervoor gezorgd moeten worden dat de persoonsgegevens goed worden beschermd. Op grond van artikel 25 AVG dient de verwerkingsverantwoordelijke onder meer maatregelen te treffen om ervoor te zorgen dat de privacybeginselen, zoals dataminimalisatie en opslagbeperking, op een doeltreffende manier worden toegepast.
- Privacy by default brengt mee dat de standaardinstellingen zo moeten worden ingericht dat alléén persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel van een bepaald systeem of app.

8. Stel een procedure op voor de meldplicht datalekken

Sinds 1 januari 2016 kent Nederland de meldplicht datalekken, die onder de AVG hetzelfde blijft (artikel 33 AVG en artikel 34 AVG). Een datalek moet binnen 72 uur bij de Autoriteit Persoonsgegevens worden gemeld worden, tenzij er geen nadelige gevolgen voor de betrokkenen te verwachten zijn. Of er gemeld moet worden hangt af van de risico's voor betrokkenen. Tevens kan de verplichting bestaan om betrokkenen te informeren, zodat zij maatregelen zouden kunnen nemen om zich te beschermen.

Melden bij de Autoriteit Persoonsgegevens

- Om te bepalen of een datalek gemeld moet worden bij de Autoriteit Persoonsgegevens heeft zij beleidsregels geschreven waar in staat hoe die afweging kan worden gemaakt. Die kan als leidraad dienen.
- Relevant is om te bepalen of de gelekte gegevens van *gevoelige aard* zijn. Gegevens van gevoelige aard zijn enerzijds de bijzondere persoonsgegevens zoals opgenomen in artikel 9 en artikel 10 AVG en daarnaast financiële gegevens, of gegevens over schulden, gegevens die stigmatiserend kunnen zijn (verslaving, naaktfoto's, specifieke problemen), inloggegevens, gegevens die bruikbaar zijn voor identiteitsfraude (kopie ID, BSN, handtekening, biometrische gegevens) en gegevens die vallen onder een beroepsgeheim. Als één zo'n gegeven is gelekt, dan moet er gemeld worden.

Informeren betrokkenen

- Als een datalek gemeld moet worden bij de Autoriteit Persoonsgegevens moet tevens worden beoordeeld of de getroffen betrokkenen moeten worden geïnformeerd. Als het datalek ongunstige gevolgen kan hebben voor de persoonlijke levenssfeer zullen op grond van artikel 34 AVG ook de betrokkenen moeten worden geïnformeerd

---

Deze checklist procedure meldplicht datalekken kan helpen bij het opstellen van een procedure voor de meldplicht datalekken.

Lees voor meer informatie deze blogpost en de guidelines van de Europese privacy toezichthouders.

9. Rechten van betrokkenen

Betrokkenen hebben diverse rechten op grond van de AVG. Daar zal de verwerkingsverantwoordelijke gehoor aan moeten geven, dus het goed deze rechten in beeld te hebben en voorbereid te zijn.

Inzageverzoek

- Op grond van artikel 15 AVG heeft de betrokkenen het recht om inzage te vragen in de persoonsgegevens die van hem worden verwerkt. Indien een betrokkene om inzage verzoekt dient deze binnen een maand een overzicht te krijgen met zijn of haar gegevensverwerkingen.

✓ **Correctierecht**

- Als zijn persoonsgegevens niet kloppen of onvolledig zijn, dan kan de betrokkene op grond van artikel 16 AVG een verzoek doen op rectificatie en aanvulling. In dat geval zullen de onjuiste persoonsgegevens aangepast moeten worden. Denk aan een adreswijziging of foutieve vermelding van een geslacht.

✓ **Recht op gegevenswissing**

- Het recht om vergeten te worden is een nieuw recht dat betrokkenen op grond van artikel 17 AVG krijgen. Dit is het recht om persoonsgegevens te laten wissen die bijvoorbeeld niet meer relevant zijn of die onrechtmatig zijn verwerkt.
- Tevens heeft de betrokkene op grond van artikel 18 AVG het recht om te vragen dat minder gegevens worden verwerkt.

✓ **Recht op dataportabiliteit**

- Betrokkenen krijgen op grond van artikel 20 AVG het recht op overdraagbaarheid van gegevens, oftewel het recht op *dataportabiliteit.*
- De betrokken mag vragen om zijn persoonsgegevens die digitaal zijn verwerkt "*in een gestructureerde, gangbare en machinaal leesbare vorm*" te verkrijgen en eventueel over te dragen aan een ander.

10. Doorgifte naar landen buiten de EER

✓ **Als persoonsgegevens worden doorgegeven aan landen buiten de EER gelden extra eisen**

- De EER bestaat uit alle landen van de EU, Liechtenstein, Noorwegen en IJsland. Deze laatste drie landen hebben zich ertoe verplicht de AVG te implementeren.
- Doorgifte kan opslag in een derde land zijn, bijvoorbeeld via een Amerikaanse cloudprovider, maar dit geldt bijvoorbeeld ook als personen uit een derde land toegang hebben tot de persoonsgegevens die zich in Europa bevinden. Zoals een systeembeheerder die vanuit India toegang heeft tot de systemen waarin persoonsgegevens staan.

✓ **Mogelijkheden**

- In artikel 49 AVG zijn er uitzonderingen opgenomen op grond waarvan doorgifte aan een derde land is toegestaan die geen passend beschermingsniveau hebben.

11. Functionaris voor de Gegevensbescherming

Drie categorieën organisaties zijn op grond van artikel 37 AVG verplicht om een Functionaris voor de Gegevensbescherming (FG) te hebben. De grootte van de organisatie is niet bepalend of een FG verplicht is, maar in geval van een hele kleine organisatie of een ZZP-er, zal niet snel sprake zijn van een grootschalige verwerking.

✓ **De volgende organisaties moeten een FG hebben:**

- overheidsinstellingen en publieke organisaties;
- organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen, zoals het stelselmatig observeren van personen;
- organisaties die hoofdzakelijk zijn belast met het grootschalig verwerken van bijzondere persoonsgegevens.

⚠ De Autoriteit Persoonsgegevens heeft (nog) geen lijst gepubliceerd met organisaties die verplicht zijn een FG aan te stellen. Dit zal dus zelf moeten worden beoordeeld. Kijk voor meer informatie op de website van de Autoriteit Persoonsgegevens en de informatie uit deze richtlijn van de Europese privacy toezichthouders.

✓ **Taken en positie FG**

- De FG heeft als hoofdtaak het bevorderen van een 'privacy cultuur' binnen de organisatie.
- De FG zal intern toezicht moeten houden op het naleven van de privacywetgeving.
- De FG is binnen de organisatie het aanspreekpunt voor de Autoriteit Persoonsgegevens.
- De FG moet zijn taken zo onafhankelijk mogelijk kunnen uitvoeren. De organisatie mag de FG geen instructies geven over de uitvoering van zijn taken.
- De FG mag niet ontslagen worden voor de uitvoering van zijn taken.

12. Interne bewustwording en borging

Alleen het hebben van de vereiste documenten is onvoldoende om te kunnen voldoen aan de privacywetgeving. Alle personen binnen de organisatie zullen zorgvuldig en in overeenstemming met de AVG moeten omgaan met persoonsgegevens. Daarnaast vragen de documenten aanpassing als er wijzigingen optreden in de verwerkingen. Dat zal geborgd moeten worden.

✓ **Intern bewustwordingsprogramma**

- Door middel van trainingen, workshops, flyers en dergelijke kan aandacht worden gegeven aan de zorgvuldige omgang met persoonsgegevens
- Steekproefsgewijze controles kunnen helpen bij bewuste omgang met persoonsgegevens
- Aandacht voor privacy besteden bij de introductie van nieuwe medewerkers

✓ **Borging van privacy**

- Bepaal wie welke documenten zal bijhouden, zoals het register van verwerkingsactiviteiten en de privacyverklaring
- Zorg voor evaluatiemomenten van de onderdelen uit deze checklist
- Let op bij nieuwe verwerkingen, zoals een nieuwe website of een nieuw systeem, dat de vereisten uit de AVG worden meegenomen

Bijlage TO-DO list AVG

Deze TO-DO list AVG hoort bij de Checklist AVG van MOS B.V.

- ☐ Maak een register van verwerkingsactiviteiten en zorg dat deze *up to date* wordt gehouden
  - Check of niet meer gegevens worden verwerkt dan nodig voor de doelen uit het register
  - Check of er bijzondere persoonsgegevens worden verwerkt en zo ja, of daar een wettelijke uitzondering op het verwerkingsverbod voor is

- ☐ Stel een privacyverklaring op, publiceer die op uw website en zorg ervoor dat betrokkenen naar de privacyverklaring worden verwezen (bijvoorbeeld via een link op (inschrijf)formulieren, brieven of overeenkomsten)

- ☐ Maak afspraken met partijen waar persoonsgegevens worden gedeeld (verwerkersovereenkomst of afspraken omtrent de omgang met persoonsgegevens)

- ☐ Stem beveiligingsmaatregelen af op het risico en leg ze vast in een beveiligingsbeleid

- ☐ Beoordeel of ten aanzien van nieuwe verwerkingen (bijvoorbeeld bij een nieuwe website of een nieuw IT systeem) een DPIA is vereist en houd rekening met 'privacy by design' en 'privacy by default'

- ☐ Stel een procedure meldplicht datalekken op en houd een datalekregister bij

- ☐ Check of voldaan kan worden aan de rechten van betrokkenen

- ☐ Check of voldaan wordt aan de extra eisen die gelden indien persoonsgegevens worden doorgegeven aan landen buiten de EER

- ☐ Beoordeel of een Functionaris voor de Gegevensbescherming moet worden aangesteld