Checklist voorbereiding op de AVG

Vanaf 25 mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG is een Europese verordening en werkt rechtstreeks door in alle lidstaten van de EU. De AVG vervangt de Wet bescherming persoonsgegevens (Wbp), maar is veel strenger dan de Wpb. Zo geeft de AVG burgers meer en stevigere privacyrechten en u als organisatie meer verantwoordelijkheden. Bovendien moet u kunnen aantonen dat u zich aan de AVG houdt.

Alle organisaties binnen de EU moeten vanaf 25 mei 2018 aan de AVG voldoen, uw organisatie dus ook! Doet u dat niet? Dan wachten u mogelijk hoge boetes. De Autoriteit Persoonsgegevens krijgt vanaf 25 mei 2018 meer bevoegdheden, onder meer om hoge boetes op te leggen. Het gaat om boetes tot twintig miljoen euro of 4% van de wereldwijde jaaromzet.

Om u te helpen u op de AVG voor te bereiden heeft Oprecht Advocaten deze checklist opgesteld. Wij geven aan welke stappen u moet nemen, en geven daarbij zo duidelijk mogelijk aan waarom. Heeft u tijdens het invullen van deze checklist behoefte aan meer toelichting? Of heeft u vragen? Neemt u dan gerust contact met ons op.

★ **Wijs binnen uw organisatie een verantwoordelijke aan voor implementatie van de AVG.**

Het kost tijd en capaciteit om u voor te bereiden op de AVG. U zult zich in de nieuwe regelgeving moeten verdiepen, zaken moeten uitzoeken en beleid moeten vastleggen, uw verwerkerscontracten moeten (laten) nagaan en mogelijk uw werkprocessen en/of (online) beveiligingssystemen moeten aanpassen.

Onder de AVG zijn sommige organisaties verplicht om een zogenaamde Functionaris Gegevensverwerking (FG) aan te stellen. Een FG is op de hoogte van de AVG. Een FG is verantwoordelijk voor naleving van de verplichtingen die daaruit voortvloeien en hij/zij is de contactpersoon voor uw organisatie voor betrokkenen en de toezichthouder. Een FG is verplicht:

- voor overheidsinstanties en publieke instanties
- als er systematisch en grootschalig persoonsgegevens worden verzameld
- als er op grote schaal bijzondere persoonsgegevens (zie de volgende stap) worden verwerkt

Ook als u niet verplicht bent een FG aan te stellen, adviseren wij u om één of meer medewerkers binnen uw organisatie verantwoordelijk te maken voor uw privacy compliance.

★ **Werkt u internationaal? Bepaal onder welke toezichthouder u valt.**

Onder de AVG krijgt u met één toezichthouder te maken, ook als u vestigingen heeft in meerdere EU-landen of grensoverschrijdende gegevensverwerkingen (gegevensverwerkingen in verschillende EU-lidstaten óf verwerkingen met impact in meerdere lidstaten) uitvoert. Deze toezichthouder wordt de 'leidende toezichthouder' genoemd.

De hoofdregel is dat de toezichthouder van de EU-lidstaat waar de hoofdvestiging van een organisatie is gevestigd, de leidende toezichthouder is.

Werkt u alleen in Nederland? Of is uw hoofdvestiging in Nederland? Dan valt u onder toezicht van de Nederlandse toezichthouder: de Autoriteit Persoonsgegevens.

★ **Breng de persoonsgegevens die u verwerkt in kaart.**

Door de ruime formulering van de AVG vallen straks meer gegevens dan nu onder het begrip 'persoonsgegevens'. Alle informatie over een geïdentificeerde of identificeerbaar natuurlijk persoon, die direct of indirect (bijvoorbeeld door middel van combinatie met andere gegevens) kan leiden tot identificatie van een natuurlijk persoon is een persoonsgegeven. Denkt u daarbij niet alleen aan iemands naam, adres, BSN-nummer of e-mailadres, maar ook aan IP-adressen of kentekengegevens.

Het begrip 'verwerking' wordt in de AVG als volgt gedefinieerd:

> "*Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwisselen of vernietigen van gegevens.*"

Van verwerking is dus al snel sprake. Zodra uw organisatie ook maar 'iets' doet met persoonsgegevens valt u onder de AVG.

Sommige persoonsgegevens worden als bijzondere persoonsgegevens aangemerkt. Dit zijn persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijken, alsmede genetische gegevens en gegevens over gezondheid of seksueel gedrag. Ook de persoonsgegevens van minderjarige kinderen vallen hieronder.

Bijzondere persoonsgegevens mogen onder de AVG in principe niet (zonder toestemming) worden verwerkt. De overige persoonsgegevens mag u alleen verwerken als daar een grondslag voor is. U mag bovendien alleen die gegevens verwerken die noodzakelijk zijn (dataminimalisatie).

Op grond van de AVG zult u dus uw gegevensverwerkingen in kaart moeten brengen. Beantwoord daarvoor de volgende vragen:

- Welke persoonsgegevens verwerken wij?
- Op basis van welke wettelijke grondslag?
- Met welk doel verwerken wij de gegevens?
- Wat zijn de gegevensstromen (waar komen ze vandaan en met wie delen wij ze)?
- Hoe gevoelig zijn de gegevens?
- Welke risico's lopen wij daarbij?

Denkt u hierbij niet alleen aan persoonsgegevens die u voor uw primaire processen verwerkt, maar bijvoorbeeld ook aan de persoonsgegevens van sollicitanten, bezoekers, personeel (als u de salarisadministratie heeft uitbesteed), alsmede aan gegevens die u van websitebezoekers verzamelt.

★ **Voer, als dat nodig is, een DPIA uit.**

Als de verwerking van persoonsgegevens een hoog privacyrisico met zich meebrengt voor de betrokkenen, kunt u op grond van de AVG verplicht zijn om een Data Protection Impact Assessment (DPIA) uit te voeren. In goed Nederlands heet de DPIA een 'gegevensbeschermingseffectbeoordeling'.

U hoeft niet voor elke gegevensverwerking een DPIA uit te voeren. Een DPIA is alleen verplicht als er een hoog privacyrisico is. Dat is in ieder geval zo als u:

- systematisch en uitvoerig persoonlijke aspecten evalueert
- op grote schaal bijzondere persoonsgegevens verwerkt
- op grote schaal en systematisch mensen volgt in publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht)

De Autoriteit Persoonsgegevens zal een lijst publiceren met verwerkingen waarvoor een DPIA verplicht is. Op dit moment is die lijst er nog niet. De Europese privacytoezichthouders hebben wel een lijst met 9 criteria opgesteld. Als uw gegevensverwerking aan 2 of meer van die criteria voldoet moet u een DPIA uitvoeren. De lijst met criteria vindt u hier.

Met een DPIA brengt u de privacyrisico's van uw gegevensverwerkingen gedetailleerd in kaart, waarna u concrete maatregelen kunt nemen om die risico's te beperken. Pas nadat u de DPIA heeft uitgevoerd en de resultaten zijn geïmplementeerd, mag u op grond van de AVG de verwerking uitvoeren.

★ **Stem uw privacy- en beveiligingsbeleid af op de AVG**

Als u weet welke persoonsgegevens u verzamelt, of u dat mag en welke risico's u daarbij loopt wordt het tijd om uw privacy- en beveiligingsbeleid op de AVG af te stemmen. Dit beleid dient u vervolgens te implementeren in uw processen en u dient dit onder de aandacht te brengen van uw medewerkers. Een bewustwordingsprogramma voor uw medewerkers kan daarbij geen kwaad. Het is daarbij belangrijk om op de volgende punten uw beleid te herzien, of beleid te maken:

- De AVG hanteert het principe van dataminimalisatie. Dat betekent dat u nooit meer persoonsgegevens mag verwerken dan noodzakelijk is. Bepaal welke gegevens dat zijn. Daarnaast moet u bepalen hoe lang u die persoonsgegevens bewaart. Let daarbij op maximale en minimale wettelijke bewaartermijnen. Beschrijf ook hoe u ervoor zorgt dat persoonsgegevens daadwerkelijk tijdig worden verwijderd.

- Voor een aantal gegevensverwerkingen heeft u op grond van de AVG toestemming van de betrokkene nodig. Bovendien moet u kunnen aantonen dat u die toestemming op de juiste manier heeft gevraagd en gekregen. De AVG stelt daarbij (strenge) eisen aan de manier waarop u toestemming vraagt, krijgt en registreert. Op grond van de AVG is van een rechtsgeldige toestemming pas sprake als deze zonder druk, ondubbelzinnig, geïnformeerd en specifiek is gegeven. Dit moet door middel van een actieve handeling, zoals een verklaring of het aanvinken van een vakje. Het impliciet aannemen van toestemming (bijvoorbeeld in een cookieverklaring of het vooraf invullen van vinkjes) is onvoldoende om rechtsgeldige toestemming te krijgen. Kinderen tot 16 jaar mogen niet zelf toestemming geven. Tot slot moet u betrokkenen het recht bieden om al gegeven toestemming te allen tijde eenvoudig in te trekken.

- De betrokkenen van wie u persoonsgegevens verwerkt krijgen onder de AVG meer en verbeterde rechten. Zo hebben zij straks niet alleen recht op inzage in hun gegevens en recht op correctie en verwijdering, maar ook het recht op dataportabiliteit. Dat betekent dat u er als verwerker voor moet zorgen dat de betrokkene de gegevens die u heeft verzameld op zijn of haar verzoek kan ontvangen en kan doorgeven aan een andere organisatie. Zorgt u dus dat u daar als organisatie op ingericht bent.

- Onder de AVG moet u passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen. U moet bovendien kunnen aantonen dat u die maatregelen heeft getroffen en waarom. Stel daarom een AVG-proof beveiligingsbeleid op, waarin u beschrijft welke maatregelen u per type verwerking heeft genomen, waarom u vindt dat dat voldoende is en hoe u dat test en evalueert.

- De AVG hanteert de verplichte uitgangspunten van privacy by design en privacy by default. Dit houdt in dat uw organisatie er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens worden beschermd en dat u alleen die persoonsgegevens verwerkt die noodzakelijk zijn voor het doel dat u wilt bereiken. Houdt daar bij het ontwerpen van producten en diensten dus ook daadwerkelijk

rekening mee. Neem bijvoorbeeld in uw beleid op dat de FG altijd wordt betrokken bij het ontwerp.

★ Maak een AVG-proof privacyverklaring

Onder de AVG moet u betrokkenen informeren over de verwerking van persoonsgegevens. Dit kan met een privacyverklaring. De specifieke inhoud van uw privacyverklaring hangt af van het type persoonsgegevens dat u verzamelt en hoe u deze gegevens verwerkt. Sommige gegevens zijn gevoeliger dan andere, waardoor u ook strengere waarborgen moet inbouwen. Maar elke organisatie is verplicht om tenminste de volgende informatie in de privacyverklaring opnemen:

- De naam en het adres van uw organisatie en, als u een FG heeft, de naam en contactgegevens van de FG.
- De categorieën persoonsgegevens die u verwerkt.
- Het doel waarvoor u de persoonsgegevens verwerkt. Bijvoorbeeld voor marketingdoeleinden, relatiebeheer en/of voor het uitvoeren van de overeenkomst. Als dit een wettelijke of contractuele verplichting of noodzakelijke voorwaarde voor de uitvoering van de overeenkomst is, moet u ook de gevolgen van het niet verstrekken van de persoonsgegevens vermelden.
- Aan wie u de persoonsgegevens verstrekt, of wie nog meer toegang hebben tot de gegevens. Bijvoorbeeld hosting bedrijven, Google AdWords, of MailChimp.
- Of u gegevens doorgeeft aan landen buiten de EU.
- Hoe lang u de gegevens bewaart. Dit mag niet langer zijn dan voor het doel, waarvoor u deze verzamelt, nodig is.
- Hoe de betrokkene gebruik kan maken van het recht op inzage in de gegevens die u verwerkt.
- Hoe de betrokkene zijn of haar gegevens kan laten corrigeren of verwijderen, of de toestemming voor de verwerking kan intrekken.
- Hoe de betrokkene gebruik kan maken van het recht van overdracht van zijn of haar gegevens aan een derde partij.
- Hoe de betrokkenen een klacht kan indienen bij de Autoriteit Persoonsgegevens.

Deze informatie moet beknopt, transparant, begrijpelijk en makkelijk toegankelijk zijn. U moet de informatie schriftelijk of ‘met andere middelen’ verstrekken, in beginsel op het moment dat de persoonsgegevens worden verzameld. Zo kunt u bijvoorbeeld uw privacyverklaring op uw website opnemen. U kunt dan in andere vormen van (elektronische) communicatie eenvoudig een link naar die pagina opnemen.

★ Check of uw verwerkersovereenkomsten voldoen aan de AVG

Verzamelt u persoonsgegevens, maar schakelt u andere partijen (verwerkers) in bij de verwerking ervan? Bijvoorbeeld omdat u gebruik maakt van de diensten van een salarisadministrateur, expediteur, vervoerder of clouddienstverlener? Dan blijft u verantwoordelijk en dus ook aansprakelijk voor wat er met die persoonsgegevens gebeurt. U bent in die gevallen op grond van de AVG verplicht om een verwerkersovereenkomst af te sluiten.

In een verwerkersovereenkomst legt u vast dat de verwerkers waar u mee werkt de persoonsgegevens van uw medewerkers, klanten of andere betrokkenen op dezelfde manier verwerken en beveiligen als u dat doet. U neemt er onder andere in op dat de verwerker:

- persoonsgegevens alleen op uw instructie verwerkt
- passende technische en organisatorische beveiligingsmaatregelen neemt
- alle persoonsgegevens vertrouwelijk behandelt
- meewerkt als een betrokkene zijn of haar rechten inroept
- de persoonsgegevens na afloop van de verwerking wist of teruggeeft aan u
- meewerkt aan verzoeken van toezichthouders
- alle eigen verplichtingen uit de AVG nakomt

Maak dus inzichtelijk wie uw gegevens verwerkt, controleer of de overeenkomsten die u met hen heeft voldoen aan de AVG en laat deze overeenkomsten waar nodig aanpassen.

★ **Stel een protocol datalekken op**

Een datalek zit in een klein hoekje. We spreken van een datalek als persoonsgegevens in handen vallen van derden die eigenlijk geen toegang tot die gegevens zouden mogen hebben. Daarvoor is het niet nodig dat de gegevens gehackt of gestolen zijn. Ook een door een medewerker verloren laptop of usb-stick, een verkeerd geadresseerde e-mail of een uitgeprinte lijst met klantgegevens die wordt verloren, is een datalek.

Onder de AVG bent u verplicht om bepaalde datalekken zo snel mogelijk (liefst binnen 72 uur) te melden aan de toezichthouder. Ook zult u onder omstandigheden de betrokkenen over een datalek moeten informeren. Het is dus belangrijk dat u een protocol datalekken opstelt en in uw organisatie implementeert. Daarnaast moet u in uw verwerkersovereenkomsten goede afspraken maken, voor het geval zich bij een verwerker een datalek voordoet.

U moet bovendien een register bijhouden van alle datalekken die zich bij u voordoen. Dus ook van de datalekken die u niet hoeft te melden bij de toezichthouder.

★ Leg een register aan van uw gegevensverwerkingen

Vanaf 25 mei 2018 moeten organisaties met meer dan 250 werknemers kunnen aantonen dat zij in overeenstemming met de AVG handelen. Zij moeten een register bijhouden van alle gegevensverwerkingen die binnen die organisatie, of onder verantwoordelijkheid van die organisatie plaatsvinden.
Deze verplichting geldt ook voor organisaties met minder dan 250 werknemers die:

- gegevens verwerken waar een DPIA verplicht is
- structureel persoonsgegevens verwerken
- bijzondere persoonsgegevens verwerken

In dit register staat in ieder geval de volgende informatie:

- De naam en het adres van uw organisatie en, als u een FG heeft, de naam en contactgegevens van de FG.
- Het doel waarvoor u de persoonsgegevens verwerkt.
- De categorieën persoonsgegevens die u verwerkt (NAW-gegevens, contactgegevens, betaalgegevens).
- De categorieën betrokkenen (werknemers, klanten, websitebezoekers)
- Aan wie u de persoonsgegevens verstrekt.
- Of u gegevens doorgeeft aan landen buiten de EU.
- De bewaartermijn van de gegevens.
- De wijze van beveiliging (encryptie, pseudonimisering).

De Autoriteit Persoonsgegevens mag het register opvragen. U bent dan verplicht om inzage te geven.