VAN IERSEL
LUCHTMAN
ADVOCATEN

FACTSHEET: **IE / IT & PRIVACY**

Bent u AVG-compliant?

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze verordening stelt privacyregels vast voor de gehele Europese Unie. Uw organisatie zal ook aan deze regelgeving moeten voldoen. In deze factsheet lichten wij toe wat uw organisatie moet doen om AVG-compliant te worden en hoe wij u hierin kunnen bijstaan.

BENT U AVG-COMPLIANT?

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van kracht. De AVG geldt voor de hele Europese Unie en is in het Engels bekend als de General Data Protection Regulation (GDPR).

UITGANGSPUNTEN

AVG-grondslagen

Niet iedereen mag zomaar persoonsgegevens verwerken. U heeft hier alleen het recht toe als u zich kunt baseren op minimaal één van de volgende grondslagen:

- u heeft toestemming van de betreffende persoon;
- het is noodzakelijk voor de uitvoering van een overeenkomst;
- het is noodzakelijk om de vitale belangen (bijv. gezondheid) van iemand te beschermen;
- het is noodzakelijk voor de vervulling van een taak van algemeen belang of het openbaar gezag;
- het is noodzakelijk voor de behartiging van uw gerechtvaardigde belangen.

De AVG hanteert enkele uitgangspunten die in acht genomen moeten worden bij de verwerking van persoonsgegevens:

- Rechtmatigheid, behoorlijkheid en transparantie
  Verwerkingen moeten rechtmatig, behoorlijk en transparant zijn.
- Doelbinding
  Verwerking mag enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
- Minimale gegevensverwerking
  Verwerkingen moeten tot enkel het noodzakelijke beperkt worden.
- Juistheid
  Persoonsgegevens moeten juist zijn en waar nodig geactualiseerd (of gewist) worden.
- Opslagbeperking
  Persoonsgegevens mogen niet langer opgeslagen worden dan noodzakelijk.
- Integriteit en vertrouwelijkheid
  Passende technische en organisatorische maatregelen moeten genomen worden om onrechtmatige of ongeoorloofde verwerking te voorkomen en onopzettelijk verlies, vernietiging of beschadiging van persoonsgegevens te voorkomen.

Aan de hand van de volgende punten lichten wij toe wat uw organisatie moet doen om aan de AVG te voldoen en hoe wij u hierin kunnen bijstaan:

- Privacyverklaring
- Verwerkersovereenkomst
- Privacy Impact Assessment (PIA)
- Functionaris Gegevensbescherming (FG)
- Verwerkingsregister

Afsluitend gaan we kort in op mogelijke gevolgen indien uw organisatie niet voldoet aan de AVG.

VANIERSEL LUCHTMAN
advocaten die naast u staan

PRIVACYVERKLARING

Opstellen formats

Wij kunnen u bijstaan met het opstellen van een privacyverklaring of een verwerkersovereenkomst. Hiervoor hebben we standaard formats ontworpen die we samen verder invullen en toespitsen op uw organisatie.

Met betrekking tot de verwerkersovereenkomst hebben wij formats die zijn toegespitst op de rol die u inneemt als verwerkingsverantwoordelijke, verwerker of sub-verwerker.

Iedere organisatie die persoonsgegevens verwerkt, dient een privacyverklaring te hebben om betrokkenen te informeren. Hierbij hebben we te maken met interne betrokkenen (eigen personeel) en externe betrokkenen (klanten, leveranciers en andere relaties).

U dient onder meer de volgende zaken in een privacyverklaring op te nemen:

- welke persoonsgegevens u verzamelt;
- voor welke doeleinden u ze gebruikt;
- hoe lang u ze bewaart;
- met wie u gegevens deelt;
- welke technische en organisatorische beveiligingsmaatregelen u heeft genomen. Denk hierbij aan:
  - beveiligingsbeleid
  - omgang met datadragers
  - protocol voor datalekken
  - toegangsbeleid
  - beleid over de omgang met verzoeken van betrokkenen

Verder moeten betrokkenen geïnformeerd en gewezen worden op hun rechten. Denk onder andere aan inzage, correctie en verwijdering van hun persoonsgegevens. Maar ook het recht om bezwaar te maken en het klachtrecht bij de Autoriteit Persoonsgegevens.

Zorg er tevens voor dat de door uw organisatie getroffen beveiligingsmaatregelen voldoen aan het criterium van 'passende technische en organisatorische maatregelen'. Welke dit precies zijn hangt af van de gevoeligheid en hoeveelheid van de persoonsgegevens die u verwerkt. Hoe gevoeliger de persoonsgegevens zijn, of hoe groter het aantal persoonsgegevens dat u verzamelt, des te strenger moeten de veiligheidsmaatregelen zijn.

VERWERKINGSOVEREENKOMST

Indien u een andere partij inschakelt om gegevens voor u te verwerken, of zelf daarvoor wordt ingeschakeld, dient u in principe een verwerkersovereenkomst met die partij te sluiten. In deze overeenkomst moeten in ieder geval de volgende onderwerpen geregeld worden:

- welke persoonsgegevens voor welke doeleinden verwerkt worden;
- het doel van de verwerking;
- de beveiligingsmaatregelen die moeten worden genomen, of al zijn genomen;
- de wijze waarop verwerker over beveiligingsincidenten / datalekken rapporteert;
- de rol van de verwerker bij meldingen aan de Autoriteit Persoonsgegevens / betrokkenen;
- de inschakeling van sub-verwerkers;
- de verwerking van persoonsgegevens buiten Nederland;
- de wijze waarop verantwoordelijke toeziet op de naleving;
- de verdeling van aansprakelijkheid voor eventuele schade;
- de voorwaarden voor heronderhandeling of beëindiging van de overeenkomst en de gevolgen daarvan.

PRIVACY IMPACT ASSESSMENT (PIA)

Uitvoeren PIA

Mocht uit het PIA stappenplan blijken dat uw organisatie een PIA moet uitvoeren, dan kunnen wij u antwoord bieden omtrent de volgende punten:

- Wie dient u bij de PIA te betrekken?
- Waar dient de PIA op te zien?
- Wat dient er in de PIA meegenomen te worden?
- Wat moet er gebeuren als er een hoog restrisico is?
- Hoe zit het met veranderende verwerkingen?

Het kan zijn dat u een PIA, oftewel een 'gegevensbeschermingseffectbeoordeling', moet uitvoeren. Dit is een uitgebreide risicoanalyse van de verwerking van persoonsgegevens binnen en door uw organisatie. De verwerkingen, de risico's die daarmee gepaard gaan, de maatregelen die zijn genomen om risico's te beperken en de restrisico's die aanwezig zijn, worden daarbij in kaart gebracht.

Om te bepalen of uw organisatie een PIA moet uitvoeren, dient u te toetsen of de verwerkingen die u verricht, gelet op de aard, omvang, context en doeleinden daarvan waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. Dit is een vage omschrijving. En het is niet altijd eenvoudig om vast te stellen of een PIA verplicht is. Daarom hebben wij een stappenplan samengesteld.

VAN IERSEL LUCHTMAN
advocaten die naast u staan

PIA stappenplan
Indien uw organisatie aan minimaal twee van de volgende indicatoren voldoet, zal de verwerking van gegevens waarschijnlijk een hoog risico inhouden. U moet zich hierbij afvragen of er sprake is van:

- geautomatiseerde beoordeling van betrokkenen die (rechts)gevolgen hebben voor die betrokkenen;
- geautomatiseerde verwerking van persoonsgegevens om persoonlijke aspecten te analyseren c.q. te voorspellen (profiling);
- stelselmatige observatie;
- grootschalige verwerking;
- verwerking van gevoelige of bijzondere persoonsgegevens;
- gekoppelde databases die normaal niet gekoppeld zouden zijn;
- verwerking van persoonsgegevens over kwetsbare groepen (kinderen, zieken, werknemers);
- gebruik van innovatieve technologische of organisatorische oplossingen;
- doorgifte van gegevens buiten de EU;
- beperking van de rechten van betrokkenen of diens mogelijkheden om een dienst of overeenkomst te gebruiken bij de verwerking.

Bovenstaande criteria zijn niet altijd even makkelijk toe te passen. Wij kunnen een op uw organisatie toegespitste toets uitvoeren om te beoordelen of uw organisatie een PIA dient uit te voeren.

FUNCTIONARIS GEGEVENSBESCHERMING (FG)

Invulling FG

Wij kunnen toetsen of uw organisatie verplicht is om een FG aan te stellen.
Indien dit het geval is informeren wij u over de eisen waaraan een FG moet voldoen. Hoe zorgt u er bijvoorbeeld voor dat deze onafhankelijk optreedt? En welke opleiding en werkervaring dient de FG te hebben? Indien wenselijk leveren wij een hiernaast besproken Privacy-team zodat u deze functie extern kunt regelen.

De functionaris voor de gegevensbescherming (FG) houdt binnen een organisatie toezicht op de toepassing en naleving van de AVG. In een aantal gevallen zijn organisaties verplicht om een FG aan te stellen. U zult moeten toetsen of dat ook voor uw organisatie geldt. Dit doet u aan de hand van de volgende punten. Als één van deze situaties zich voordoet, bent u verplicht een FG aan te stellen:

1. U bent een overheidsinstantie/orgaan (met uitzondering van de rechterlijke macht) die een verwerking verricht.

2. Uw organisatie is hoofdzakelijk belast met verwerkingen die regelmatige of stelselmatige observatie op grote schaal van betrokkenen vereisen.

3. Uw organisatie is hoofdzakelijk belast met grootschalige verwerking van bijzondere categorieën van persoonsgegevens of strafrechtelijke veroordelingen en strafbare feiten.

Privacy-team
Indien u een FG aanstelt, kunt u deze functie intern of extern beleggen. In het tweede geval kan ons Privacy-team voor u als FG optreden. Maar het team kan ook uw FG ondersteunen.

Ons Privacy-team bestaat uit advocaten die naast het privacyrecht nog een ander specialisme hebben. Denk hierbij bijvoorbeeld aan arbeidsrecht, ICT-recht, ondernemingsrecht en gezondheidsrecht. U kunt het team inzetten naar gelang de capaciteit die u nodig heeft. Is het bijvoorbeeld een periode wat rustiger, dan schaalt u het terug. Is er onverhoopt sprake van een datalek en heeft u meer ondersteuning nodig, dan kunt u opschalen.

VERWERKINGSREGISTER

Opstellen verwerkingsregister

Voor het verwerkingsregister hebben wij een format ontwikkeld.
Het blijkt vaak een tijdrovende klus te zijn om een verwerkingsregister voor de eerste keer in te vullen, maar u zult merken dat het verhelderend werkt en goed is om een overzicht te hebben. Het is zaak om het register up-to-date te houden.

Bijna iedere organisatie die persoonsgegevens verwerkt, moet een verwerkingsregister bijhouden. De enige uitzondering is voor kleine organisaties, die incidenteel persoonsgegevens verwerken waar weinig risico aan kleeft. Dit betreft dus geen gevoelige of bijzondere persoonsgegevens.

In een verwerkingsregister houdt u onder meer bij welke persoonsgegevens u verwerkt, voor welke doeleinden, hoe lang en met wie u ze deelt. Het verwerkingsregister is voor interne doeleinden, zodat u een duidelijk overzicht heeft van de verwerkingen binnen uw organisatie. U dient het verwerkingsregister up-to-date te houden als de verwerkingen binnen uw organisatie veranderen. De Autoriteit Persoonsgegevens kan inzage vorderen in het verwerkingsregister van uw organisatie.

VAN IERSEL LUCHTMAN
advocaten die naast u staan

HANDHAVING

Procedure

Mocht de Autoriteit Persoonsgegevens handhavend tegen uw organisatie optreden, kunnen wij u bijstaan.
Onze experts op het gebied van bestuursrechtelijke sanctieprocedures staan u bij in het gehele traject. Van onderzoek tot en met een beroepsprocedure tegen de sanctie bij de rechtbank.

Indien uw organisatie niet voldoet aan de AVG, kan de Autoriteit Persoonsgegevens sancties opleggen. U zult het al vaak gehoord hebben: boetes van maximaal € 20.000.000 of 4% van de wereldwijde jaaromzet als dat hoger is. Hier dienen wel een aantal kanttekeningen bij geplaatst te worden:

1. Een boete wordt niet zomaar opgelegd. Doorgaans volgt er eerst een bindende aanzegging van de Autoriteit Persoonsgegevens.

2. Een boete zal redelijk en evenredig moeten zijn in relatie tot de inbreuk.

3. De Autoriteit Persoonsgegevens kan voor een andere maatregel kiezen. Denk hierbij aan een last onder bestuursdwang of een last onder dwangsom. Dat houdt in dat de betreffende organisatie eerst de instructie krijgt om een overtreding te beëindigen. Wordt hier vervolgens geen gehoor aan gegeven, zal de Autoriteit zelf ingrijpen, of moeten er (alsnog) dwangsommen worden betaald.

Reputatieschade
Los van bovenstaande kanttekeningen, zal de Autoriteit Persoonsgegevens onderzoeken die zij verricht, en handhavingsmaatregelingen die zij treft, (doorgaans) wel publiceren. Dit kan voor reputatieschade zorgen wat voor een bedrijf minstens zo schadelijk kan zijn als een sanctie.

VAN IERSEL LUCHTMAN ADVOCATEN

Meer informatie

Mocht u na het doorlopen van deze factsheet meer informatie wensen, dan kunt u contact opnemen met Rik Geurts of Dewi Harkink van de sectie **IE/IT & Privacy**. Zij bieden u graag een passend advies.

RIK GEURTS

r.geurts@vil.nl / 088 - 90 80 838

Rik is advocaat sinds 2006 en heeft een bovengemiddelde vakkennis van privacywetgeving en van de praktijk van gegevensbescherming. Verder heeft hij ruime ervaring met IT-vraagstukken, automatiseringscontracten en automatiseringsgeschillen. Binnen het intellectuele eigendomsrecht is Rik thuis op het gebied van het auteursrecht, databankenrecht, het merken- en modellenrecht, het handelsnaamrecht en reclamerecht. Rik is lid van de Vereniging voor Auteursrecht en de Beneluxvereniging voor Merken- en Modellenrecht. Over bovengenoemde onderwerpen geeft hij regelmatig presentaties voor bedrijven, brancheorganisaties en onderwijsinstellingen.

DEWI HARKINK

d.harkink@vil.nl / 088 - 90 80 843

Dewi heeft zich gespecialiseerd in privacyvraagstukken en zijn vakkennis op dit gebied is dan ook bovengemiddeld. Hij heeft rechten gestudeerd aan Tilburg University en heeft zijn bachelor met genoegen afgerond. Tevens heeft Dewi het Honors Programme Top Class Law met succes voltooid en een master gevolgd in zowel het privaatrecht (cum laude) als in het strafrecht (met genoegen). Dewi liep destijds stage bij een kantoor dat is gespecialiseerd op het gebied van IE/IT & Privacy. Binnen Van Iersel Luchtman maakt hij tevens deel uit van het brancheteam Gaming.

Een overzicht van al onze advocaten vindt u op **www.vil.nl**

Middels deze factsheet delen wij graag onze juridische kennis met u. Wij zijn een team van circa 40 samenwerkende advocaten die naast u staan en optimaal gebruikmaken van elkaars kennis. Daarbij worden wij samen met u gedreven door hetzelfde doel. Uw branche is onze branche, uw uitdagingen zijn onze uitdagingen, uw kansen zijn onze kansen. We zeggen dan ook niet voor niets, Van Iersel Luchtman & U.

CONTACT

T. (088) 90 80 800

W. www.vil.nl

E. info@vil.nl

Breda

Wilhelminapark 15

4818 SL Breda

Postbus 4810

4803 EV Breda

's-Hertogenbosch

Meerendonkweg 21

5216 TZ 's-Hertogenbosch

Postbus 44

5201 AA 's-Hertogenbosch