Factsheet Algemene Verordening Gegevensbescherming (AVG)

Op 25 mei 2018 dient uw organisatie "AVG-proof" te zijn, of anders gezegd: u moet dan aan nog meer eisen op het gebied van privacy voldoen dan nu al het geval is. De (Europese) Algemene Verordening Gegevensbescherming (AVG) treedt dan in werking en is rechtstreeks van toepassing op iedere onderneming die persoonsgegevens verzamelt of verwerkt.

Afwachten?

Afwachten en we zien wel, gaat niet werken. Nu al kunnen bij schending van privacyregels hoge boetes worden opgelegd tot maximaal €820.000,- of 10% van de jaaromzet, maar vanaf mei 2018 kan dat oplopen tot maar liefst €20.000.000,- of 4% van de wereldwijde omzet. Denk verder aan bestuurdersaansprakelijkheid, dwangmaatregelen, een verbod op het nog langer verwerken van persoonsgegevens, negatieve publiciteit en ontevreden klanten en stakeholders.

Een woud van extra regels

Er moet aan flink wat voorwaarden voldaan zijn, ook door het midden – en kleinbedrijf. Denk aan:

- Een passend beveiligingsniveau van de IT-systemen, waarbij meestal de verplichting bestaat gegevens te pseudonimiseren of anderszins te versleutelen
- Het recht van de datasubjecten (degenen wier persoonsgegevens worden verwerkt) op inzage en rectificatie
- De plicht van om gegevens te wissen van datasubjecten
- Verplichtingen ten aanzien van de inrichting van organisatie en systemen opdat de gevraagde informatie snel en adequaat verstrekt kan worden
- Meer adequate verwerkingsovereenkomsten met alle verwerkers, die bovendien aan minimale kwaliteitsnormen moeten voldoen die moeten worden gegarandeerd en vooraf worden gecontroleerd
- Het aan te leggen register met alle persoonsverwerkingen
- Het altijd kunnen aantonen dat toestemming tot verwerking is verleend wanneer toestemming een vereiste is

- De verplichting alles in dit kader schriftelijk gedocumenteerd te hebben en aan een toezichthouder kunnen aantonen wat het beleid is en waarom bepaalde keuzes zijn gemaakt
- De meldplichten voor datalekken. Maar zo zijn er nog meer plichten en voorwaarden.

Verwerker of Verantwoordelijke

De verwerkingsverantwoordelijke of "Verantwoordelijke" is kortgezegd degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt en de verwerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. Het is niet altijd eenvoudig vast te stellen of het gaat om een verantwoordelijke of verwerker omdat die rollen wel eens door elkaar lopen. Accountants bijvoorbeeld zijn zelf ook altijd verantwoordelijk met hen hoef je geen verwerkersovereenkomst te sluiten maar een salarisstrokenverwerker is weer wel verwerker.

Wat zijn de belangrijkste AVG aandachtspunten?

1. Awareness

Zorg ervoor dat de relevante sleutelfiguren begrijpen wat de nieuwe privacyregels inhouden en wat deze betekenen voor uw organisatie. Denk daarbij aan alle stakeholders. Realiseert u zich dat er echt wat moet gebeuren en dat de boetes en niet te vergeten schadeclaims hoog kunnen oplopen als u niets doet. Schakel zo nodig adviseurs in om tijdig compliant te worden.

2. Rechten van betrokkenen

De rechten van betrokkenen zijn in de AVG aanzienlijk versterkt door onder meer de navolgende rechten, en daar moet u uw systemen op inrichten:

Recht op informatie
Op grond van beginselen transparantie dient betrokkene op de hoogte te worden gesteld van verwerking, ook ingeval persoonsgegevens niet van betrokkene zijn verkregen. Uit deze artikelen volgt uit de opsomming van punten feitelijk dat er uitgebreide volledige informatie dient te worden gegeven. Wie is verwerker, doeleinden daarvan, gaat het naar landen buiten de EU, duur, inzagerecht, vertrouwelijkheid en zo verder.

Recht van inzage
De betrokkene heeft het recht van de verwerker te vernemen wat er met zijn persoonsgegevens gebeurt, met een recht van rectificatie en onder meer het recht op kopieën van de verwerking.

Recht op rectificatie
Het recht op rectificatie van onjuiste persoonsgegevens wordt verder uitgewerkt in dit artikel. Betrokkene heeft ook recht op vervolledigen van persoonsgegevens onder meer door een aanvullende verklaring te verstrekken.

Recht op gegevenswissing / vergetelheid
De betrokkene heeft in veel gevallen recht op wissen van gegevens, bijvoorbeeld als de persoonsgegevens niet langer nodig zijn of onrechtmatig zijn verwerkt.

Recht op beperking van de verwerking
De betrokkene heeft onder meer recht op beperking van de verwerking gedurende de periode dat de verwerker de juistheid van de gegevens controleert, of in afwachting is van de door de betrokkene gemaakte bezwaren tegen de verwerking.

Recht op overdraagbaarheid / dataportabiliteit
De betrokkene heeft gratis recht op een gangbaar bestand van zijn data om die aan een andere verwerker ter beschikking te kunnen stellen.

Recht van bezwaar
De betrokkene mag altijd bezwaar maken tegen de verwerking van zijn persoonsgegevens, tenzij de verwerking bijvoorbeeld noodzakelijk is voor een taak van algemeen belang.

Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profiling
Er moet een menselijke tussenkomst zijn. Dit recht heeft de betrokkene als de verwerking hem in aanmerkelijke mate treft, maar bijvoorbeeld niet als het ter uitvoering van een overeenkomst is tussen een betrokkene en een verantwoordelijke. Indien gebruik gemaakt wordt van geautomatiseerde besluitvorming (ook wel profilering genoemd) dan dient de betrokkene hiervan op de hoogte gesteld te worden.

3. Verwerkingsregister en accountability

U dient een register aan te leggen van alle persoonsgegevensverwerkingen en een beleid te hebben ontwikkeld waar u zo nodig verantwoording over dient te kunnen afleggen. Dit is een behoorlijk klus omdat u alle persoonsgegevens verzamelingen binnen uw organisatie in beeld moet zien te krijgen. Welke persoonsgegevens verwerkt u, met welk doel, waar komen deze gegevens vandaan, met wie deelt u ze, welke bewaartermijnen gelden, bent u verwerker of verantwoordelijke, is er een verwerkersovereenkomst, wie is intern verantwoordelijk en zo verder. U kunt dit doen met behulp van een Excel spreadsheet of één van de vele tools die daarvoor zijn ontwikkeld.

4. Datalek draaiboek

U doet er verstandig aan een draaiboek te maken voor datalekken, en daar een team voor te formeren. Alle datalekken dient u te documenteren. U dient "serieuse" datalekken binnen 72 uur te melden bij de AP, en deze tevens onverwijld te melden aan betrokkenen. U dient zich in dit verband verder aan de te verwachten AVG-richtlijnen te houden.

5. Data Protection Impact Assessments (DPIA'S) , Privacy by design and default

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking een hoog privacy-risico met zich meebrengt. Privacy by design betekent dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk voor het doel van de verwerking. Privacy by default houdt in

dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Maar ook dat u uw systemen veilig inricht en ontwerpt door bijvoorbeeld persoonsgegevens te pseudonimiseren, te separeren, te abstraheren, te minimaliseren of te verbergen.

6. Data Protection Officer (DPO) of functionaris persoonsgegevens

Een DPO dient aangesteld te worden als de gegevens worden verwerkt door een overheidsinstelling, door een onderneming van meer dan 250 werknemers of ingeval door een organisatie substantieel veel persoonsgegevens worden verwerkt. Het kan ook op vrijwillige basis. Een dergelijke verplichte functionaris heeft in dienstverband een onafhankelijke positie en ontslagbescherming, en kan ook extern ingehuurd worden. Bij álle aangelegenheden die verband houden met de bescherming van persoonsgegevens moet de functionaris naar behoren en tijdig worden betrokken en om advies worden gevraagd. Dit houdt in dat de functionaris toegang wordt verschaft tot persoonsgegevens en verwerkingsactiviteiten. Verder moeten de benodigde middelen voor het kunnen vervullen van de taken en het in standhouden van de deskundigheid aan de functionaris ter beschikking worden gesteld. Indien van het advies van de functionaris wordt afgeweken, dient dit te worden gedocumenteerd. Omdat de functionaris zijn werk onafhankelijk moet kunnen verrichten, mogen geen instructies worden gegeven met betrekking tot de uitvoering van de taken. Ook mag de functionaris niet worden ontslagen of gestraft voor de uitvoering van zijn taken. De functionaris geniet dezelfde bescherming als leden van de ondernemingsraad en is gehouden tot geheimhouding of vertrouwelijkheid. Als de functionaris ook nog andere werkzaamheden verricht, mogen deze niet tot een belangenconflict leiden. Zo mogen bijvoorbeeld bestuursleden deze functie niet vervullen.

7. Toestemming van betrokkenen

Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring of het aanklikken van een vakje op een website, waaruit duidelijk blijkt dat vrijelijk, geïnformeerd en ondubbelzinnig wordt ingestemd met de voorgestelde verwerking van persoonsgegevens.

Vereisten voor rechtsgeldige toestemming: Vrijwillig, Specifiek, Jip & Janneke taal, Granulair, Geen conditie voor uitvoering contract, “Intrekbaar”. U moet bijvoorbeeld een app niet standaard de locatie van gebruikers laten registeren, vakjes niet vooraf aanvinken. U moet achteraf ook kunnen aantonen dat u geldige toestemming van betrokkenen heeft gekregen om hun persoonsgegevens te verwerken.

8. Verwerkersovereenkomsten

Wanneer u uw gegevensverwerking uitbesteedt aan een verwerker, dient u te controleren of de overeengekomen maatregelen in bestaande contracten met uw verwerkers nog steeds toereikend zijn. De verantwoordelijke kan niet zomaar een verwerker inschakelen, maar moet diens kwaliteit met afdoende garanties controleren. Een verwerker mag ook geen andere verwerker in dienst nemen zonder schriftelijke toestemming van de verantwoordelijke. Persoonsgegevens mogen uitsluitend verwerkt worden op basis van schriftelijke instructies van de verantwoordelijke en op basis van een overeenkomst. De verwerkersovereenkomst dient de elementen als genoemd in onze factsheet verwerkersovereenkomst te bevatten. Wanneer u meer wilt weten over de verwerkersovereenkomst en welke informatie hierin dient te staan, verwijzen wij graag naar onze factsheet verwerkersovereenkomst.

9. One stop shop

Heeft uw organisatie vestigingen in meerdere EU-lidstaten of gegevensverwerkingen in meerdere lidstaten, dan hoeft u maar met één privacy toezichthouder te werken, die van de hoofdvestiging, de leidende toezichthouder genoemd. Deze leidende toezichthouder coördineert het toezicht met de andere toezichthouders in andere staten.

10. Bescherming kinderen

Voor kinderen jonger dan 16 is voor verwerking persoonsgegevens toestemming nodig van de ouderlijke verantwoordelijke. De verantwoordelijke dient redelijke inspanningen te verrichten met inachtneming van beschikbare technologie om deze toestemming te verifiëren.

11. Verboden verwerking van bijzondere categorieën

Verwerking van persoonsgegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze en levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op unieke identificatie van een persoon, of gegevens over gezondheid of gegevens met betrekking tot iemands seksuele gedrag of gerichtheid, zijn verboden. Daar zijn een aantal in de AVG specifiek genoemde uitzonderingen op; bijvoorbeeld in geval van uitdrukkelijke toestemming, als de vitale belangen van betrokkene in het geding zijn en zelf geen toestemming kan worden gegeven, zwaarwegend algemeen belang, bescherming volksgezondheid, wetenschappelijk of historisch onderzoek en dergelijke.

12. Verwerking persoonsgegevens

Persoonsgegevens mogen enkel verwerkt worden als hiervoor een wettelijke grondslag aanwezig is. In totaal zijn er 6 wettelijke grondslagen. De grondslagen zijn, in het kort: Toestemming, Overeenkomst, Wet, Vitaal belang van betrokkene, Taak van algemeen belang/openbaar gezag of een Gerechtvaardigd belang.

13. Beveiliging moet in orde zijn en in control

Beveiliging van persoonsgegevens is essentieel. U dient onder meer gebruik te maken van encryptie en gedegen toegangsbeveiliging, en uw beveiliging steeds te monitoren. Denk aan

controlemiddelen waaronder gebruik van monitoringsoftware. Rekening houdend met de stand van de techniek en onder meer de aard van het soort persoonsgegevens dat verwerkt wordt, dienen passende technische en organisatorische maatregelen getroffen te worden met een, op het risico afgestemd, beveiligingsniveau.

14. Verwerken persoonsgegevens en definitie persoonsgegevens dient ruim opgevat te worden

Alle informatie over een geïdentificeerde of in meest ruime zin identificeerbare natuurlijke persoon. Niet alleen het begrip persoonsgegevens dient u zeer ruim te zien. Denk hierbij bijvoorbeeld aan aan alle mogelijke identificatoren als ip-adressen, bankrekeningen en dergelijke, maar ook het verwerken daarvan omvat iedere denkbare handeling zoals bijvoorbeeld het vernietigen van persoonsgegevens, maar ook het anonimiseren daarvan.

15. Anonimiseren en pseudonimiseren

Persoonsgegevens die volledig geanonimiseerd zijn, zijn geen persoonsgegevens in de zin van de AVG. Pseudonimisering van persoonsgegevens ontdoet deze niet van de status persoonsgegevens, tenzij de betrokkenen in het geheel niet of niet meer identificeerbaar zijn. Aan dat laatste is gezien de stand van de techniek en het bijvoorbeeld aanvullen of verrijken van gegevens niet gemakkelijk te voldoen.

16. Privacy statement

Een privacy statement dient nog transparanter te zijn en in begrijpelijke Jip en Janneke taal aan te geven welke persoonsgegevens met welk doel worden verwerkt. U dient ook te wijzen op het recht van wijziging, verwijdering, inzage, en vergetelheid. Profiling dient eveneens gemeld te worden.

17. Heeft u vragen?

Voor aanvullende informatie en advies over de wet meldplicht datalekken en andere privacy vraagstukken, waaronder het opstellen en beoordelen van afspraken tussen verantwoordelijke en bewerker en draaiboeken voor bewerker en/of verantwoordelijke, kan contact worden opgenomen met Irvette Tempelman van Cordemeyer & Slager / Advocaten, Lawyers for IT
i.m.tempelman@cslaw.nl

LawyersforIT®

Cordemeyer & Slager / Advocaten

Chubb. Insured.℠