Handleiding

Algemene Verordening Gegevensbescherming (AVG)

yspeert advocaten

Colofon

Auteurs

mr. M. Dijkstra en mr. M. Akkerman

Telefoon

+31 (0)512 334 124

E-mail

m.dijkstra@yspeert.nl

m.akkerman@yspeert.nl

INHOUDSOPGAVE

I. De nieuwe privacywetgeving

Vanaf 25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Dit brengt voor zowel bedrijven, overheden als natuurlijke personen die met persoonsgegevens werken een aantal verplichtingen met zich. De Autoriteit Persoonsgegevens (AP) heeft onder de nieuwe wetgeving de bevoegdheid om sancties op te leggen, indien er bepalingen van de AVG worden overtreden. De maximale boete voor bepaalde overtredingen zal 20 miljoen euro of 4% van de totale wereldwijde jaaromzet van een organisatie bedragen.

Voor u ligt een handleiding waarin een aantal tips, adviezen en aandachtspunten worden benoemd, die kunnen worden gebruikt om zo veel mogelijk in overeenstemming te handelen met de nieuwe privacywetgeving. In deze handleiding wordt telkens geredeneerd vanuit de "*onderneming*", maar vanzelfsprekend is dit document op elke entiteit van toepassing die te maken heeft met de AVG.

De AVG is op een aantal onderdelen niet altijd even duidelijk, waardoor niet tot in detail kan worden bepaald wat er van een onderneming wordt verwacht om aan de nieuwe privacywetgeving te voldoen. Deze handleiding bevat dan ook niet een garantie dat uw onderneming AVG-proof zal zijn, maar bevat wel enkele handvatten om kennis te maken met de AVG en zo veel mogelijk daarmee in overeenstemming te gaan handelen. In alle gevallen geldt dat de wettekst van de AVG leidend is. Ook wordt geadviseerd om de website van de Autoriteit Persoonsgegevens te blijven raadplegen. Voordat concreet actie wordt ondernomen naar aanleiding van deze handleiding, wordt geadviseerd om juridische bijstand in te schakelen. Datzelfde geldt vanzelfsprekend ook op het moment dat er vragen zijn over de AVG.

Januari 2018,

Mart Dijkstra
Malou Akkerman

II. Begrippen

De volgende definities zijn onder meer relevant:

"*AVG*"	Algemene Verordening Gegevensbescherming, voluit: Verordening (EU) 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG
"*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, door alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een ander persoon om de natuurlijke persoon direct of indirect te identificeren
"*Betrokkene*"	de natuurlijke persoon op wie de Persoonsgegevens betrekking hebben. Dit kan zijn een consument, een websitebezoeker, etc.
"*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
"*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
"*Verwerker*"	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die / dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt

"*Datalek*"	een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens
"*AP*"	Autoriteit Persoonsgegevens, ook College Bescherming Persoonsgegevens genoemd, de toezichthoudende autoriteit voor de naleving van de geldende privacywetgeving
"*DPIA*"	Data Protection Impact Assessment, gegevensbeschermingseffectbeoordeling
"*Toestemming*"	elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt

III. Tips, adviezen en aandachtspunten

1. Toepasselijkheid AVG en inventarisatie persoonsgegevens

Allereerst is het van belang om na te gaan of de AVG op uw situatie van toepassing is. Beoordeel of u te maken heeft met een *verwerking* van *persoonsgegevens*, of u *verwerkingsverantwoordelijke* en/of *verwerker* bent in een specifieke situatie. De kans is groot dat uw situatie onder het bereik van de AVG valt, indien u op enige manier te maken heeft met persoonsgegevens. Bijvoorbeeld als u persoonsgegevens van uw personeel of uw klanten verwerkt.

Als de AVG van toepassing is, is het raadzaam om alle verwerkingen van persoonsgegevens in uw organisatie in kaart te brengen. Ga dus na welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen, met wie u ze deelt en wie verwerkingsverantwoordelijke is.

Het verwerken van *bijzondere persoonsgegevens* (ras, politieke opvattingen, godsdienstige en andere geloofsovertuigingen, lidmaatschap van vakbonden, seksuele geaardheid of gedrag, of genetische gegevens, biometrische gegevens en gegevens over de gezondheid) is niet toegestaan, tenzij de AVG een uitzondering geeft.

2. Rechtmatige verwerking persoonsgegevens

Persoonsgegevens dienen rechtmatig te worden verwerkt. Zo moet er sprake zijn van een wettelijke basis, die de verwerking van persoonsgegevens rechtvaardigt. De persoonsgegevens moeten bovendien juist zijn en op behoorlijke wijze worden verwerkt. De AVG geeft verschillende grondslagen voor de verwerking van persoonsgegevens.

Persoonsgegevens mogen bijvoorbeeld rechtmatig worden verwerkt als een onderneming daarvoor *toestemming* heeft verkregen van de betrokkene. Het moet voor de betrokkene duidelijk zijn waar toestemming voor wordt gevraagd. De toestemming mag daarom niet te vaag of algemeen geformuleerd worden en moet specifiek en ondubbelzinnig blijken uit een verklaring of een actieve handeling, zoals het actief aanklikken van een 'vinkje' op een website. Indien de betrokkene een kind is, gelden andere vereisten voor toestemming. Onder de AVG moet de onderneming daarnaast kunnen *aantonen* dat zij toestemming heeft verkregen.

Het kan ook zijn dat het noodzakelijk is voor de onderneming om persoonsgegevens van de betrokkene te verwerken voor het uitvoeren van de *overeenkomst* met de betrokkene. De overeenkomst biedt dan de grondslag voor de verwerking van persoonsgegevens. Denk bijvoorbeeld aan de situatie dat het hebben van de adresgegevens (persoonsgegevens) van de betrokkene nodig is om een online bestelling bij de betrokkene te laten bezorgen.

Er bestaan ook andere wettelijke grondslagen voor het verwerken van persoonsgegevens. Deze zijn vermeld in de AVG. De onderneming dient in alle gevallen na te gaan of er een wettelijke basis aanwezig is.

3. Doeleinden van verwerking van persoonsgegevens

Zorg dat gegevens rechtmatig worden verwerkt en verwerk alleen persoonsgegevens die *noodzakelijk* zijn voor het specifieke *doel* dat dient te worden bereikt. Bepaal dus voor welke doeleinden de persoonsgegevens worden verwerkt. Deze doeleinden dienen in een *privacyverklaring* te worden vermeld, zodat de betrokkenen weten wat er met hun persoonsgegevens wordt gedaan. U kunt de privacyverklaring bijvoorbeeld op uw website plaatsen.

Zorg ervoor dat bij het verzamelen en verwerken van persoonsgegevens niet meer gegevens worden gebruikt dan nodig is om het doel, waarvoor ze gebruikt zullen worden, te bereiken. Zorg dus voor dataminimalisatie.

4. Verwerkingenregister

Houd een register bij waarin alle persoonsgegevens worden verwerkt. Documenteer welke persoonsgegevens worden verwerkt, met welk doel, waar ze vandaan komen en met wie ze worden gedeeld. In een bepaald aantal gevallen is het verplicht om een verwerkingenregister te hebben. De AVG bevat een uitgebreide regeling over het verwerkingenregister.

5. Verwerkersovereenkomst

Als u verwerkingsverantwoordelijke bent ten aanzien van de verwerking van persoonsgegevens en u laat deze *verwerken* door een derde partij (een *verwerker*), dan dient u daar afspraken over te maken in de vorm van een schriftelijke *verwerkersovereenkomst*. De verwerkersovereenkomst bevat de afspraken over de persoonsgegevens en de manier waarop daarmee moet worden omgegaan door de verwerker.

Inventariseer dus of u *verwerkingsverantwoordelijke* bent en wie persoonsgegevens van u als *verwerker* verwerken. Als u verwerkingsverantwoordelijke bent, sluit dan vervolgens verwerkersovereenkomsten met verwerkers. Mocht u al verwerkersovereenkomsten hebben, zorg er dan voor dat deze in overeenstemming zijn met de AVG.

6. Informatieverplichting

Ondernemingen die persoonsgegevens verzamelen van betrokkenen, moeten hierover transparant en in eenvoudige taal communiceren met de betrokkene. Er moet duidelijkheid worden gegeven over het feit dat de gegevens van de betrokkene worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Vermeld bijvoorbeeld in de *privacyverklaring* de volgende gegevens:

- de identiteit, de contactgegevens en die van de eventuele Functionaris voor de Gegevensbescherming (FG) van de onderneming
- de doeleinden waarvoor de gegevens worden verwerkt en de grondslag voor die verwerking
- de (soorten) ontvangers aan wie de gegevens worden verstrekt
- eventuele doorgiften naar niet-EU-landen en de daarbij geboden waarborgen
- de rechten die betrokkenen hebben (bijvoorbeeld inzage, correctie, bezwaar, etc.)
- welke passende technische en organisatorische maatregelen er zijn genomen om persoonsgegevens te beveiligen

- in geval van profilering: de essentie van de onderliggende logica en de eventuele gevolgen van de verwerking voor de betrokkene
- als de website gebruik maakt van cookies, geef dan aan wat dit inhoudt en wat er met informatie wordt gedaan
- eventuele bewaartermijnen van de persoonsgegevens

7. Bewaartermijnen

Persoonsgegevens mogen niet langer worden bewaard dan *noodzakelijk* is voor het doel waarvoor ze zijn verzameld. Als onderneming moet je goed kunnen aangeven gedurende welke periode de gegevens van een betrokkene worden bewaard. Zorg er dus voor dat per verwerking duidelijk is hoe lang deze gegevens (afhankelijk van het doel waarvoor ze zijn verzameld) mogen worden bewaard.

8. Recht van bezwaar van betrokkene

De betrokkene die zijn persoonsgegevens deelt, kan op elk moment bezwaar maken tegen de verwerking van deze gegevens. Het gaat hier om het *recht van bezwaar*. Ondernemingen moeten de betrokkene informeren over het feit dat de betrokkene bezwaar kan maken tegen het verdere gebruik van zijn gegevens voor bijvoorbeeld marketingdoeleinden. Ondernemingen moeten gehoor geven aan een dergelijk bewaar, tenzij er gerechtvaardigde gronden zijn om de persoonsgegevens te blijven verwerken die zwaarder wegen dan die van de betrokkene.

9. Recht op dataportabiliteit van betrokkene

Ondernemingen moeten de door haar verzamelde persoonsgegevens van de betrokkene op verzoek van de betrokkene overdragen. Het gaat hier om het *recht op dataportabiliteit*. Voor ondernemingen betekent dit bijvoorbeeld dat een betrokkene kan verzoeken om zijn persoonsgegevens over te laten dragen aan hemzelf of aan een andere partij. Als de betrokkene de gegevens zelf wil ontvangen, moet dit binnen een maand gebeuren op een manier waarop de gegevens voor hem gemakkelijk toegankelijk zijn.

Als de betrokkene verzoekt om zijn gegevens over te dragen aan een andere partij, dan moeten deze ook binnen een maand in een gangbaar elektronisch formaat naar een ander informatiesysteem worden verstuurd. In sommige gevallen mag de onderneming de termijn verlengen tot drie maanden, zolang de betrokkene of derde partij hiervan op de hoogte wordt gebracht.

10. Recht om vergeten te worden van betrokkene

Het recht om vergeten te worden houdt in dat, als een betrokkene hierom vraagt, een onderneming in een beperkt aantal gevallen de persoonsgegevens van de betrokkene moet verwijderen. Het gaat hier om het *recht op vergetelheid*. Hierbij heeft de onderneming soms ook de plicht om derde partijen ervan op de hoogte te stellen dat een betrokkene wenst dat diens gegevens verwijderd worden. De betrokkene heeft het recht op verwijdering van zijn gegevens als er geen geldige reden meer is om zijn gegevens nog langer te bewaren / te verwerken of als de gegevens onrechtmatig zijn verwerkt. De AVG bevat een uitgebreide bepaling over dit recht van de betrokkene.

11. Andere rechten van betrokkene

Betrokkenen hebben naast de eerder genoemde rechten ook andere rechten, te weten:

- recht op inzage in persoonsgegevens
- het recht om informatie te ontvangen over de wijze waarop hun persoonsgegevens worden verwerkt
- recht om een kopie te ontvangen van hun persoonsgegevens
- recht op correctie van of aanvulling op de persoonsgegevens
- recht op beperking van de verwerking van persoonsgegevens
- recht op bezwaar tegen profilering
- recht om een klacht in te dienen bij de AP over de verwerking van hun persoonsgegevens

Zorg ervoor dat het duidelijk is met wie de betrokkene binnen de onderneming contact kan opnemen als er vragen zijn of als de betrokkene gebruik wil maken van zijn wettelijke rechten.

De aanwezigheid van een verwerkingenregister kan zinvol zijn, ook als een onderneming op grond van de AVG niet verplicht is om een verwerkingenregister te hebben. Immers, als een betrokkene gebruik maakt van zijn wettelijke rechten, kan een onderneming met een verwerkingenregister daar eenvoudig op inspelen en daar vervolgens naar handelen.

12. Profilering

Er is sprake van *profilering* als een onderneming op basis van verkregen persoonsgegevens automatisch een profiel van de betrokkene opstelt via de verzameling, analyse en koppeling van persoonsgegevens. De gegevens worden gecombineerd om de betrokkene zo in te kunnen delen in een bepaalde categorie of groep, zodat hij op deze manier benaderd of beoordeeld kan worden. Deze categorieën/individuele profielen worden bijvoorbeeld gebruikt voor *direct marketing* en om gericht advertenties aan de betrokkene te laten zien.

Onder de AVG is elke vorm van *geautomatiseerde* verwerking van persoonsgegevens (waaronder profilering) niet toegestaan als daar voor de betrokkene rechtsgevolgen aan zijn verbonden of het hem in aanmerkelijke mate treft. In de AVG is nog niet een heldere definitie opgenomen. Er is al wel een aantal uitzonderingen op deze hoofdregel opgenomen in de AVG.

Wanneer een onderneming profilering toepast, moeten er bepaalde zekerheden voor de betrokkene worden ingebouwd. De betrokkene dient van specifieke informatie te worden voorzien, zoals waarom bepaalde beslissingen op basis van zijn profiel worden genomen. Daarnaast heeft de betrokkene bij geautomatiseerd genomen beslissingen altijd het recht om: zijn standpunt kenbaar te kunnen maken, uitleg te krijgen over het genomen besluit, dit besluit aan te kunnen vechten.

13. Data Protection Impact Assessment (DPIA)

Een Data Protection Impact Assessment ("*DPIA*") moet worden uitgevoerd door een onderneming als:

- het gaat om systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder *profilering*, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen
- het gaat om verwerken van *bijzondere persoonsgegevens* op grote schaal
- het gaat om stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten
- overige gevallen die een hoog risico voor de betrokkene met zich meebrengen

Aan de hand van een DPIA wordt het effect van de verwerking van de persoonsgegevens vooraf beoordeeld.

Een DPIA geeft ondernemingen inzicht in hoe groot de kans is dat de privacy van de betrokkenen wordt geschaad, waar deze risico's zich bevinden en welke gevolgen daaraan zijn verbonden. Op basis van de uitkomsten van de DPIA kan men gericht acties ondernemen om deze risico's te verminderen. Onder omstandigheden is een onderneming verplicht om een DPIA uit te voeren. We verwijzen naar de website van de AP en bijvoorbeeld naar de website van de beroepsorganisatie van IT-auditors (NOREA).

Als uit een DPIA naar voren komt dat een beoogde verwerking een hoog risico met zich meebrengt en het niet lukt om het risico te verkleinen, dan dient de onderneming met de AP te overleggen voordat de gegevensverwerking plaatsvindt. De AP beoordeelt dan of de gegevensverwerking in strijd is met de AVG. Dit heet een *voorafgaande raadpleging*.

14. Privacy by design en Privacy by default

Privacy by design houdt in dat een onderneming er al bij het ontwikkelen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. In de voorfase wordt dus al rekening gehouden met privacy. Er dienen niet meer gegevens te worden verzameld dan noodzakelijk voor het doel van de verwerking. Op voorhand wordt onderzocht op welke manier de privacyregels feitelijk en technisch kunnen worden toegepast en welke maatregelen kunnen worden genomen om de rechten van de betrokkene te beschermen (bijvoorbeeld dataminimalisatie).

Privacy by default betekent dat er technische en organisatorische maatregelen dienen te worden genomen om te zorgen dat alleen persoonsgegevens worden gebruikt die noodzakelijk zijn voor de doeleinden waarvoor ze worden verzameld. Een onderneming dient bijvoorbeeld haar website zo privacyvriendelijk mogelijk in te richten.

Een onderneming dient passende technische en organisatorische beschermingsmaatregelen te nemen om in overeenstemming te handelen met de AVG. Hieronder is een aantal voorbeelden opgenomen.

Technische maatregelen

1. <u>Dataminimalisatie</u>
   Zorg dat er zo weinig mogelijk persoonsgegevens worden verwerkt. Bedenk altijd of en welke gegevens er nodig zijn om het doel te bereiken.

2. Verschillende databases
   Zorg voor verschillende databases/opslaglocaties wanneer er veel verschillende soorten persoonsgegevens van een persoon worden verzameld. Mocht er een datalek in het systeem zijn, dan wordt op die manier gewaarborgd dat er niet complete profielen van een persoon op straat komen te liggen, maar losse gegevens die afzonderlijk van elkaar weinig betekenen.

3. Gericht doel bepalen
   Verzamel alleen de gegevens die nodig zijn/relevant zijn voor het doel dat met de gegevens moet worden bereikt.

4. Bescherm en beveilig de gegevens die worden verwerkt
   Zorg voor passende en actuele technische beschermingsmaatregelen, zoals: virusscanners, pseudonimiseren, versleutelen, anonimiseren etc. om datalekken, of de gevolgen daarvan, te beperken. Test, beoordeel en evalueer de doeltreffendheid van de beveiligingsmaatregelen.

Organisatorische maatregelen

1. Duidelijke informatie
   Informeer de betrokkene over het feit dat hun persoonsgegevens worden verwerkt. Doe dat in heldere en eenvoudige bewoordingen en zorg ervoor dat de informatie eenvoudig te vinden is.

2. Geef controle aan de betrokkene
   Zorg dat degene van wie de gegevens worden verwerkt de mogelijkheid heeft om (waar nodig) toestemming te geven. Ook moet de betrokkene de verzamelde gegevens kunnen corrigeren of laten verwijderen en andere rechten kunnen uitoefenen.

3. Maak een privacybeleid
   Stel een privacybeleid op en handel naar dit beleid. Zorg ook dat alle medewerkers op de hoogte zijn van dit privacy beleid.

4. Toon aan dat de persoonsgegevens op een privacyvriendelijke manier worden verwerkt
   Er geldt een verantwoordingsplicht. Maak het controleerbaar en aantoonbaar dat er in overeenstemming wordt gehandeld met de privacywetgeving.

15. Meldplicht datalekken en bijhouden register

Een *datalek* is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Datalekken moeten binnen 72 uur na ontdekking worden gemeld bij de AP en onder omstandigheden ook aan de betrokkenen. Schakel altijd juridische bijstand in op het moment van een (vermoeden van een) datalek.

Een datalek kan zowel per ongeluk als opzettelijk ontstaan. Per ongeluk: bijvoorbeeld als een onderneming een e-mail met klantgegevens stuurt naar

de verkeerde afzender. Met opzet: bijvoorbeeld als de onderneming wordt aangevallen door virussen van buitenaf en er klantgegevens worden buitgemaakt door hackers.

Er dient een register te worden bijhouden met daarin vermeld alle datalekken van de onderneming. In dit register moet bijgehouden worden wanneer het datalek plaatsvond, wie de betrokkenen zijn, wat de gevolgen van het datalek zijn en welke maatregelen de onderneming naar aanleiding van het datalek heeft genomen.

16. Vestigingen in EU-lidstaten en data buiten Europa

Als u vestigingen in andere lidstaten van de EU heeft, dan dient u na te gaan met welke toezichthouder (AP of andere toezichthouder) u te maken heeft. Uitgangspunt is dat u met één toezichthouder te maken heeft.

Verder dient u na te gaan of u persoonsgegevens *buiten* Europa exporteert en of dit is toegestaan. In dat geval gelden namelijk aanvullende vereisten uit de AVG.

17. Verplicht medewerkers tot geheimhouding

Leg medewerkers die betrokken zijn bij de verwerking van persoonsgegevens een schriftelijke plicht tot geheimhouding op, zowel binnen als buiten de organisatie. Zo wordt gewaarborgd dat er vertrouwelijk wordt omgegaan met persoonsgegevens.

18. Hoge boetes en toezicht AP

In Nederland houdt de AP toezicht op de naleving van de AVG. De AP heeft vergaande bevoegdheden om haar doelen te verwezenlijken. Zo mag de AP onder omstandigheden een woning of een bedrijf doorzoeken. De AP mag zichzelf ook toegang verschaffen tot bijvoorbeeld USB-sticks, computers, laptops, etc.

De AP heeft in geval van overtreding van de AVG de bevoegdheid om boetes en maatregelen op te leggen. De boetemaxima zijn 20 miljoen euro of 4% van de wereldwijde jaaromzet van een organisatie per overtreding, afhankelijk van het soort overtreding.

19. Functionaris voor de Gegevensbescherming

Het aanstellen van een Functionaris voor de Gegevensbescherming ("*FG*") of Data Privacy Officer ("*DPO*") is voor een onderneming verplicht als:

- de verwerking wordt verricht door een overheidsinstantie en overheidsorgaan
- de verwerkingsverantwoordelijke of verwerker hoofdzakelijk is belast met grootschalige verwerking van *bijzondere persoonsgegevens*
- de verwerkingsverantwoordelijke of verwerker hoofdzakelijk belast is met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokken personen vereisen

De FG houdt zich binnen de onderneming bezig met privacyrechtelijke vraagstukken. Een medewerker binnen de onderneming kan worden aangewezen als FG, maar er kan ook een externe FG worden aangesteld. Een

FG van buiten de onderneming kan vanuit financieel oogpunt zinvol zijn voor de kleinere ondernemingen. Zij kunnen dan een overeenkomst sluiten met deze externe FG.

Een concern mag volstaan met één FG, mits eenvoudig contact gelegd kan worden met deze FG vanuit de verschillende vestigingen binnen het concern. De AP heeft richtlijnen opgesteld die specifiek betrekking hebben op de FG. Hoewel het niet in alle gevallen verplicht is om een FG aan te stellen, kan het onder omstandigheden raadzaam zijn om een FG aan te stellen.

20. Bewustwording en Privacy beleid

Breng uw medewerkers op de hoogte van de AVG en de gevolgen daarvan door middel van trainingen en/of voorlichtingen. Stel interne protocollen op voor uw organisatie, waardoor wordt gewaarborgd dat de AVG wordt nageleefd. Denk bijvoorbeeld aan een *protocol meldplicht datalekken*, zodat u precies weet wat u moet doen op het moment dat er sprake is van een datalek. Omschrijf bijvoorbeeld ook op welke manier u de verzamelde persoonsgegevens beveiligt.

21. Lees de AVG

Lees de AVG om na te gaan wat deze wetgeving voor u betekent.

IV. Wat yspeert advocaten voor u kan betekenen

Wij realiseren ons dat het doorlezen van deze materie over de AVG veel vragen oproept. Wat staat mij nu te doen? Waar moet ik beginnen?

yspeert advocaten kan u verder helpen. Zo kunnen wij voor u:

- een verwerkersovereenkomst opstellen
- uw bestaande verwerkersovereenkomsten beoordelen en aanpassen
- een privacyverklaring opstellen
- een intern beleid voor uw onderneming opstellen voor het intern en extern melden van datalekken
- u bijstaan als u wordt geconfronteerd met een datalek
- u bijstaan als een betrokkene zijn privacyrechten uitoefent en/of een procedure tegen u start
- u bijstaan als u wordt geconfronteerd met een maatregel of boete van de AP en/of de AP een procedure tegen u start
- een lezing geven over de AVG
- specifieke vragen over de AVG in relatie tot uw organisatie beantwoorden

U staat er niet alleen voor. Neem dus gerust contact met ons op voor advies.

Namens yspeert advocaten,

Mart Dijkstra en Malou Akkerman


yspeert
advocaten