Hoe maakt u uw bedrijf AVG-compliant?

Horlings Accountants & Belastingadviseurs B.V.
Koningin Wilhelminaplein 30
1062 KR Amsterdam

Postbus 53045
1007 RA Amsterdam

T: +31 (0)20 5700 200
info@horlings.nl | horlings.nl

Inleiding

De nieuwe en strengere Europese privacywet, de Algemene verordening gegevensbescherming (AVG), is per 25 mei ingetreden. Deze wet vervangt de Wet bescherming persoonsgegevens (Wbp). De AVG verplicht bedrijven om precies te documenteren welke persoonsgegevens van wie ze in bezit hebben, hoelang ze die bewaren en wat ze ermee doen.
Veel ondernemers zijn nog bezig om hun bedrijf AVG-compliant te maken. U wellicht ook. De toezichthouder Autoriteit Persoonsgegevens zal waarschijnlijk niet zo snel bij u op de stoep staan, maar desondanks is het wel zaak zo snel mogelijk te voldoen aan de wet.

Deze nieuwsbrief informeert en ondersteunt u over de te nemen stappen. Lees de volgende vier artikelen die als handvat dienen voor de te nemen maatregelen:

Wij wensen u veel leesplezier en zijn uiteraard altijd bereid tot het geven van een nadere toelichting.

Anne-Marie Dijkhorst en Inez Janse

Horlings Accountants & Belastingadviseurs B.V.

September 2018

1 Hoe lang mag u persoonsgegevens bewaren?

Hoe lang mag u bij een vacature bijvoorbeeld de sollicitatiegegevens van kandidaten bewaren? Wat zijn de regels rond het bewaren van camerabeelden en de gegevens over het internetgebruik van uw medewerkers? Hoe lang bent u verplicht bepaalde gegevens, zoals facturen en dergelijke, minimaal op te slaan?

Volgens de AVG, dat was ook al zo onder de Wet bescherming persoonsgegevens (Wbp), mag u persoonsgegevens niet langer bewaren dan nodig voor het doel waarvoor u ze heeft verzameld. Daarna moet u de persoonsgegevens ook daadwerkelijk vernietigen.

Wat zijn persoonsgegevens?

Het gaat in het kader van de AVG altijd over persoonsgegevens. Persoonsgegevens zijn gegevens die, alleen of in combinatie met andere gegevens, terug te herleiden zijn naar een natuurlijk persoon. Voorbeelden van persoonsgegevens zijn onder andere naam, adres, woonplaats, kentekennummer, personeelsnummer, mailadres en videobeelden.

Concrete termijnen

In de AVG zijn echter geen concrete termijnen opgenomen voor het bewaren van persoonsgegevens. In sommige gevallen schiet andere wetgeving u te hulp waarin specifieke bewaartermijnen zijn opgenomen. Dit kunnen maximale bewaartermijnen zijn, daarna dient u de gegevens te vernietigen, of minimale bewaartermijnen, waarbij u zelf een passende termijn moet bepalen voor het eventueel langer bewaren. Is er geen wetgeving, dan dient u zelf – beargumenteerd – bewaartermijnen te bepalen.

Vereisten bewaren persoonsgegevens

U dient voor het bewaren van persoonsgegevens aan de volgende vereisten te voldoen:

- u dient vooraf vast te stellen hoelang bepaalde documenten met persoonsgegevens bewaard gaan worden,
- de bewaartermijnen moeten opgenomen worden in een zogenaamd verwerkingsregister.
- de personen van wie u gegevens verwerkt dienen geïnformeerd te worden over deze bewaartermijnen,
- de bepaalde bewaar- en vernietigingstermijn dienen zo mogelijk te worden vertaald naar passende technische en organisatorische maatregelen,
- na het verstrijken van de bewaartermijn dienen de persoonsgegevens daadwerkelijk vernietigd of geanonimiseerd te worden.

Salaris, factuur en verzuim

Er zijn binnen uw organisatie diverse processen en activiteiten waarin verschillende categorieën van persoonsgegevens nodig zijn, waarvan de verwerkingsdoelen per proces verschillen en waarvoor ook andere bewaartermijnen kunnen gelden. Denk aan salarisafspraken, facturen en verzuimbeheer. Hieronder hebben we enkele processen in een tabel gezet die meestal voorkomen in organisaties, met daarbij opgenomen wat de bewaartermijnen zijn en op welke wetgeving dit gebaseerd is. De bewaartermijn gaat lopen na bijvoorbeeld het einde van een dienstverband, het einde van een boekjaar of het doen van een registratie. Overigens kan het soms zo zijn dat de genoemde termijn wordt overruled door een andere wettelijke bewaarplicht (meestal is dit dan fiscale wetgeving).

processen	Maximale bewaartermijn	grondslag
Sollicitatieprocedure	4 weken	Vrijstellingsbesluit Wbp
Indiensttreding arbeidsovereenkomst	2 jaar	Wet op de Rijksbelastingen
Verzuimbeheer	2 jaar	Vrijstellingsbesluit Wbp
Beveiligingscamera's	4 weken	Vrijstellingsbesluit Wbp
Bezoekersregistratie	6 maanden	Vrijstellingsbesluit Wbp
Logging internetgebruik, netwerk	6 maanden	Vrijstellingsbesluit Wbp
Gerechtelijke procedures	2 jaar	Vrijstellingsbesluit Wbp
Klantcontactmanagement	n.t.b.	Zelf vaststellen

processen	Minimale bewaartermijn	grondslag
Salarisafspraken	7 jaar	Wet op de Rijksbelastingen
Loonbelasting en identiteitsbewijzen	5 jaar	Uitvoeringsregeling LB
Debiteuren- en crediteurenadministratie	7 jaar	Wet op de Rijksbelastingen

Tip:
Bepaal als organisatie zelf – beargumenteerd – bewaartermijnen voor de processen waarin dit niet wettelijk is bepaald.

Vernietiging persoonsgegevens

Is de bewaartermijn van persoonsgegevens verstreken of zijn de gegevens niet meer noodzakelijk voor het doel? Dan moeten de gegevens vernietigd worden. Denk bijvoorbeeld aan gegevens over loonbeslag als het loonbeslag is opgeheven. Vernietiging moet gebeuren onder controle van uw bedrijf. Vernietigen houdt in dat de gegevens niet langer meer bestaan of niet langer meer bestaan in een bruikbare vorm. De AVG stelt geen extra vereisten aan het vernietigen van persoonsgegevens.

Tip:
Verwerkt Horlings gegevens voor u, bijvoorbeeld de salarisadministratie? Dan maken we graag goede afspraken over de bewaartermijnen van persoonsgegevens.

2 Hoe maakt u een register van verwerkingen?

De belangrijkste nieuwe eis in de strengere privacywet AVG is de verantwoordingsplicht. Dit houdt in dat u bepaalde zaken moet hebben ingericht om de naleving van de AVG aan te kunnen tonen.

Dit geldt onder andere voor het opstellen van een zogenaamd verwerkingsregister. Hiermee verkrijgt u inzicht in welke persoonsgegevens u verwerkt binnen uw organisatie.

Wat is een verwerkingsregister?

Het verwerkingsregister is een registratie van de persoonsgegevens die binnen uw organisatie worden verwerkt. Afhankelijk of u verwerker of verwerkingsverantwoordelijke bent, dient u minimaal bepaalde informatie vast te leggen.

Een verwerkingsverantwoordelijke is een organisatie die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Een verwerker is een organisatie die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Voor bijna elk mkb-bedrijf verplicht

Heeft uw bedrijf meer dan 250 werknemers? Dan bent u verplicht een register van verwerkingen bij te houden. Heeft een bedrijf minder dan 250 werknemers in dienst, dan moet het ook over een verwerkingsregister beschikken, wanneer:

- de verwerking niet incidenteel is,
- het waarschijnlijk is dat de verwerking die het bedrijf verricht een risico inhoudt voor de rechten en vrijheden van de betrokkene(n),
- de verwerking bijzondere categorieën van gegevens of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten bevatten.

Let op!
Aangezien veruit de meeste verwerkingen niet incidenteel zijn, denk aan het verwerken van persoonsgegevens van medewerkers of klanten, zullen de meeste mkb-bedrijven vrijwel altijd een verwerkingsregister op moet stellen.

Vereisten verwerkingsregister

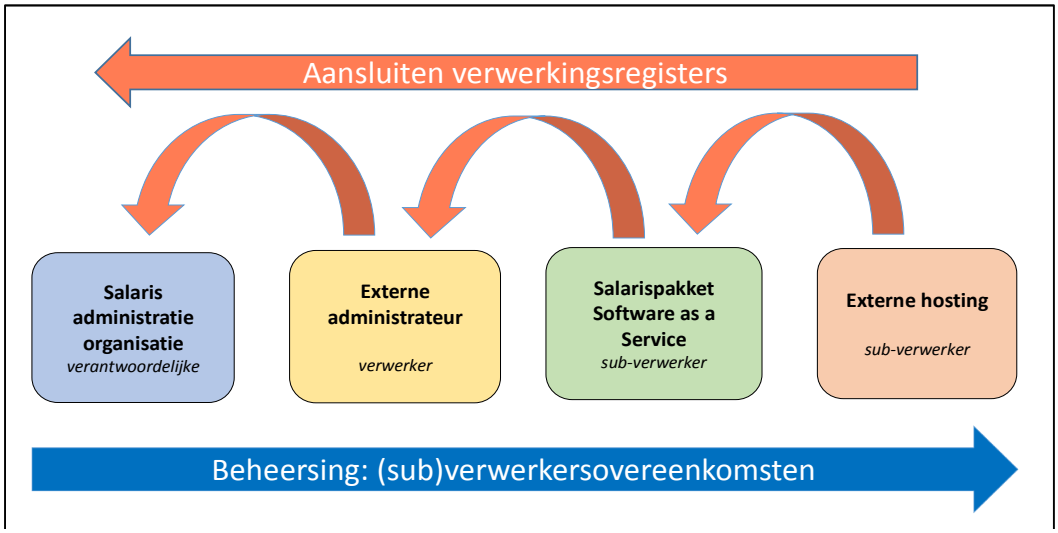
Het register van de verwerkingsverantwoordelijke moet de volgende gegevens bevatten:

- de verwerkingsdoelen en de grondslagen voor verwerking,
- een beschrijving van de categorieën van betrokkenen,
- een beschrijving van de categorieën van persoonsgegevens,
- de verwerkers die diensten voor u verlenen en beschikking hebben over uw persoonsgegevens,
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt,
- indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie,
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist,
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen,
- in voorkomend geval de naam van de functionaris voor gegevensbescherming.

Het register van de verwerker moet de volgende gegevens bevatten:

- de naam en de contactgegevens van de verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt,
- de categorieën van verwerkingen die voor rekening van iedere verwerkingsverantwoordelijke zijn uitgevoerd,
- indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie,
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen,
- in voorkomend geval de naam van de functionaris voor gegevensbescherming.

In het geval een verantwoordelijke persoonsgegevens laat verwerken door een verwerker (denk bijvoorbeeld aan de uitbestede salarisadministratie van uw organisatie), dan dienen de verwerkingsregisters van verantwoordelijke en verwerker op elkaar aan te sluiten. In het geval de verwerker op zijn beurt ook weer bepaalde verwerkingen uitbesteedt (denk aan een SAAS-dienstverlener of een hostingpartij), dan dient de subverwerker ook een verwerkingsregister te hebben. Zie onderstaande afbeelding van een verwerkingsketen.



Voorbeeld register van verwerkingen

In onderstaande afbeelding is te zien op welke wijze u dit register kunt opzetten in een eenvoudige tabel of spreadsheet. Bovenaan de kolommen staan de categorieën van gegevens vermeld die u per proces dient te registeren. Ook maakt u hiermee inzichtelijk welke partijen (verwerkers) beschikken over uw persoonsgegevens en welke maatregelen u heeft getroffen om deze te beschermen.

Proces	Persoons-gegevens	Betrokkenen	Ontvangers	(Sub)ver-werkers	Verwerkings-doel	Grondslag	Bewaar-termijn	Maat-regelen
HR								
Inkoop								
Verkoop								
Webshop								
Netwerk								
Administratie								

Welke acties moet u in gang zetten?

Het verwerkingsregister geeft u inzicht in wat u heeft geregeld met betrekking tot de verwerking van persoonsgegevens. Met behulp van het ingevulde register kunt u bepalen in welk proces of voor welke activiteit u zaken nog niet heeft ingeregeld, welke risico's u mogelijk loopt en of de maatregelen die u heeft getroffen afdoende zijn. U kunt dit ook periodiek evalueren.

Mogelijke acties op basis van het verwerkingsregister:

controleren van de gemaakte afspraken met verwerkers en mogelijk aanvullen van de verwerkersovereenkomsten,
vaststellen (privacy)beleid op specifieke onderwerpen,
aanvullen van verwerkingsdoelen en grondslagen van de gegevensverwerking,
vaststellen bewaartermijnen en inregelen vernietiging persoonsgegevens na het verstrijken van de bewaartermijnen,
controleren of de technische en organisatorische maatregelen zowel in uw eigen organisatie als bij uw verwerkers afdoende zijn,
gebruiken van de informatie uit het verwerkingsregister om de betrokkene(n) te informeren.

Tip:
Wij kunnen u helpen om AVG-proof te worden als het gaat om de verwerkersovereenkomst die u met ons dient af te sluiten. Wij hebben een modelovereenkomst voor u klaarliggen. Belt u ons erover!

3 Hoe beveiligt u deze persoonsgegevens?

U moet persoonsgegevens op een juiste en doeltreffende manier beveiligen, zo schrijft de AVG voor. Op welke wijze geeft u daar invulling aan? Zijn er zaken die minimaal geregeld moeten worden? Hoe gaat u met deze verplichting om richting uw leveranciers en serviceproviders?

Uw onderneming is volgens de AVG verantwoordelijk voor het nemen van passende technische én organisatorische maatregelen om een adequaat beveiligingsniveau te waarborgen voor de verwerking van persoonsgegevens.

Persoonsgegevens goed beveiligen

Hoe moet u volgens de AVG die persoonsgegevens dan goed beveiligen? Hiervoor moet u met de volgende zaken rekening houden:

- de stand van de techniek – de huidige technische stand van de techniek is wat betreft technische maatregelen bepalend voor wat er minimaal van u verwacht wordt,
- de aard, de omvang en doeleinden van de verwerkingen – de categorieën van persoonsgegevens in samenhang met de hoeveelheid persoonsgegevens en de verwerkingsdoelen zijn medebepalend voor de te nemen maatregelen,
- de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de personen – feitelijk dient u een risico-inschatting te maken van uw verwerkingen en op basis hiervan uw maatregelen te treffen,
- verwerkers – u kunt alleen een beroep doen op verwerkers die afdoende garanties met betrekking tot het toepassen van technische en organisatorische maatregelen bieden; deze maatregelen moeten worden opgenomen in een verwerkersovereenkomst en u bent bovendien gerechtigd te (laten) controleren bij uw verwerker(s) of de maatregelen adequaat zijn,
- de uitvoeringskosten – de AVG biedt tevens ruimte om een kostenafweging te maken. Indien de risico's beperkt zijn, wordt niet van u verwacht dat u grote investeringen doet om een hoog beschermingsniveau te bereiken,
- beleid – als u van mening bent dat u, gezien voorgaande zaken hoge risico's loopt bij de verwerking van persoonsgegevens, dan dient u een passend gegevensbeschermingsbeleid uit te voeren. Dat houdt in dat u op basis van een risico-inschatting de beschermingsmaatregelen bepaalt. Voor de meeste mkb-ondernemingen zal een gegevensbeschermingsbeleid niet nodig zijn.

Maatregelen

Vervolgens geeft de AVG enkele voorbeelden van mogelijke maatregelen, namelijk:

- pseudonimiseren en versleuteling van persoonsgegevens,
- op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de systemen en diensten garanderen,
- het tijdig herstellen van toegang en beschikbaarheid bij een incident, zoals een datalek,
- een evaluatieprocedure om doeltreffendheid van de maatregelen te testen en te beoordelen.

Pseudonimiseren van persoonsgegevens

Persoonsgegevens kunnen in het geval van pseudonimiseren niet meer aan een specifieke betrokkene worden gekoppeld zonder dat er aanvullende gegevens nodig zijn (een zogenaamde sleutel om informatie te decoderen). Omdat het via het gebruik van een sleutel nog steeds mogelijk is om de betreffende persoon (indirect) te identificeren, kwalificeren pseudoniemen nog steeds als persoonsgegevens. Dit in tegenstelling tot het anonimiseren van persoonsgegevens.

Andere maatregelen

Andere maatregelen die u sowieso moet treffen, zijn:

- wachtwoordbeleid en rechten- en autorisatiestructuur inrichten,
- logging en controle (monitoring) van toegang tot de informatiesystemen,
- implementatie van actuele beveiligingsupdates,
- viruscontrole en firewall inregelen,
- monitoring kwetsbaarheden op het interne en externe netwerk,
- adequate fysieke beschermingsmaatregelen treffen,
- procedures opstellen voor opslag, onderhoud en vernietiging van data,
- procedures opstellen voor het behandelen van informatiebeveiligingsincidenten en datalekken,
- back-upbeleid opzetten en uitvoeren adequate back-ups.

Gedragscode of certificering

Door als onderneming aan te sluiten bij een gedragscode voor de verwerking van persoonsgegevens (bijvoorbeeld binnen uw branche) of een specifieke certificering, kunt u aantonen dat u aan de vereisten voor technische en organisatorische maatregelen die de AVG stelt, voldoet. Een voorbeeld van een algemeen geaccepteerde standaard voor informatiebeveiliging is ISO27001.

Tip:
Indien u gebruik wilt maken van bepaalde certificeringen om wat betreft technische en organisatorische maatregelen te voldoen aan de verplichtingen uit de AVG, maak dan keuzes. Want het kan zijn dat uw onderneming niet alle onderdelen van die certificeringen nodig heeft!

4 Toch een datalek! Wat nu?

De AVG schrijft voor dat uw organisatie bepaalde inbreuken in verband met de verwerking van persoonsgegevens, zogenaamde datalekken, moet melden bij de Autoriteit Persoonsgegevens (AP). Wat betekent dit voor uw bedrijf? Waaraan moet u precies voldoen?

In sommige situaties dient u ook de betrokkene(n) bij het datalek te informeren. Deze verplichting is niet nieuw in de AVG en was ook al voorgeschreven in de Wet bescherming persoonsgegevens (Wpb).

Wat is een datalek?

Een datalek wordt in de AVG (artikel 4) omschreven als 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.

Er is alleen sprake van een datalek als zich een beveiligingsincident heeft voorgedaan én indien persoonsgegevens verloren zijn gegaan dan wel onrechtmatige verwerking van de persoonsgegevens redelijkerwijs niet uit te sluiten is.

Datalek snel melden

Indien een datalek heeft plaatsgevonden, meldt u deze zonder onredelijke vertraging, maar wel uiterlijk 72 uur nadat u er kennis van heeft genomen. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, moet u motiveren waardoor de vertraging is opgetreden. Een (sub)verwerker, zoals een leverancier, moet u, omdat u verantwoordelijke bent, onverwijld informeren zodra hij kennis heeft genomen van een datalek, zodat u nog de gelegenheid heeft tijdig de AP te informeren. Normaal gesproken maakt u hierover afspraken met uw verwerkers in een zogenaamde verwerkersovereenkomst. Het is dan ook raadzaam om met uw verwerker af te spreken dat deze uiterlijk binnen 24 uur aan u meldt, zodat u nog voldoende tijd heeft om te melden bij de AP.

Niet melden

Een datalek hoeft niet gemeld te worden als, zoals de AVG bepaalt, het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. In andere bewoordingen houdt dit in dat het datalek geen betrekking heeft op persoonsgegevens van gevoelige aard en/of het datalek niet leidt tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens of de kans hierop.

Persoonsgegevens van gevoelige aard en factoren met kans op ernstige nadelige gevolgen

Persoonsgegevens van gevoelige aard zijn:

- bijzondere persoonsgegevens zoals religieuze of levensbeschouwelijke overtuiging, ras, politieke opvattingen en gegevens over gezondheid,
- BSN-nummer,
- gegevens die kunnen leiden tot stigmatisering of uitsluiting,
- gegevens die onderworpen zijn aan geheimhouding/beroepsgeheim.

Factoren met (kans op) ernstige nadelige gevolgen:

- omvangrijke verwerkingen of een keten van gegevensverwerking,
- ingrijpende beslissingen die worden genomen met de gegevens,
- kwetsbare groepen zoals kinderen en gehandicapten.

Hoe meld je een datalek?

Organisaties die een datalek moeten melden, doen dit bij de AP via het digitale meldingsformulier op de website van de AP. U kunt met dit formulier ook een voorlopige melding doen en deze later aanvullen of intrekken.

Welke informatie moet u verstrekken?

De volgende informatie moet u verstrekken:

- de aard van het datalek, waar mogelijk onder vermelding van de categorieën van betrokkenen en het aantal betrokkenen,
- de naam van de persoon met wie contact kan worden opgenomen voor meer informatie
- de (waarschijnlijke) gevolgen van het datalek,
- de maatregelen die u heeft voorgesteld en/of genomen om het datalek aan te pakken.

Documentatieplicht

Voor alle datalekken (ongeacht of u deze heeft gemeld) geldt dat u deze moet vastleggen in bijvoorbeeld een incidentenregister, waarbij u bovenstaande gegevens vastlegt. Daarbij is het raadzaam vast te leggen wat het meldingsnummer van het datalek is dan wel de reden waarom is besloten af te zien van melding.

Melding aan betrokkene(n)

Wanneer een inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (ofwel ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkene(n)), dient u de betrokkene(n) direct te informeren. De mededeling aan de betrokkene(n) bevat een toelichting, in duidelijke en eenvoudige taal, op wat er is gebeurd, op de acties en maatregelen die zijn ondernomen, wat het betekent voor de betrokkene(n) en het advies dat u geeft over wat betrokkene(n) het beste kan (kunnen) doen.

Let op!
In de volgende situaties dient altijd gemeld te worden aan betrokkene(n): het betreft lekken van persoonsgegevens van gevoelige aard, bijvoorbeeld BSN-nummers of financiële gegevens, de persoonsgegevens zijn blootgesteld aan vernietiging of aantasting of de versleuteling van de persoonsgegevens is niet adequaat of niet volledig.

Niet melden aan betrokkene(n)

De mededeling aan de betrokkene(n) is niet vereist wanneer een van de volgende voorwaarden is vervuld:

- u heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling van gegevens,
- u heeft achteraf maatregelen genomen om ervoor te zorgen dat het bedoelde hoge risico voor de rechten en vrijheden van betrokkene(n) zich waarschijnlijk niet meer zal voordoen,
- de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkene(n) even doeltreffend wordt (worden) geïnformeerd.

Heeft u vragen over de AVG? Bel of mail ons! Wij helpen u graag verder.

Anne-Marie Dijkhorst - adijkhorst@horlings.nl
Inez Janse - ijanse@horlings.nl
T: +31 (0)20 5700 200