Speciale AVG-nieuwsbrief

11 mei 2018

Per 25 mei 2018 treedt de AVG, de nieuwe Europese privacywet, in werking. Ook u krijgt vrijwel zeker met deze wetgeving te maken. Uiteraard zijn wij u hierbij graag van dienst.

In deze speciale AVG-nieuwsbrief treft u 5 actuele en praktische artikelen aan die u bij de uitvoering van de AVG ondersteunen.

1. Voldoe in 5 stappen aan AVG

Het kan u niet ontgaan zijn. Op 25 mei 2018 wordt definitief de Algemene Verordening Gegevensbescherming van toepassing. De AVG brengt nieuwe verplichtingen en verantwoordelijkheden met zich mee.

Alle bedrijven en organisaties die werken met persoonsgegevens moeten zich voorbereiden op deze AVG, dus ook kleine mkb'ers en zzp'ers. In vijf stappen bent u AVG-proof.

Stap 1: Creëer intern bewustwording, zorg voor een vast aanspreekpunt
Informeer uw medewerkers over de wetgeving, de impact van de AVG op uw huidige processen en bij wie zij terecht kunnen bij vragen. Onder de AVG krijgen uw klanten meer privacyrechten.

Stap 2: Maak een register met persoonsgegevens die u verwerkt
Documenteer welke persoonsgegevens u verwerkt en met welk doel, waar deze gegevens vandaan komen en met wie u ze deelt. Belangrijk is de wijze waarop u de toestemming van uw klanten vraagt, krijgt en registreert.

Stap 3: Breng risico's in kaart en zorg voor beveiligingsmaatregelen
Standaard moeten in uw bedrijfsvoering en ICT ingevoerd zijn:

1. 'Privacy by design' voor de bescherming van persoonsgegevens: dit houdt in dat u al tijdens de ontwikkeling van nieuwe producten en diensten aandacht besteedt aan privacyverhogende maatregelen. (NB: Dit geldt alleen indien u zelf software of andere producten en diensten ontwikkelt)
2. 'Dataminimalisatie' waarmee u zorgt dat u alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het doel. Hiermee bespaart u zich ook nog eens een hoop werk.

Stap 4: Zorg voor documentatie van datalekken
Bij een datalek vallen persoonsgegevens in handen van derden die geen toegang tot die gegevens zouden mogen hebben. De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde, alleen de eisen voor de registratie zijn strenger.

Stap 5: Breng verwerkingen door derden in kaart, sluit verwerkersovereenkomsten
Check de contracten en gemaakte afspraken goed voor alle pakketten die u heeft uitbesteed aan derden, denk aan een administratiekantoor of een arbodienst, en zorg ervoor dat alles goed is vastgelegd (de zogenaamde verwerkersovereenkomsten).

Tip: Meer informatie is te vinden op de site van de Autoriteit Persoonsgegevens.

Extra:
Wat betreft de evt. verwerkersovereenkomst die u met ons dient af te sluiten, zullen wij u binnenkort benaderen indien dit nodig mocht zijn. Wij zijn druk met de verwerkersovereenkomsten met subverwerkers en daarna kunnen wij met u de overeenkomsten vernieuwen.

2. Hoe lang mag u persoonsgegevens bewaren?

Hoe lang mag u bij een vacature bijvoorbeeld de sollicitatiegegevens van kandidaten bewaren, of camerabeelden? 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? Wat zegt de strengere AVG erover die per 25 mei 2018 ingaat en ook voor uw bedrijf gaat gelden?

Volgens de AVG, dat is ook al zo onder de Wet bescherming persoonsgegevens (WBP), mag u persoonsgegevens niet langer mag 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 voldoen:

- U dient vooraf vast te stellen hoelang bepaalde documenten met persoonsgegevens bewaard gaan worden.
- De bewaartermijnen moeten openomen 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 verstrijken van de bewaartermijn dienen de persoonsgegevens daadwerkelijk vernietigd te worden of geanonimiseerd.

Salaris, factuur en verzuim
Er zijn binnen uw organisatie diverse processen en activiteiten waarin verschillende categorieën van persoonsgegevens nodig zijn 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
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 en arbeidsvoorwaarden	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.

3. Hoe maak ik een register van verwerkingen?
(incl. voorbeeldregister)

De belangrijkste nieuwe eis in de strengere privacywet AVG, die per 25 mei ingaat, 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. Met het verwerkingsregister 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.

Voor bijna elk mkb-bedrijf verplicht
Heeft uw bedrijf met 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 betrokkenen
- 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:

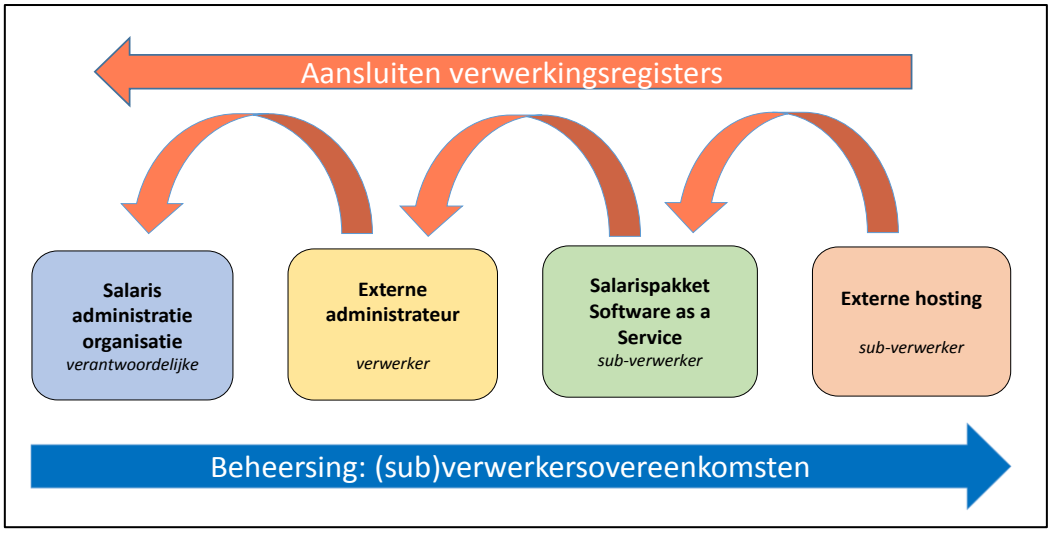
- de verwerkingsdoelen en de grondslagen voor verwerking
- een beschrijving van de categorieën van betrokkenen
- een beschrijving van de categorieën van persoonsgegevens
- de verwerkers die diensten voor u verlenen en beschikking over uw persoonsgegevens
- de categorieën van ontvangers aan wie de persoonsgegevens 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

Verwerkingsverantwoordelijke: een organisatie die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
Verwerker: een organisatie die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

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 uitbesteed, 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 ziet u op welke wijze u dit register op kunt zetten in en 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) verwerkers	Verwerkings-doel	Grondslag	Bewaar termijn	Maatregelen
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 welke proces of 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

4. Toestemming gebruik foto werknemer

Gebruikt u foto's van werknemers voor bijvoorbeeld uw website of een smoelenboek? Dat mag op grond van de privacywetgeving alleen wanneer uw werknemer hier uitdrukkelijk toestemming voor gegeven heeft en de werknemer weet waarvoor hij deze toestemming precies geeft.

Zorg dus dat u schriftelijk toestemming vraagt, en daarbij duidelijk uitlegt voor welke specifieke doeleinden u deze informatie wilt hebben. Zorg vervolgens dat de foto's goed beveiligd worden tegen misbruik. Deze regels gelden al onder de huidige wet maar worden wel strenger uitgelegd bij de invoer van de nieuwe privacyregels per 25 mei 2018 als de AVG (Algemene Verordening Gegevensbescherming) in werking treedt. Nieuw is bijvoorbeeld de boete bij niet naleving van maximaal € 20 miljoen of 4% van de wereldwijde jaaromzet wanneer dat meer is.

Let op!
Geeft de werknemer de toestemming niet, gebruik de foto dan ook niet.

5. Veel bedrijven nog niet klaar voor nieuwe privacywet AVG

Boetes

De nieuwe privacywet, de Algemene Verordening Gegevensbescherming (AVG), bevat strengere regels voor het opslaan en verwerken van gegevens. Wie niet aan de nieuwe regels voldoet, kan een boete gepresenteerd krijgen. Er kan echter in eerste instantie ook een waarschuwing worden uitgedeeld bij overtreding van de regels.

Let op!
De wet geldt voor bedrijven, overheden, organisaties en verenigingen, dus ook voor sportclubs.