De Resultaatbepalers

## Informatiegids Algemene Verordening Gegevensbescherming

Vanaf 25 mei 2018 is de AVG van toepassing. Deze wet geldt voor alle lidstaten van de Europese Unie. Het doel van de AVG is het beschermen van natuurlijke personen voor wat betreft de verwerking van hun gegevens.

**Wie valt er onder de AVG?**

De AVG is van toepassing op iedere organisatie, groot of klein, die persoonsgegevens geheel of gedeeltelijk verwerkt of opneemt in een bestand. Persoonsgegevens zijn te kenmerken als alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijk persoon. Zo'n persoon wordt binnen de AVG een betrokkene genoemd.

**Maar wat is dan verwerken?**

Verwerken is iedere bewerking waarmee persoonsgegevens zijn gemoeid. Dit kan het verzamelen, vastleggen, opslaan, wijzigen, opvragen, raadplegen of gebruiken van persoonsgegevens zijn. Hierbij wordt binnen de AVG onderscheid gemaakt tussen de verwerkingsverantwoordelijke en de verwerker. Hier is de verwerkingsverantwoordelijke degene die bepaalt op welke wijze en waarom er persoonsgegevens worden verwerkt. Dus een organisatie is bijvoorbeeld verwerkings-verantwoordelijke bij het verwerken van klantgegevens in een klantenbestand, bij het verwerken van klantgegevens op de verkoopfacturen of bij het vastleggen van gegevens van personeel. De verwerker is degene die in opdracht van de verwerkingsverantwoordelijke de persoonsgegevens verwerkt. Het is aan de verwerker om de instructies van de verwerkingsverantwoordelijke op te volgen. Denk hierbij aan de software leverancier, uitbestede loonadministratie of het accountantskantoor van de betreffende organisatie.

**Zijn gegevens van organisaties ook persoonsgegevens?**

Gegevens van organisaties zijn in principe geen persoonsgegevens. Of het moet zo zijn dat deze gegevens op een bepaalde manier terug te leiden zijn tot een natuurlijk persoon binnen die organisatie. Hierbij kun je denken aan bijvoorbeeld een bedrijfsnaam die hetzelfde is als de naam van de eigenaar, een persoonlijk e-mailadres of een mobiel telefoonnummer dat ook door de betreffende persoon in privé wordt gebruikt.

**Mag ik als organisatie persoonsgegevens verwerken?**

Zolang de persoonsgegevens in overeenstemming met de AVG worden verwerkt dan mag dit. Hierbij moet continu in de gaten worden gehouden met welk doel deze gegevens worden verzameld.

Een belangrijk doel is de toestemming van een betrokkene. Deze moet specifiek en eenduidig zijn. Daarbij moet de betrokkene de keuze hebben om te weigeren en weten waarvoor toestemming wordt gegeven. Er mogen geen twijfels aanwezig zijn over het feit dat een betrokkenen toestemming heeft gegeven. Organisaties zullen er over na moeten denken hoe dit kan worden gewaarborgd. Een gegeven toestemming moet altijd kunnen worden ingetrokken.

Een ander belangrijk doel is de noodzaak om een overeenkomst uit te kunnen voeren. Kortom, welke gegevens zijn absoluut essentieel om aan de overeenkomst te kunnen voldoen. Zo heeft een belastingadviseur het BSN-nummer van zijn cliënt nodig om een aangifte inkomstenbelasting in te dienen. Maar het BSN-nummer is daarentegen weer niet nodig wanneer er een pakketje geleverd moet worden, in dat geval volstaan alleen de NAW-gegevens.

Het laatste veel voorkomende belangrijke doel is het voldoen aan de wettelijke verplichting van de verwerkingsverantwoordelijke. Denk hierbij aan het bewaren van een identiteitsbewijs, omdat dit een verplichting is binnen een personeelsdossier.

**Wat zijn de verplichtingen van de verwerkingsverantwoordelijke?**

Als verwerkingsverantwoordelijke moeten maatregelen worden genomen om de verwerking van persoonsgegevens volgens de AVG te laten verlopen. De te nemen maatregelen zijn erg afhankelijk van de soort persoonsgegevens. Daarnaast is het afhankelijk van het doel van de verwerking en de risico’s die er worden gelopen bij de verwerking. Om dit voor een organisatie in beeld te krijgen moet er een verwerkingsregister worden opgemaakt. Nadat deze is opgemaakt moet deze continu up-to-date worden gehouden. Verder moeten er maatregelen worden genomen om de persoonsgegevens die worden verwerkt zo goed mogelijk te beschermen. Ook moeten er afspraken zijn gemaakt met de verwerkers waarmee de organisatie zaken doet. Dit kan worden gedaan met verwerkers-overeenkomsten. Wanneer op basis van toestemming persoonsgegevens worden verwerkt, dan moet de wijze waarop toestemming wordt gevraagd en het bewijs van het geven van deze toestemming worden vastgelegd. Om naar de betrokkenen en het personeel van de organisatie duidelijk te maken wat er met de persoonsgegevens wordt gedaan is het verstandig om een privacybeleid op te stellen. Deze wordt intern aan het personeel verstrekt en moet onderdeel worden van de arbeidscontracten. Voor de betrokkenen bij de organisatie kan er voor worden gekozen om het privacybeleid op de website te plaatsen en onderdeel te maken van overeenkomsten en de algemene voorwaarden.

**In de AVG gaat het over privacy by design en privacy by default, wat houdt dat in?**

Dit betekent privacy door ontwerp en privacy door standaardinstellingen. Privacy moet onderdeel worden van het beleid van een organisatie. Het vormt de basis en het uitgangspunt bij de verwerking van persoonsgegevens. Bij het toepassen van nieuwe systemen moeten standaard-instellingen worden verwerkt die helpen om te voldoen aan de AVG.

**Wat is een datalek?**

Er is sprake van een datalek op het moment dat persoonsgegevens in de handen vallen van derden die geen toegang tot die gegevens mogen hebben. Doorgaans is dit het gevolg van een beveiligingsprobleem. Het gaat om inbreuken op de beveiliging van gegevens, verlies, ongeoorloofde wijziging, verstrekking of toegang tot persoonsgegevens. Als voorbeelden kan gedacht worden aan een gehackte database, het verliezen van een USB-stick met persoonsgegevens, het per ongeluk leveren aan een verkeerd persoon of een email die wordt verzonden naar het verkeerde adres. Dreiging van een inbreuk op de beveiliging of een tekortkoming in de beveiliging wordt niet gezien als een datalek. Op het moment dat er sprake is van een datalek dan moet hiervan melding worden gemaakt bij de Autoriteit Persoonsgegevens en mogelijk ook aan de betrokkenen.

**Hoe moet een datalek worden gemeld?**

Een datalek moet binnen 72 uur nadat het datalek is geconstateerd zijn gemeld bij de Autoriteit Persoonsgegevens en mogelijk aan de getroffen betrokkenen. Dit moet ook gebeuren wanneer nog niet alles rondom het datalek bekend is. Dit is geen reden om de melding uit te stellen. De melding bevat informatie over:

- Aard en omvang van de inbreuk
- De categorieën en aantallen van betrokkenen en persoonsgegevensregisters
- De waarschijnlijke gevolgen van de inbreuk
- De maatregelen die zijn genomen om de nadelige gevolgen van de inbreuk te beperken

Om dit goed te doen en niets te vergeten richt de organisatie een procedure datalekken in. Deze procedure kan worden gevolgd in geval er sprake is van een datalek.

**Welke afspraken moeten worden gemaakt met verwerkers?**

Het is vanuit de AVG verplicht gesteld dat afspraken met verwerkers schriftelijk worden vastgelegd in een verwerkersovereenkomst. Deze regelt een aantal zaken:

- Inhoud en duur van de verwerking
- Aard en doel van de verwerking
- De soorten persoonsgegevens en de categorieën van betrokkenen
- De rechten en verplichtingen van de verwerkingsverantwoordelijke
- Instructies voor de verwerking
- Waarborgen rondom toegang tot persoonsgegevens
- Waarborgen rondom het niveau van beveiliging van de persoonsgegevens
- Vernietiging of teruggave van gegevens bij beëindiging van de overeenkomst met de verwerker
- Afspraken met betrekking tot sub-verwerkers

De organisatie sluit verwerkersovereenkomsten met leveranciers die persoonsgegevens voor de organisatie beheren of verwerken. Dat zijn bijvoorbeeld de accountant, externe loonadministratie, software leveranciers en andere leveranciers die persoonsgegevens beheren of verwerken waar de organisatie de verwerkingsverantwoordelijke van is.

**Wat zijn de verplichtingen van de verwerker?**

Een verwerker handelt op basis van de instructies die zijn meegegeven door de verwerkings-verantwoordelijke. Daarmee is de verwerker verplicht om de verwerkingsverantwoordelijke te helpen bij het uitvoeren van een deel van zijn plichten. Denk hierbij bijvoorbeeld aan de rechten van de betrokkenen en het melden van datalekken. Het is de verwerker verplicht om een verwerkers-

overeenkomst met de verwerkingsverantwoordelijke te ondertekenen. Ook de verwerker is verplicht om te zorgen voor voldoende beveiliging en ook hij zorgt voor een verwerkingsregister. De verwerker is aansprakelijk ten opzichte van de verwerkingsverantwoordelijke voor wat betreft de gegevensbescherming. Dat geldt ook voor het naleven van verplichtingen door de sub-verwerker.

Hoewel de verplichting om persoonsgegevens te beschermen is opgelegd aan de verwerkings-verantwoordelijke, is ook de verwerker zelfstandig verplicht om te zorgen voor voldoende maatregelen om de persoonsgegevens te beschermen. De verwerker moet er voor zorgen dat de medewerkers die toegang hebben tot persoonsgegevens dit alleen in opdracht van de verwerkings-verantwoordelijke verwerken en dit vertrouwelijk behandelen.

Het is toegestaan om voor de verwerking van persoonsgegevens een sub-verwerker in te schakelen. Hiervoor is vooraf een schriftelijke toestemming nodig van de verwerkingsverantwoordelijke. De sub-verwerkers moeten er voor zorgen dat zij minimaal hetzelfde beveiligingsniveau als dat van de verwerker hebben. Op het moment dat een verwerkingsopdracht ten einde komt moet de verwerker de betrokken persoonsgegevens verwijderen of teruggeven aan de verwerkings-verantwoordelijke, tenzij er sprake is van een wettelijke verplichting om deze gegevens te bewaren.

**Wat voor rechten hebben betrokkenen?**

Een betrokkene heeft de volgende rechten ten opzichte van de verwerkingsverantwoordelijke:

- Het recht op informatie over de verwerkingen
- Het recht op inzage in zijn gegevens
- Het recht op correctie van de gegevens als deze niet kloppen
- Het recht op verwijdering van de gegevens en het recht om vergeten te worden
- Het recht op beperking van de gegevensverwerking
- Het recht op verzet tegen de gegevensverwerking
- Het recht op overdracht van zijn gegevens (dataportabiliteit)
- Het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming

Wanneer een betrokkene een van de voorgenoemde rechten uitoefent dan heeft de verwerkingsverantwoordelijke de plicht om aan het gedane verzoek gehoor te geven. Dat moet dan gebeuren binnen een maand na ontvangst van het verzoek. Uitzondering hierop is een situatie waarin het gaat om veel of complexe verzoeken. Er kunnen dan twee extra maanden worden geclaimd om aan het verzoek te voldoen. Ondanks dat er in zo'n geval sprake is van drie maanden tijd moet de betrokkene wel binnen een maand op de hoogte worden gesteld dat zijn verzoek is ontvangen. De informatie hierover moet duidelijk en eenvoudig worden verstrekt en zegt in ieder geval iets over:

- De doelen waarvoor de gegevens worden verwerkt
- De categorieën persoonsgegevens die worden verwerkt van de betrokkene
- De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of worden doorgegeven

- Hoe lang de gegevens worden bewaard of welke criteria de bewaartermijn van de gegevens bepalen
- Het recht op wijziging, verwijdering, beperking of bezwaar
- Het recht om een klacht in te dienen bij de toezichthouder

Het recht op het laten wissen van de gegevens van een betrokkene bestaat in de volgende gevallen:

- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld
- De betrokkene trekt zijn toestemming voor het verwerken in
- De betrokkene heeft gegrond bezwaar gemaakt tegen de verwerking
- De persoonsgegevens zijn onrechtmatig verwerkt
- De persoonsgegevens moeten worden gewist op grond van een wettelijke verplichting
- De persoonsgegevens houden verband met een aanbod van internetdiensten aan een kind

Tot slot bestaat er voor een betrokkene recht op schadevergoeding op het moment dat deze (im)materiële schade lijdt door een overtreding van de AVG. Hiervoor is de verwerkings-verantwoordelijke aansprakelijk. De verwerker is aansprakelijk op het moment dat hij niet heeft voldaan aan de verplichten vanuit de AVG of wanneer hij niet heeft gehandeld volgens de afspraken die zijn gemaakt met de verwerkingsverantwoordelijke.

**Met welke doelen mogen persoonsgegevens worden verwerkt?**

Vanuit de AVG zijn er in totaal zes rechtsgrondslagen waarop het doel van een verwerking van persoonsgegevens kan zijn gebaseerd. Op het moment dat er persoonsgegevens worden verwerkt die niet zijn gebaseerd op een van deze grondslagen dan is dit niet toegestaan. In totaal zijn er zes grondslagen:

1. De betrokkene heeft toestemming voor de verwerking gegeven
2. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst met de betrokkene
3. De verwerking berust op een wettelijke verplichting van de verantwoordelijke
4. De bescherming is noodzakelijk om de belangen van de betrokkene te beschermen
5. Verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag
6. De verantwoordelijke heeft een gerechtvaardigd belang bij de verwerking

Voor de nummers 2 t/m 6 geldt dat de verwerking alleen gerechtvaardigd is op het moment dat deze noodzakelijk is voor het genoemde doel. Er hoeft in dat geval geen toestemming te worden gegeven door de betrokkene. Tot slot moet de verwerking van gegevens in proportie staan en moet het in de betreffende situatie de meest logische en beste manier zijn om het doel te bereiken.

**Wordt er toezicht gehouden op de naleving van de AVG?**

In Nederland verzorgt de Autoriteit Persoonsgegevens het toezicht op de naleving van de AVG. Binnen de Europese Unie werken de toezichthouders met elkaar samen. Zo wordt een samenhangende en consistente interpretatie van de AVG bewerkstelligd. Als uitgangspunt is gehanteerd dat de verwerkingsverantwoordelijken in principe met één toezichthouder te maken hebben. Ook wanneer er sprake is van vestigingen in meerdere landen of verkoop van goederen/diensten in meerdere landen. Er wordt in zo'n geval gekeken naar de hoofdvestiging.

Voor het uitvoeren van het toezicht heeft de Autoriteit Persoonsgegevens verschillende bevoegdheden. Zo mogen zij controles uitvoeren en informatie verkrijgen. Het is verplicht om hier als verwerkingsverantwoordelijk of verwerker aan mee te werken.

Op Europees niveau is er het Europees Comité voor de gegevensbescherming. Dit comité zorgt voor een uniforme uitleg van de AVG binnen de EU.

**Worden er boetes uitgedeeld bij het niet naleven van de AVG?**

Op het moment dat de AVG niet wordt nageleefd kan er een boete worden opgelegd. Deze kan oplopen tot € 10 miljoen of 2% van de wereldwijde jaaromzet als dat hoger is voor het niet voldoen aan verplichtingen. De boete kan oplopen tot een bedrag van € 20 miljoen of 4% van de wereldwijde jaaromzet als dat hoger is voor het schenden van principes, rechtsgrondslagen en rechten van betrokkenen.