(AVG) Algemene Verordening Gegevensbescherming

LET OP! De AVG is een omvangrijk stuk, dat slechts beperkt is toegelicht. De precieze invulling van begrippen en bepalingen is onduidelijk. De toezichthouders en de Europese rechter zullen die begrippen nader moeten invullen.

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing in alle lidstaten van de Europese Unie. De AVG heeft rechtstreekse werking en vervangt in Nederland de Wet bescherming persoonsgegevens.

Rechtstreekse werking wil zeggen dat de AVG niet eerst in nationale wetgeving verwerkt hoeft te worden. Het doel van de AVG is de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie. De AVG biedt de lidstaten op een aantal onderdelen de ruimte om bepalingen nader in te vullen in nationale uitvoeringswetten. Nederland heeft daarvan gebruik gemaakt.

Op wie is de AVG van toepassing?

De AVG is van toepassing op iedereen die persoonsgegevens geheel of gedeeltelijk (automatisch) verwerkt of opneemt in een bestand. Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon. De AVG duidt deze persoon aan als betrokkene.

Verwerken is iedere bewerking die betrekking heeft op persoonsgegevens. Dat kan zijn verzamelen, vastleggen, opslaan, wijzigen, opvragen, raadplegen of gebruiken.

De AVG maakt onderscheid tussen de verwerkingsverantwoordelijke en de verwerker. De verwerkingsverantwoordelijke bepaalt hoe en waarom er persoonsgegevens worden verwerkt. De verwerker is degene die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. De verwerker moet de instructies van de verwerkingsverantwoordelijke opvolgen.

Gegevens van organisaties zijn geen persoonsgegevens, tenzij het gaat om gegevens die betrekking hebben op of herleidbaar zijn tot een natuurlijke persoon binnen die organisatie, zoals een persoonlijk emailadres.

Mag ik gegevens verwerken?

Persoonsgegevens mogen worden verwerkt zolang dat in overeenstemming met de AVG gebeurt. Belangrijk is dat persoonsgegevens alleen verwerkt mogen worden voor het doel waarvoor ze verzameld zijn. Persoonsgegevens mogen gebruikt worden voor andere doelen als die doelen verenigbaar zijn met het oorspronkelijke doel. Dat doel moet duidelijk omschreven zijn en gebaseerd zijn op een van de in de AVG opgenomen grondslagen. De belangrijkste grondslagen zijn toestemming van de betrokkene en de noodzaak voor de uitvoering van een overeenkomst met de betrokkene of om te voldoen aan een wettelijke verplichting van de verwerkingsverantwoordelijke.

Wanneer persoonsgegevens worden verwerkt op basis van toestemming, dan moet deze vrij, specifiek en ondubbelzinnig worden gegeven. De betrokkene moet dus de keuze hebben om te weigeren en moet weten waarvoor hij zijn toestemming geeft. Verder mag er geen twijfel bestaan over het feit dat een betrokkene toestemming heeft gegeven. Het aanvinken van een vakje op een website volstaat; het niet uitvinken van een al ingevuld vakje volstaat

niet als toestemming. Eenmaal gegeven toestemming kan op ieder moment weer worden ingetrokken.

Een voorbeeld van het gebruik van persoonsgegevens die nodig zijn voor de uitvoering van een overeenkomst is het gebruik van NAW-gegevens van een klant voor de verzending door een leverancier van een besteld artikel.

Een voorbeeld van persoonsgegevens die verwerkt worden om te voldoen aan een wettelijke plicht is het bewaren van een kopie van het identiteitsbewijs van een werknemer bij de loonadministratie.

Plichten van de verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke moet passende en effectieve maatregelen nemen om te zorgen dat de verwerkingen in lijn met de AVG plaatsvinden. Welke maatregelen dat zijn hangt af van de aard van de gegevens, het doel van de verwerking en de risico's van de verwerking. In het kort komt het erop neer dat er een register van verwerkingsactiviteiten wordt bijgehouden, dat er passende beveiligingsmaatregelen worden genomen om de persoonsgegevens te beschermen en dat er afspraken worden gemaakt met verwerkers van gegevens. Wanneer toestemming de grondslag voor verwerking is moet de wijze waarop toestemming wordt gevraagd worden vastgelegd. Ook het bewijs dat toestemming is verleend moet worden vastgelegd.

Het kan verstandig zijn een gegevensbeschermingsbeleid op te stellen, waarin wordt bepaald welke technische en organisatorische maatregelen genomen moeten worden, hoe deze vorm krijgen in de praktijk en wie verantwoordelijk is voor de uitvoering ervan.

Om duidelijk te maken wat er met verzamelde persoonsgegevens wordt gedaan verdient het aanbeveling om een privacy statement op te stellen.

Privacy door ontwerp en standaardinstellingen (by design and by default)

Nieuw in de AVG is het beginsel van privacy door ontwerp en door standaardinstellingen. Dit houdt in dat privacy en gegevens- bescherming worden meegenomen als eisen bij de ontwikkeling van nieuw beleid of het ontwerp van nieuwe systemen waarmee persoonsgegevens worden verwerkt.

Datalek

Een datalek, dat is een inbreuk in verband met persoonsgegevens, moet worden gemeld aan de Autoriteit Persoonsgegevens en mogelijk ook aan de betrokkenen. Het gaat om inbreuken op de beveiliging van gegevens, verlies, ongeoorloofde wijziging, verstrekking of toegang tot persoonsgegevens. De dreiging van een inbreuk op de beveiliging of een tekortkoming in de beveiliging is geen datalek.

Een datalek moet binnen 72 uur na de ontdekking daarvan worden gemeld bij de Autoriteit Persoonsgegevens, ook als nog niet alle informatie voorhanden is. De melding omvat in ieder geval:

- aard en omvang van de inbreuk;
- de categorieën en aantallen van betrokkenen en persoons- gegevensregisters;
- de waarschijnlijke gevolgen van de inbreuk;
- de maatregelen die zijn genomen ter beperking van de eventuele nadelige gevolgen van de inbreuk.

Afspraken met verwerkers

De AVG schrijft voor dat afspraken met verwerkers in een overeenkomst schriftelijk worden vastgelegd. Deze verwerkersovereenkomst regelt in ieder geval:

- onderwerp 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 omtrent toegang tot de persoonsgegevens;
- waarborgen omtrent het niveau van beveiliging van de persoonsgegevens;
- vernietiging of teruggave van gegevens na beëindiging van de overeenkomst met de verwerker;
- afspraken met betrekking tot sub-verwerkers.

In plaats van individuele overeenkomsten kan gekozen worden voor door de Europese Commissie of Autoriteit Persoonsgegevens vastgestelde standaard contractbepalingen.

Plichten van de verwerker

De verwerker handelt op basis van instructies van de verwerkingsverantwoordelijke. De verwerker is verplicht de verwerkingsverantwoordelijke te helpen bij het uitvoeren van sommige van diens plichten, zoals de invulling van de rechten van de betrokkenen en het melden van datalekken.

De verwerker is verplicht een verwerkersovereenkomst met de verwerkingsverantwoordelijke te tekenen. Daarnaast is de verwerker verplicht om de persoonsgegevens te beveiligen en moet hij een register van verwerkingsactiviteiten bijhouden. Organisaties tot 250 personen hoeven geen register bij te houden, tenzij het verwerkingen met een hoog risico voor betrokkenen betreft of niet-incidentele verwerkingen.

De verwerker is ten opzichte van de verwerkingsverantwoordelijke aansprakelijk voor de gegevensbescherming. Dat geldt ook voor de naleving van verplichtingen door de sub-verwerker.

Hoewel de verplichting om persoonsgegevens te beschermen is opgelegd aan de verwerkingsverantwoordelijke, is ook de verwerker zelfstandig verplicht om passende beveiligingsmaatregelen te treffen. De verwerker moet erop toezien dat medewerkers die toegang hebben tot persoonsgegevens deze enkel in opdracht van de verwerkingsverantwoordelijke verwerken en vertrouwelijk behandelen.

Het inschakelen van sub-verwerkers bij de verwerking van persoonsgegevens is mogelijk met voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke. Met deze sub- verwerkers moet de verwerker een overeenkomst sluiten waarin de sub-verwerker wordt verplicht om minimaal hetzelfde niveau van bescherming te bieden als de verwerker zelf hanteert.

Bij het einde van de verwerkingsopdracht moet de verwerker de betrokken persoonsgegevens wissen of teruggeven aan de verwerkingsverantwoordelijke, behoudens afwijkende wettelijke bepalingen.

Rechten van betrokkenen

De betrokkene heeft de volgende rechten jegens 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 gegevens- verwerking;
- het recht op verzet tegen de gegevens- verwerking;
- het recht op overdracht van zijn gegevens (dataportabiliteit);
- het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming.

De verwerkingsverantwoordelijke is verplicht om gehoor te geven aan een verzoek van een betrokkene ter uitoefening van zijn rechten. Dat moet binnen een maand na ontvangst van het verzoek, tenzij het gaat om veel of complexe verzoeken. In dat geval geldt een extra termijn van twee maanden. Wel moet de betrokkene binnen een maand na ontvangst van het verzoek daarvan op de hoogte gesteld worden. Informatie moet in duidelijke en eenvoudige taal verstrekt worden. Een overzicht van informatie aan een betrokkene omvat ten minste:

- de doelen waarvoor de gegevens worden verwerkt;
- de categorieën persoonsgegevens die van de betrokkene worden verwerkt
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of worden doorgegeven;
- hoe lang gegevens worden bewaard of welke criteria de bewaartermijn bepalen;
- het recht op wijziging, verwijdering, beperking of bezwaar;
- het recht om een klacht in te dienen bij de toezichthouder.

Iedere betrokkene heeft het recht om zijn gegevens te laten wissen 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.

Recht op schadevergoeding

Een betrokkene die (im)materiële schade heeft geleden door een overtreding van de AVG heeft recht op vergoeding van de geleden schade. De verwerkings-verantwoordelijke is daarvoor aansprakelijk. De verwerker is slechts aansprakelijk voor zover hij niet heeft voldaan aan zijn verplichtingen uit hoofde van de AVG of als hij in strijd heeft gehandeld met de afspraken met de verantwoordelijke.

Rechtvaardigingsgrondslagen verwerking

De AVG bevat in totaal zes rechtsgrondslagen waarop het doel van een verwerking van persoonsgegevens kan zijn gebaseerd. Een verwerking die niet op een van deze grondslagen is gebaseerd is niet toegestaan. De zes grondslagen zijn:

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 verwerking 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.

Toezicht op naleving

Voor de grondslagen 2 tot en met 6 geldt dat de verwerking alleen gerechtvaardigd is wanneer deze noodzakelijk is voor het genoemde doel. De verwerking van gegevens moet proportioneel zijn en voldoen aan de eis van subsidiariteit. Als met de verwerking van de gegevens het gestelde doel niet kan worden bereikt, dan is deze verwerking niet proportioneel.

Het doel dat wordt nagestreefd moet in verhouding staan tot het feit dat daarvoor persoonsgegevens moeten worden verwerkt. Subsidiariteit betreft de vraag of het doel niet op een andere, minder ingrijpende, wijze kan worden bereikt.

Als de verwerking van persoonsgegevens noodzakelijk is voor één van de onder b tot en met f genoemde doelen, is toestemming van de betrokkene(n) niet nodig.

In Nederland is de Autoriteit Persoonsgegevens belast met het toezicht op de naleving van de AVG. Voor een samenhangende en consistente interpretatie van de AVG werken de Europese toezichthouders met elkaar samen. Uitgangspunt van de AVG is dat verwerkings-verantwoordelijken in beginsel met één toezichthouder te maken hebben, ook wanneer zij vestigingen hebben in meerdere lidstaten of wanneer zij goederen of diensten aanbieden in meerdere lidstaten. De locatie van de hoofdvestiging is daarbij bepalend.

Voor het uitvoeren van hun taken hebben de toezichthouders verschillende bevoegdheden, waaronder de bevoegdheid om controles te verrichten en om informatie te verkrijgen. De Autoriteit Persoonsgegevens kan inlichtingen vorderen en mag panden betreden in het kader van een onderzoek of controle. Verwerkingsverantwoordelijken en verwerkers zijn verplicht om mee te werken met de Autoriteit Persoonsgegevens.

Op Europees niveau is er het Europees Comité voor de gegevensbescherming. Dat comité is een orgaan van de Europese Unie en bestaat uit de voorzitters van de nationale toezichthouders en de Europese toezichthouder. Het Europees Comité moet zorgen voor een uniforme uitlegging van de AVG in de EU.

Boete

Wanneer de AVG niet wordt nageleefd kan de toezichthouder een administratieve boete opleggen. De boete kan oplopen tot € 10 miljoen of 2% van de wereldwijde jaaromzet als dat hoger is voor het niet voldoen aan verplichtingen zoals het uitvoeren van een gegevensbeschermings- effectbeoordeling of het niet melden van een datalek. 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.