AUXILIUM
adviesgroep

De Algemene Verordening Gegevensbescherming

In mei 2016 is er een nieuwe Europese verordening geïntroduceerd waarin privacyrechten zijn uitgebreid en bedrijven meer moeten verantwoorden over de omgang met persoonsgegevens. Er is een voorbereidingsperiode gegeven van twee jaar. Op 25 mei 2018 trad de verordening - ook wel afgekort AVG - in werking in heel Europa. Op dat moment verviel de toenmalige Wet bescherming persoonsgegevens (Wbp). De AVG vraagt ook de nodige inspanningen van u als MKB-bedrijf en de boetes bij overtredingen zijn significant. Heeft u al de vereiste maatregelen toegepast?

De geïntroduceerde verplichtingen in de omgang met persoonsgegevens komen voort uit de steeds verdergaande digitalisering van de maatschappij. Bij de invoering van de Wet bescherming persoonsgegevens in 2000 waren begrippen als 'cloud-computing', 'smartphones' en 'glasvezel' nog geen gemeengoed. Door de technologische ontwikkeling is het delen en verspreiden van gegevens inmiddels veel eenvoudiger geworden. Het is voor individuen echter moeilijk om nog goed toe te zien op een zorgvuldige omgang met hun gegevens door bedrijven. Daar brengt de AVG verandering in.

Individuen hebben meer rechten (bijvoorbeeld om vergeten te worden of gegevens mee te nemen) en u moet kunnen aantonen dat u voldoende maatregelen heeft genomen om de gegevens goed te beschermen. Ook als u een deel van uw gegevensverwerkingen heeft uitbesteed. Het gaat daarbij voornamelijk - maar niet uitsluitend - om geautomatiseerde verwerkingen.

Om te beginnen: welke gegevens mag ik verwerken?

Het is verstandig om allereerst goed te kijken naar de persoonsgegevens die u als bedrijf verzamelt en verwerkt. Alle gegevens die betrekking hebben op, of te herleiden zijn naar een natuurlijk persoon (direct en indirect) vallen onder de noemer persoonsgegevens. U mag als bedrijf alleen persoonsgegevens verwerken als u een 'grondslag' heeft. Er zijn zes grondslagen: u verwerkt gegevens waarbij u expliciet toestemming heeft gevraagd én gekregen, of als uitvloeisel van een contract/overeenkomst, of omdat u wettelijk verplicht bent, of omdat er een algemeen-, vitaal- of een gerechtvaardigd belang is.

U kunt dus niet zondermeer gegevens verwerken. Als u gegevens verzamelt nadat u hier expliciet toestemming voor heeft gekregen, is het goed om u te realiseren dat u deze toestemming naderhand moet kunnen aantonen. Zorgvuldige vastlegging is dus noodzakelijk.

Met de persoonsgegevens die u verwerkt moet u als een 'goed huisvader' omgaan. Ze moeten bijvoorbeeld beschermd zijn tegen verlies of inbreuk, niet langer worden bewaard dan noodzakelijk en u dient niet méér gegevens te verzamelen dan nodig is om uw doel te bereiken.

Opletten bij gevoelige- en bijzondere persoonsgegevens

Persoonsgegevens moeten dus goed beschermd zijn. Daarbij is de stelregel dat gegevens met een groter risico, met extra zorg en aandacht behandeld moeten worden. Hierbij wordt gekeken naar de impact die het heeft op het individu. Het onzorgvuldig omgaan met identiteitsgegevens of gegevens over iemands gezondheid kan bijvoorbeeld een grote impact hebben op de levenssfeer van betrokkene.

Als er een inbreuk is waarbij gevoelige- of bijzondere persoonsgegevens zijn ontvreemd, moet u dit altijd melden bij de Autoriteit Persoonsgegevens. Voorbeelden zijn gegevens over godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond of strafrechtelijk verleden.

U mag deze gegevens überhaupt alleen verwerken als u zich kunt beroepen op een van de tien wettelijke uitzonderingen. Verwerkt u deze gegevens als kernactiviteit en/of op grote schaal, of bent u een overheidsinstantie, dan kunt u daarnaast onder de AVG verplicht zijn om een functionaris voor de gegevensbescherming aan te stellen en/of een *Data protection impact assessment* uit te voeren. Het gaat dan om verwerking met een hoog privacy risico. Als er twijfel bestaat over deze noodzaak dan dient u te kunnen onderbouwen waarom u daarvan in voorkomende gevallen heeft afgezien.

Een overzicht van persoonsgegevens die u verwerkt

Het uitzoeken of u gegevens mag verwerken en of u gegevens verwerkt met een hoog privacy risico is een opstapje naar de verantwoordingsplicht. De AVG schrijft namelijk voor dat elk bedrijf met meer dan 250 werknemers verplicht is om een register van verwerkingsactiviteiten op te stellen. Kleinere bedrijven moeten dit ook doen, maar alleen voor gegevens die op structurele basis verwerkt worden. Dit register is één van de verantwoordingsverplichtingen. Het overzicht brengt in beeld wat u verwerkt en hoe u dat vorm geeft. U legt er ook in vast of gegevens binnen of buiten de EU worden verwerkt. Verwerkt u gegevens buiten de EU? Het land waar u de gegevens mee uitwisselt moet dan een vergelijkbaar beschermingsniveau hanteren anders bent u genoodzaakt om extra waarborgen te treffen.

Afspraken maken met partijen die u inschakelt

Als u op dit moment derde partijen inschakelt om een (deel van de) verwerking voor u uit te voeren dan bent u genoodzaakt om daar afspraken mee te maken. Hierin leggen u en de verwerker schriftelijk vast hoe er wordt omgegaan met privacy aspecten van de verwerkte gegevens. Dit wordt ook wel een verwerkingsovereenkomst genoemd. Het is essentieel om hierover te beschikken en in het belang van beide partijen. Onder verwerking wordt bijvoorbeeld ook verstaan: het bewaren, raadplegen, wijzigen, opvragen, vastleggen en combineren van gegevens. Ook met veel IT-leveranciers moet u dus in voorkomende gevallen een verwerkingsovereenkomst afsluiten.

Datalekken en bewustzijn

Het is van wezenlijk belang dat uw bedrijf goed op de hoogte is van de AVG. U kunt dan goed herkennen of er zich situaties voordoen die een risico vormen voor de bescherming van de persoonsgegevens. Of als er sprake is van een inbreuk (beter bekend als 'datalek'). De AVG introduceert ook een uitbreiding op de bestaande Wet meldplicht datalekken: álle datalekken binnen uw bedrijf dient u in een register te documenteren als onderdeel van de verantwoordingsverplichting. Een gestolen laptop kan daar een voorbeeld van zijn. Niet voor niets geeft de Autoriteit Persoonsgegevens aan dat **bewustzijn de eerste belangrijke stap is op weg naar de AVG**. Wellicht kunt u één of twee collega's de verantwoordelijkheid geven om binnen het bedrijf de nalevering van de AVG in de gaten te houden. Stel een jaarlijks evaluatiemoment vast om te onderzoeken of uw verantwoordingsdocumentatie nog actueel is en evalueer of uw informatiebeveiligingsniveau nog passend is.

Uw website en privacy

Naast de persoonsgegevens die u binnen uw bedrijf verwerkt is de kans groot dat u op uw website ook persoonsgegevens verwerkt. Bijvoorbeeld als u over een contactformulier beschikt of veel met zogenaamde cookies werkt. Ook op uw website moet u dan passende maatregelen nemen om de gegevens te beschermen en heldere informatie te verschaffen, bijvoorbeeld in de vorm van een privacy verklaring. Hierin maakt u kenbaar op welke wijze u omgaat met de gegevens en bij wie bezoekers terecht kunnen als er vragen zijn. Let bij uw website ook op standaardinstellingen. Deze moeten zodanig zijn ingesteld, dat ze standaard de minste impact hebben op de privacy van de betrokkenen. De AVG duidt deze aspecten als Privacy by Design en Privacy by Default. Als u zelf betrokken bent bij het ontwerpen van informatiesystemen dient u dit eveneens na te streven.

AUXILIUM
adviesgroep

Telefoon 033 - 433 72 17 | **E-mail** info@auxiliumadviesgroep.nl | **Website** www.auxiliumadviesgroep.nl