Wet bescherming persoonsgegevens (Wbp) gewijzigd

Per 1 januari 2016 is de Wet bescherming persoonsgegevens (Wbp) gewijzigd. De meest besproken wijziging ziet toe op de invoering van de zogenaamde meldplicht bij datalekken. Daarnaast heeft de Autoriteit Persoonsgegevens meer sanctie instrumenten gekregen en is ook de boetebevoegdheid uitgebreid.

Wet meldplicht datalekken

De Wbp bepaalt (onder meer) dat persoonsgegevens door middel van passende technische en organisatorische maatregelen dienen te worden beveiligd. De gegevens moeten derhalve niet alleen op technische wijze worden beschermd tegen toegang door derden, maar een organisatie dient er bijvoorbeeld ook intern voor te zorgen dat de gegevens uitsluitend toegankelijk zijn voor die onderdelen van een bedrijf die de gegevens nodig hebben voor de uitvoering van hun taken. Er moet nu melding worden gemaakt van iedere inbreuk op de (technische of organisatorische) maatregelen ter beveiliging tegen verlies of onrechtmatige verwerking van persoonsgegevens. Bij een inbreuk kan worden gedacht aan een hack of een technisch falen, maar ook aan verlies of diefstal van een laptop waarop persoonsgegevens staan. Een ‘datalek’ kan dus in vele vormen voorkomen.

De meldplicht geldt alleen als de inbreuk leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens (of een aanzienlijke kans daarop). Of hiervan sprake is van een inbreuk, moet u zelf beoordelen, maar de Autoriteit geeft wel (op dit moment nog niet-definitieve) richtsnoeren.

Melden aan de Autoriteit en aan de betrokkene

De melding dient te worden gedaan aan de Autoriteit Persoonsgegevens. Daarbij dient niet alleen te worden gemeld om wat voor inbreuk het gaat en welke (mogelijke) gevolgen die heeft, maar ook welke maatregelen zijn en/of worden genomen om de gevolgen te verhelpen. Indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de persoon waar de gegevens betrekking op hebben, dan moet ook de betrokkene in kennis worden gesteld van het lek. Indien gelekte gegevens (afdoende) versleuteld zijn, hoeft geen melding te worden gemaakt aan de betrokkene, maar wel aan de Autoriteit.

Uitbesteding van gegevensverwerking

Zowel de verplichting om te zorgen voor een gedegen beveiliging en om het te melden als dat is misgegaan, rust op de verantwoordelijke die de gegevensbewerking doet. Heeft u de gegevensverwerking uitbesteed aan een ander, dan is dat de bewerker. Wees u er zich van bewust dat bij een gebrekkige beveiliging het de verantwoordelijke is die het boeterisico loopt. Het is daarom van groot belang dat u in de bewerkersovereenkomst goede afspraken maakt over de beveiliging en het melden van een datalek.

Wat zijn persoonsgegevens?

Persoonsgegevens zijn: naam- en adresgegevens, e-mailadressen, pasfoto's, maar ook bijvoorbeeld IP-adressen.

Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die zo gevoelig zijn dat de verwerking ervan iemands privacy ernstig kan aantasten. Zulke gegevens mogen dan ook alleen onder zeer strenge voorwaarden worden verwerkt. Onder bijzondere of gevoelige persoonsgegevens vallen: gegevens over iemands ras, godsdienst, gezondheid, strafrechtelijk verleden of seksuele leven. Ook een lidmaatschap van een vakvereniging en het burgerservicenummer (BSN) zijn bijzondere persoonsgegevens.

Wanneer is er sprake van verwerking van persoonsgegevens?

Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. De wet noemt als voorbeelden van verwerking: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.
Je zou kunnen stellen dat alles wat men met een persoonsgegeven *doet* onder verwerken valt.

TIPS

- Controleer of de wijze, waarop op dit moment gegevens worden verwerkt binnen uw organisatie rekening houdt met de nieuwe regelgeving of dat er maatregelen nodig zijn om aan de nieuwe regels te kunnen voldoen.
- Zorg voor een juiste wijze van documenteren van gegevensverwerking en pas eventueel algemene voorwaarden en privacyverklaringen aan.

- Controleer of partijen, waar uw organisatie gegevens mee deelt, ook voldoen aan de nieuwe regels. Vervang eventueel bewerkersovereenkomsten.
- Indien er nu impliciete goedkeuring wordt gebruikt voor gegevensbewerking, regel dan vervangende toestemming.