ICTRECHT

Impact van de Europese Privacyverordening

De Wet bescherming persoonsgegevens (Wbp) gaat op de schop. Dit werd al in januari 2012 door de Europese Commissie aangekondigd, en nu heeft de plaatsvervanger van de Wbp een definitieve vorm gekregen. De (Europese) toezichthouder krijgt met de komst van de verordening tanden. Er kunnen boetes worden opgelegd van maximaal € 20.000.000,- of 4% van de wereldwijde jaaromzet.

De Wbp gaat plaatsmaken voor een Europese privacyverordening, de 'Algemene Verordening Gegevensbescherming' (AVG). Deze verordening zal in heel Europa voor dezelfde regels rondom privacy gaan zorgen en brengt heel wat veranderingen met zich mee voor het bedrijfsleven. Wij hebben een aantal hoofdpunten uit de AVG voor u op een rij gezet:

1. Wat moet er in een bewerkersovereenkomst staan?

Het sluiten van een bewerkersovereenkomst (dit wordt met de AVG verwerkersovereenkomst) tussen de verantwoordelijke voor de persoonsgegevens, en de partij die de persoonsgegevens voor hem verwerkt (nu bekend als bewerker, straks verwerker), was al verplicht vanuit de Wbp. De AVG benoemt echter een aantal specifieke punten die opgenomen dienen te worden in deze overeenkomst waaronder:

- de doeleinden van de gegevensverwerking;
- het soort persoonsgegevens dat verwerkt wordt;
- de categorieën van betrokkenen op wie de gegevens zien;
- het passend beveiligen van de gegevens;
- het uitvoeren van audits;
- het na afloop vernietigen of terugleveren van de gegevens aan de verantwoordelijke.

Bovendien zal de bewerker voortaan niet meer een externe partij mogen inschakelen om persoonsgegevens te verwerken zonder voorafgaande schriftelijke toestemming van de verantwoordelijke.

2. Wat betekent Privacy by design and by default?

Gedurende het gehele ontwikkelingsproces van producten en diensten moet u rekening houden met privacy. Dit kan door technieken als pseudonimisering toe te passen en door zo min mogelijk persoonsgegevens te verwerken, namelijk door uitsluitend noodzakelijke persoonsgegevens te verwerken. Deze noodzakelijkheidseis geldt tevens voor de toegankelijkheid tot de gegevens (wie heeft toegang tot welke gegevens) en de periode dat de gegevens bewaard worden. Ook moeten de standaardinstellingen van een product of dienst altijd zo privacyvriendelijk mogelijk zijn. Producten en diensten moeten dus 'privacy proof' ontwikkeld worden en ingesteld zijn.

3. Verandert de meldplicht datalekken?

Naast de Nederlandse wettelijke meldplicht voor datalekken kent ook de AVG een meldplicht voor datalekken. Op het moment dat er per ongeluk, of opzettelijk, data verloren gaan, of op straat terecht gekomen zijn, moet dit binnen 72 uur aan de toezichthouder gemeld worden. Als het lek waarschijnlijk een hoog risico inhoudt voor de betrokkenen (de personen waar de gegevens betrekking op hebben), dan moeten zij ook van het lek op de hoogte worden gesteld.

Daarnaast kent de AVG aan de bewerker een verplichting toe om het datalek aan de verantwoordelijke te melden. Het verschil met onze huidige meldplicht, is dat er enkel een melding bij de toezichthouder gedaan hoeft te worden van een lek als het lek daadwerkelijk heeft plaatsgevonden.
Onze huidige meldplicht noemt een incident al een datalek wanneer de onrechtmatige verwerking van persoonsgegevens niet uitgesloten kan worden.

ICTRecht B.V.
Amsterdam
T +31 (0)20 663 1941
I ictrecht.nl
E info@ictrecht.nl

4. Is het aanstellen van een privacy officer verplicht?

Waar het aanstellen van een 'privacy officer' in de Wbp niet verplicht is, is het onder de AVG in sommige situaties wel verplicht. De privacy officer is een persoon die toeziet op de omgang met persoonsgegevens binnen een organisatie en controleert of de organisatie voldoet aan de wet en toepasselijke regelgeving. De privacy officer moet onafhankelijk kunnen functioneren als privacyvraagbaak en mag zowel intern als extern aangesteld worden.

De privacy officer wordt verplicht voor overheidsinstanties, maar ook voor organisaties die stelselmatig op grote schaal personen observeren of die op grote schaal bijzondere persoonsgegevens verwerken (zoals medische of strafrechtelijke gegevens). Een lidstaat mag echter zelf de gevallen aanvullen waarin een privacy officer verplicht is.

5. Moet uw organisatie een Privacy Impact Assessment (PIA) uitvoeren?

Wanneer het verwerken van persoonsgegevens, in het bijzonder met behulp van nieuwe technologieën, risico's voor betrokkenen inhoudt, is het uitvoeren van een PIA verplicht. Een PIA is in ieder geval verplicht bij profiling, grootschalige verwerking van bijzondere persoonsgegevens of monitoring van openbare ruimten. In de PIA wordt vastgelegd waarom, op welke manier en hoelang er persoonsgegevens verwerkt worden. Daarbij moeten de aanwezige risico's in kaart gebracht en beoordeeld worden. In sommige gevallen is het zelfs verplicht om de PIA met betrokkenen te bespreken.

6. Wanneer moet uw organisatie verplicht een register bijhouden?

Zowel de verantwoordelijke als de bewerker dient verplicht een schriftelijk (of elektronisch) register bij te houden, waarin alle activiteiten worden omschreven waarbij persoonsgegevens worden verwerkt. In een register dient onder andere het volgende opgenomen te worden:

- contactgegevens
- de doeleinden van de gegevensverwerking;
- een beschrijving van de categorieën van betrokkenen;
- de ontvangers van de gegevens;
- een beschrijving van de beveiligingsmaatregelen;
- en de beoogde bewaartermijnen.

Dit register is niet verplicht voor organisaties met minder dan 250 medewerkers, tenzij er stelselmatig (bijzondere) persoonsgegevens worden verwerkt, of de verwerking een risico voor de betrokkenen inhoudt. Op verzoek van de toezichthouder dient het register aan de toezichthouder overhandigd te worden ter controle.

7. Per wanneer moet uw organisatie voldoen aan de AVG?

Vanaf de officiële publicatie van de AVG geldt er twee jaar overgangsrecht voordat de AVG daadwerkelijk van toepassing is. Naar verwachting is de impact van bovengenoemde hoofdpunten groot en zullen veel organisaties tijdig aan de slag moeten gaan om een basis te leggen voor een goede implementatie.

8. Vragen?

Mocht u naar aanleiding van bovenstaande vragen hebben, of hulp nodig hebben om uw organisatie voor te bereiden op de aankomende verordening? Neem contact met ons op via 020 66 31 941 of info@ictrecht.nl en vraag naar onze privacyspecialisten.