Bescherming van de persoonsgegevens

Tijd om orde op zaken te stellen!

De nieuwe Europese privacywet 'GDPR' - de "Algemene Verordening Gegevensbescherming" in het Nederlands - die op 25 mei 2018 van toepassing wordt, is een opportuniteit voor bedrijven om zich te bezinnen over hoe ze vandaag gegevens bijhouden, hoe ze die gebruiken en hoe het staat met de bescherming ervan.

Deze nieuwe privacywetgeving is gebaseerd op de bestaande wetgeving, maar brengt op enkele vlakken toch een verbetering of uitdieping mee. In het algemeen geldt dat ondernemingen op een redelijke manier met de verwerking van persoonsgegevens om moeten gaan.

De manier waarop dit wordt ingevuld is de verantwoordelijkheid van de onderneming. De onderneming heeft hiertoe een verantwoordingsplicht. Dat houdt in dat een onderneming moet kunnen aantonen welke technische en organisatorische acties zij heeft ondernomen om aan de nieuwe privacywetgeving te voldoen.

De wetgeving gaat in vanaf 25 mei 2018 en geldt voor iedereen die goederen of diensten aanbiedt in de Europese Unie. Vanaf dan moet een onderneming dus kunnen aantonen dat zij voldoet aan de nieuwe wet. Dit gaat zowel over de manier van verzamelen van persoonlijke gegevens als over het opslaan in datacenters of in een cloud buiten de EU. Voor de meeste bedrijven is dit een enorme aanpassing.

Als men niet voldoet aan de GDPR-wetgeving dan hangen er hoge boetes boven het hoofd. Bij een 'lichte schending' kan het gaan over 2% van de jaarlijkse omzet. De maximale boete kan zelfs oplopen tot €20 miljoen of 4% van de jaarlijkse omzet.

In veel gevallen is het voor ondernemingen ook verplicht om een dataregister op te stellen. Hierin maakt men een overzicht van alle persoonsgegevens die men verzamelt en bewerkt. Belangrijk is te vermelden waar de gegevens vandaan komen, en met wie ze gedeeld worden. Gebeurt het toch dat de onderneming geconfronteerd wordt met een datalek, dan is dit document een houvast om te laten zien dat men wel degelijk volgens de regels heeft gewerkt.

De GDPR richt zich op het beschermen van de eindgebruiker. Vaak zie je dat bedrijven talloze nutteloze gegevens (al dan niet bewust) opslaan, die niet relevant zijn voor de diensten die ze aanbieden. De wetgeving staat hier als het ware als scheidsrechter aan de zijlijn om deze gegevens wanneer nodig terug te fluiten.

Om dit onder controle te houden neemt men best het begrip van 'doelbinding' in acht. Dit bepaalt dat de persoonsgegevens die men bezit, verkregen moeten worden met de uitdrukkelijke toestemming van je eindgebruiker.

Ze mogen verder ook niet verwerkt worden op een manier die niet past bij je doeleinden. Bekijk daarom zelf met een kritisch oog of je de gegevens die je verzamelt echt wel nodig hebt.

De GDPR moet allereerst een oplossing bieden voor de vele gegevenslekken die bedrijven de afgelopen jaren geleden hebben. Ondernemingen worden met deze nieuwe regelgeving met hun neus op de feiten gedrukt om bewuster om te gaan met persoonsgegevens. Ze hebben overigens vaak geen idee wat er moet gebeuren wanneer ze geconfronteerd worden met zo'n datalek.

De privacycommissie in België is belast met het onderzoeken en verwerken van datalekken. Deze laatste moeten volgens de nieuwe regelgeving verplicht gemeld worden. De meldingsplicht bedraagt hierdoor nog steeds in principe maximaal 72 uur nadat een gegevenslek werd vastgesteld.

Ronald Tiebout,
Juridisch adviseur UPTR.
E-mail : ronald@uptr.be

GDPR in de praktijk

De GDPR of in het nederlands "algemene verordening gegevensbescherminga" (AVG) zal op 28 mei 2018 van toepassing worden. Onderstaand kan u 12 eenvoudige stappen terugvinden die ervoor zorgen dat u voldoende voorbereid bent zoals voorgesteld door de Commissie voor de Bescherming van de persoonlijke levenssfeer op haar website: www.privacycommission.be.

1. **Bewustmaking**: Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. **Dataregister**: Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. **Communicatie**: Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. **Rechten van de betrokkene**: Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. **Verzoek tot toegang**: Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. **Wettelijke grondslag voor het verwerken van persoonsgegevens**: Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. **Toestemming**: Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. **Datalekken**: Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken. Niet alle datalekken zullen moeten worden gemeld aan de Privacycommissie – enkel deze waarbij het waarschijnlijk is dat de betrokkene enige vorm van schade zal leiden, bv. als gevolg van een identiteitsdiefstal of het schenden van een geheimhoudingsplicht.

9. **Gegevensbescherming door ontwerp en gegevensbeschermingseffectbeoordeling**: Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

10. **Functionaris voor gegevensbescherming**: Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.De AVG vereist voor sommige bedrijven en organisaties dat zij een functionaris voor gegevensbescherming aanwijzen, bijvoorbeeld voor openbare overheden of verwerkers wiens taak bestaat uit het regelmatig en stelselmatig observeren van betrokkenen op grote schaal.

11. **Internationaal**: Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

12. **Bestaande contracten**: Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

Bron : Commissie voor de bescherming van de persoonlijke levenssfeer