De Algemene Verordening Gegevensbescherming

Of

General Data Protection Regulation (GDPR)

Wat verandert er echt?

Vanaf 25 mei 2018 gaat een nieuwe privacywet voor heel Europa in: de Algemene Verordening Gegevensbescherming (AVG).

Een nieuwe privacywet voor heel Europa, dat is wat de Algemene Verordening Gegevensbescherming (AVG) ons brengt. Vanaf 25 mei 2018 moeten alle bedrijven voldoen aan deze strenge nieuwe wet. Wat gaat er nu allemaal veranderen?

1) Uw activiteiten vallen veel sneller onder de privacywet. Het centrale begrip 'persoonsgegevens' verandert namelijk: naast bestanden met namen, adressen en dergelijke vallen nu ook gegevens gekoppeld aan IP-adressen, MAC adressen, cookies en dergelijke onder de wet. Ook als u niet weet hoe de persoon achter een cookie heet, dient u dat gegeven te behandelen als privacygevoelig.

2) Uw privacyverklaring moet nóg transparanter. U moet in eenvoudige taal precies en volledig uitleggen wat u doet met persoonlijke gegevens. Ook moet u mensen wijzen op hun rechten, zoals dat men gegevens mag aanpassen, het dossier mag inzien of zelfs laten vernietigen. Bouwt u interesseprofielen op, dan moeten die op verzoek kunnen worden verwijderd. Bovendien moet u ze wijzen op de mogelijkheid een klacht in te dienen bij de toezichthouder, de Gegevens Beschermings Autoriteit (GBA) voorheen de Autoriteit Persoonsgegevens.

3) Alle datalekken moeten intern worden gedocumenteerd. Volgens de huidige privacywet hoeft u alleen datalekken bij te houden wanneer u ze ook moet melden aan de toezichthouder. De AVG stelt het verplicht om alle datalekken intern te documenteren, óók datalekken die niet te hoeven worden gemeld. En verwerkt u privacygevoelige data voor uw opdrachtgevers?
Dan bent u straks wettelijk verplicht alle datalekken daarbij aan hen te melden, zodat zij dit weer aan de toezichthouder kunnen melden. De tijd tussen het constateren van een datalek en het melden aan de GBA mag maximaal 72 uur bedragen.

4) U moet alle verwerkingen van persoonlijke gegevens documenteren, ook de triviale zoals uw personeelsadministratie of de nieuwsbrief. In dit register moet onder andere staan welke persoonsgegevens er verwerkt worden, voor welke doeleinden, en hoe deze gegevens beveiligd worden. Voor meer informatie over het verwerkingsregister kunt u met ons contact opnemen.

5) De boetes worden gigantisch. De maximale boete per overtreding van de huidige privacywet is nu 900.000 euro. Dit verandert met de komst van de AVG naar 20 miljoen euro of 4% van

de wereldwijde jaaromzet. Bovendien komt er komt een Europees Comité dat toeziet op de juiste toepassing van de AVG.

6) U moet met al uw leveranciers en afnemers een zogeheten verwerkersovereenkomst sluiten waarin u specifieke afspraken maakt over de omgang met persoonlijke gegevens. Een belangrijk aandachtspunt daarbij is dat wanneer u diensten uitbesteedt waarbij persoonsgegevens van een klant zijn betrokken, u hiervoor toestemming nodig hebt van die klant.

7) Mogelijk heeft u een privacy officer nodig. Een privacy officer, oftewel functionaris voor gegevensbescherming (FG), is een onafhankelijke persoon binnen de organisatie die adviseert en rapporteert over naleving van de AVG. Deze is verplicht wanneer u op grote schaal gevoelige persoonsgegevens zoals gezondheidsgegevens verwerkt, of als u structureel mensen observeert (fysiek of digitaal). Een FG kan iemand zijn die intern aangesteld wordt, maar mag ook iemand zijn die extern aangesteld wordt, zoals een Data Protection Officer (DPO) van Pro-ictief.

8) Zitten er risico's aan een verwerking, dan moet u een complete Privacy Impact Assessment (PIA) uitvoeren. Dit is een uitgebreid onderzoek om privacyrisico's in kaart te brengen en deze zo veel mogelijk weg te nemen. Pas nadat de PIA is uitgevoerd en de resultaten geïmplementeerd, mag u die risicovolle verwerking uitvoeren. Meer informatie vindt u in onze checklist over de PIA.

9) U moet zo min mogelijk privacygevoelige informatie verzamelen en deze zo snel mogelijk weer weggooien. Vanuit de gedachte van risicobeheersing vereist de AVG dat u het minimale aan persoonsgegevens onder u heeft. U moet dus actief informatie weggooien wanneer deze niet meer relevant is – en u moet beleid hebben dat uitwerkt wanneer iets wel of niet relevant is, en hoe het weggooien dan veilig wordt gerealiseerd.

10) Uw software en diensten moeten van de grond af rekening houden met privacy, Dit wordt ook wel 'Privacy by design' en 'Privacy by default' genoemd. Kort gezegd moet bij elke stap in de ontwikkeling de privacyaspecten worden benoemd en meegenomen in de uitwerking. Daarnaast moeten standaardinstellingen van een nieuwe dienst zo privacy vriendelijk mogelijk zijn.

11) Uw beveiliging moet op orde zijn – en blijven. Beveiliging van persoonlijke gegevens is cruciaal vandaag de dag. Zonder encryptie, tweefactorauthenticatie en het kunnen scheiden en veilig wissen van persoonlijke informatie neemt u een zeer groot risico. Verder zullen uw ICT-systemen regelmatig moeten worden onderzocht op nieuwe risico's.

12) U dient intern privacybeleid te publiceren waarin staat wie welke rol heeft bij de omgang met persoonsgegevens. Het is belangrijk dat medewerkers hiervan op de hoogte zijn. Zij moeten dus worden getraind, en dit moet regelmatig worden herhaald.

13) U moet kunnen omgaan met verzoeken van personen, zoals een verzoek om inzage of correctie in hun gegevens. Maar wanneer u verouderde gegevens heeft moeten deze worden gewist op verzoek. Een verzoek van een betrokkene over zijn persoonsgegevens moet normaal binnen een maand inhoudelijk afgehandeld zijn. Is uw helpdesk hier al op ingericht?

14) Heeft u online diensten waarin mensen persoonlijke informatie opslaan? Dan moeten zij in staat zijn al hun informatie te kunnen exporteren in een standaardformaat, zodat zij die naar een andere organisatie kunnen overdragen. Denk aan downloaden van foto's, social media berichten of forumbijdragen.

15) Werkt u met buitenlandse partijen, controleer dan of zij binnen of buiten de EU persoonlijke informatie voor u opslaan. Dat laatste is alleen toegestaan als er wordt voldaan aan strikte regelgeving, bijvoorbeeld als het land in kwestie door de Europese Commissie gecertificeerd is. De VS is dat: het zogeheten Privacy Shield biedt de nodige waarborgen voor gebruik van Amerikaanse partijen. Maar let op: uw klanten kunnen van u eisen dat data gewoon in het geheel niet de EU verlaat.

16) Maakt u interesseprofielen of risicoanalyses van uw klanten, bezoekers et cetera? Dan moet u hen op verzoek kunnen uitleggen hoe dat gebeurt en wat u daarmee doet. Dit speelt al bij het gebruik van cookies voor advertentiedoeleinden.

17) Maakt uw organisatie gebruik van vingerafdrukken of biometrie, bijvoorbeeld voor toegangsbeveiliging? Dit ligt gevoelig onder de AVG, omdat dergelijke biometrische gegevens een streng beschermingsregime genieten.

Wilt u meer weten over hoe Pro-ictief u kan helpen om AVG / GDPR compliant te worden?

Neem dan contact op met ons per mail info@pro-ictief.nl of telefoon +31 (0)495 566 202