White Paper

De nieuwe Privacywet ofwel AVG. Hoe er aan te voldoen?

ID Control
The European Privacy Company

Algemene Verordening Gegevensbescherming

De bestaande regels rondom de bescherming van persoonsgegevens zijn aangescherpt met de invoering van de Algemene Verordening Gegevensbescherming (AVG), in het Engels GDPR genoemd (General Data Protection Regulation). Iedere organisatie krijgt met de AVG te maken, omdat vrijwel iedere organisatie persoonsgegevens van klanten en/of werknemers verwerkt. Op 25 mei 2018 moet de verwerking van persoonsgegevens aan de AVG voldoen. In deze white paper zijn de belangrijkste gevolgen voor de organisatie samengevat en wordt ook een handvat gegeven om de databeveiliging goed in te richten.

Wat gebeurt er als de AVG niet wordt nageleefd?

De gevolgen voor het niet naleven van de AVG kunnen veel groter zijn dan nu het geval is onder de Privacyrichtlijn en de Wbp. De maximale boete bedraagt op dit moment € 4.500,-; in 2018 kan de toezichthouder op dit terrein (Autoriteit Persoonsgegevens) boetes opleggen die oplopen tot 4% van de jaaromzet of maximaal € 20 miljoen. Per overtreding! Daarnaast wilt u niet dat uw bedrijfsgeheimen op straat liggen.

Welke gegevens gelden als persoonsgegevens?

Elk gegeven dat kan worden herleid naar een levend mens, is een persoonsgegeven. Bijvoorbeeld de naam, adres, woonplaats. Door de wetgever zijn gevoelige persoonsgegevens extra beschermd zoals: ras, godsdienst of gezondheid.

Wat is zorgvuldige verwerking?

Uitgangspunt onder de AVG blijft de verplichting om persoonsgegevens zorgvuldig en in overeenstemming met de wet te verwerken. De AVG schept een aantal verplichtingen bij het verwerken van persoonsgegevens die hierna op hoofdlijnen zullen worden besproken. Wanneer uw organisatie wil weten waar zij op dit moment staat kan zij kiezen om een PIA (privacy impact analyse) te laten uitvoeren. Dit is een instrument om van voorgenomen regelgeving of projecten, waarbij persoonsgegevens worden verwerkt, de effecten voor betrokkenen in kaart te brengen en te beoordelen.

ID Control – The European Privacy Company
Tel. +31 (0) 888 SECURE (732873) http://www.idcontrol.com

Registratie- en documentatieplicht

Alle organisaties zijn straks verplicht om aan de toezichthouder, de AP, te kunnen laten zien dat ze “privacy (AVG) compliant” zijn. Een organisatie zal met documenten moeten aantonen dat passende maatregelen zijn genomen. Belangrijk hierbij zijn een bedrijfsbreed informatiebeveiligingsbeleid waarbij aandacht is voor de technische (bijv. backup & restore plan, identity & access management) maar ook de organisatorische (menskant) van de risicobeheersing (bijv: security awareness, Incident response procedure, en Bring Your Own Device beleid).

Deze registratie- en documentatieplicht geldt dus ook voor uw personeelsadministratie en klantenadministratie!

Tot slot dient u aan privacy by design en privacy by default te doen bij het ontwerpen van software. Hetgeen inhoudt dat (web-)formulieren, invulmenu’s etc. privacybeschermend staan ingesteld en geen overbodige informatie gevraagd wordt (data minimalisatie).

Verwerkersovereenkomst en verwerkingsregister

Wanneer uw organisatie gebruik maakt van een andere partij bij de verwerking van persoonsgegevens, zoals een salarisverwerker, een administratiekantoor of een hosting provider voor opslag van gegevens in de cloud dan is het sluiten van bijvoorbeeld een verwerkersovereenkomst met een salarisverwerker of een administratiekantoor verplicht. Een verwerkersovereenkomst wordt gemaakt tussen de verantwoordelijke (werkgever) en de verwerker (salarisverwerker, administratiekantoor etc.) waarin wordt vastgelegd hoe de verwerker met de persoonsgegevens moet omgaan. Ook moet de organisatie (en elke verwerker van persoonsgegevens) een verwerkingsregister bijhouden. Hierin staat onder andere: contactgegevens van de verantwoordelijken, verwerkers en naam van de FG (DPO), de doeleinden van de verzameling en de categorieën van de persoonsgegevens; de betrokkenen en de ontvangers. Ook bevat het register een algemene beschrijving van de beveiligingsmaatregelen.

Inzagerecht van o.a. werknemers en klanten:

- om hun personeelsdossier in te zien;
- een kopie van hun personeelsdossier in een standaardformaat te ontvangen (bijv als pdf-bestand);
- hij/ zij heeft het recht om begrijpelijke informatie te krijgen over het hoe en waarom van de verwerking, zijn/haar rechten en het privacybeleid van de organisatie;
- te allen tijde gratis de gegevens die op hen betrekking hebben inzien en, indien nodig, aan laten passen of te wissen (bijvoorbeeld vanwege het recht op vergetelheid).

De werkgever is straks, op straffe van een boete, verplicht alle gevraagde informatie te verschaffen.

Technisch datalekken voorkomen

Wanneer uw organisatie kan aantonen dat zij aan alle bovenstaande zaken voldoet is zij er echter nog niet. De wet verlangt ook dat u technische maatregelen treft. De wetgever heeft ingezien dat een organisatie ook technisch passende maatregelen moet nemen om de data te beveiligen. Een handig hulpmiddel hierbij is de zogenaamde AVG-Gap analyse, maar ook een penetratietest om uw organisatie eens digitaal door te lichten op zoek naar kwetsbaarheden.

Bij technische maatregelen kan gedacht worden aan het volgende:

Secure netwerk en toegang	Secure Data	Secure identiteits- en toegangsmanagement	Secure Apparaten	Secure E-mailen
Unified threat management (UTM)	Veilig data delen, collaboreren en opslaan	VPN	Mobile device management	Verzegeld en aangetekend e-mail verzenden
Security Operation Center	Back-up en herstel	Sterke authenticatie, eenmalig wachtwoord via: SMS, app, of token	Endpoint beveiliging	Automatisch beveiligd archiveren
Controle op (draadloze) netwerktoegangen		Autorisatiemanagement	Kwetsbaarheidsanalyses	

ID Control – The European Privacy Company
Tel. +31 (0) 888 SECURE (732873) http://www.idcontrol.com

FG/DPO as a service

Sommige organisaties zijn verplicht om een Functionaris Gegevens-bescherming (FG) in dienst te hebben, ook wel Data Protection Officer (DPO) genoemd. Het inhuren van een FG is raadzaam bij het implementeren van de AVG, als project. Het voordeel is dat een FG een brede scope heeft die ervoor zorgt dat alle aspecten van AVG compliancy de verdiende aandacht krijgen (juridisch, organisatorisch en technisch).

Conclusie

Organisaties moeten een overzicht van alle verwerkingen van persoons-gegevens gaan bijhouden en aantonen dat de passende **(organisatorische en technische)** maatregelen zijn genomen ter wille van de bescherming van de privacygevoelige persoonsgegevens.
We leven in een tijd van toenemende privacy bewustzijn en privacy zorg. In de pers verschijnt bijna dagelijks een bericht over hacking, lekken of privacy. Uw organisatie wilt daar niet tussen staan. Niet als het gaat om een datalek persoonsgegevens en ook niet vanwege het verlies van bedrijfsgevoelige informatie (imagoschade). Sterker, organisaties kunnen een voorsprong nemen door privacy en databeveiliging serieus te nemen!

Maak dus snel werk van het inrichten van een veilige data omgeving en bescherm uw gegevens!

ID Control – The European Privacy Company
Tel. +31 (0) 888 SECURE (732873) http://www.idcontrol.com