# Whitepaper

## 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 worden aangescherpt met de invoering van de Algemene Verordening Gegevensbescherming (AVG), in het Engels General Data Protection Regulation (GDPR) genoemd. Iedere organisatie krijgt met de AVG te maken, omdat vrijwel iedere organisatie persoonsgegevens van klanten, leveranciers of werknemers verwerkt. Op 25 mei 2018 moet de verwerking van persoonsgegevens aan de AVG voldoen. In deze whitepaper zijn de belangrijkste gevolgen voor de organisatie samengevat en wordt ook een handvat gegeven om dit op orde te krijgen.

## 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 Wet Bescherming Persoonsgegevens (WPB). De maximale boete bedraagt op dit moment € 4.500,- maar in 2018 kan de toezichthouder Autoriteit Persoonsgegevens (AP) boetes opleggen die oplopen tot 4% van de jaaromzet, of € 20 miljoen, maar net welk bedrag het hoogste is.

## Welke gegevens gelden als persoonsgegevens?

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

## Wat is zorgvuldige verwerking?

Uitgangspunt van de AVG is de verplichting om persoonsgegevens zorgvuldig en in overeenstemming met de wet te verwerken. De AVG schept hierbij een aantal verplichtingen die hierna op hoofdlijnen worden besproken. Wanneer uw organisatie wil weten waar zij op dit moment staat kan zij een Privacy Impact Analyse (PIA) 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 op impact in geval van een datalek.

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

## Registratie- en documentatieplicht

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

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

Tot slot dient uw organisatie aan ‘privacy by design’ en ‘privacy by default’ te doen. Dit houdt in dat bijvoorbeeld (web-)formulieren en invulmenu’s etc. Privacybeschermend staan ingesteld en dat geen overbodige informatie gevraagd wordt (data minimalisatie).

## Verwerkersovereenkomst en verwerkingsregister

Wanneer uw organisatie gebruik maakt van een andere partij bij de verwerking van persoonsgegevens (verwerker), zoals een salarisverwerker, administratie-kantoor of een hosting provider voor opslag van gegevens, dan is het sluiten van een verwerkersovereenkomst met deze partij verplicht. Een verwerkers-overeenkomst wordt opgesteld tussen de verantwoordelijke (opdrachtgever) en de verwerker. Hierin wordt vastgelegd hoe de verwerker met de persoons-gegevens moet omgaan.

Ook moeten zowel opdrachtgever als verwerker een verwerkingsregister bijhouden. Hierin staan onder andere de contactgegevens van opdrachtgever en verwerker, verantwoordelijke personen voor data, de naam van de Functionaris Gegevensbeveiliging (FG) als die verplicht is, doeleinden van gegevensverzameling en categorisering van persoonsgegevens. Ook staat hierin een algemene beschrijving van de beveiligingsmaatregelen.

## Inzagerecht van o.a. werknemers en klanten:

- Personeelsdossier;
- Een kopie van hun personeelsdossier in een standaardformaat (bijv als pdf-bestand);
- 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 te laten passen of te laten wissen (bijvoorbeeld vanwege het recht op vergetelheid).

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

## Technisch datalekken voorkomen

De wet verlangt dat uw organisatie technische passende maatregelen neemt om privacy gevoelige data te beveiligen. Handige hulpmiddelen hierbij zijn bijvoorbeeld een zogenaamde AVG-Gap analyse en een penetratietest om uw organisatie digitaal door te lichten op zoek naar beveilingsproblemen.

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 (bijv. printers) | Automatisch beveiligd archiveren |
| Controle op (draadloze) netwerktoegangen | | Autorisatiemanagement | Kwetsbaarheidsanalyses | |

**ID Control – The European Privacy Company**
Tel. +31 (0) 888 SECURE (732873) 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 de AVG bekeken worden (juridisch, organisatorisch en technisch).

## Conclusie

Organisaties moeten een overzicht van alle verwerkingen van persoons-gegevens gaan bijhouden en aantonen dat passende (organisatorische en technische) maatregelen zijn genomen om de bescherming van privacy-gevoelige persoonsgegevens te borgen.

We leven in een tijd waarin we ons steeds bewuster worden van privacy en de problematiek rondom het beschermen van privacy. Bijna iedere dag is er in de kranten en op het internet wel iets te lezen over een hack, een data lek of privacy schending. Uw organisatie wil toch niet tussen die berichten staan? Afgezien van al het werk en de ellende rondom datalekken lijdt uw organisatie dan mogelijk ook imagoschade. Door privacy en data-beveiliging serieus te nemen kunt u dit voorkomen en zelfs een voorsprong opbouwen ten opzichte van uw concurrenten!

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