AVG

ALGEMENE VERORDENING GEGEVENS-BESCHERMING

MOJA RADA

SPECIALIST PRIVACYWETGEVING

In Nederland was er al de Wet bescherming persoonsgegevens, waarna de Meldplicht datalekken werd toegevoegd. Maar sinds 2018 hebben we, samen met 27 andere landen in de Europese Unie, een gezamenlijke wet- en regelgeving op het gebied van privacy.

Globalisering, het in razend tempo ontwikkellen van nieuwe technologieën en het voor uiteenlopende doeleinden verwerken van data door bedrijven en organisaties, ligt hier aan ten grondslag. Daarom is per 25 mei 2018 een vervangende, Europese regelgeving van kracht: de General Data Protection Regulation (GDPR) - AVG, de Algemene verordening gegevensbescherming, in het Nederlands. Hiermee wordt de privacy van alle EU/EER-burgers beter beschermd.

De tijd tot 25 mei 2018 werd gezien als een overgangsperiode. Momenteel is het 2020. Voldoet u inmiddels al aan de AVG?

De nieuwe wetgeving

Eén van de verantwoordelijkheden binnen de AVG is, dat u als bedrijf een verantwoordingsplicht heeft. Dit betekent dat u verplicht bent om de gegevensverwerking in kaart te brengen. Welke persoonsgegevens verwerkt u? Met welk doel? Waar komen de gegevens vandaan en met wie deelt uw bedrijf de gegevens? Overtreedt uw bedrijf de AVG, dan kan de Autoriteit Persoonsgegevens u een boete opleggen. Deze kan oplopen tot maximaal 20 miljoen euro of 4 procent van de wereldwijde omzet.

Kortom: reden genoeg om goed voorbereid te zijn.

Welke voorbereidingen kunt u treffen om te voldoen aan de AVG?

1. Verwerkingen - Artikel 30
Register van verwerkingsactiviteiten

Houd een register van verwerkingsactiviteiten bij. Wanneer uw organisatie meer dan 250 medewerkers heeft bent u hier zelfs toe verplicht. Ook bent u hiertoe verplicht als uw organisatie minder dan 250 medewerkers heeft, maar u persoonsgegevens verwerkt die een hoog risico inhouden voor de rechten en vrijheden van personen. Dit is ook van toepassing als u bijzondere persoonsgegevens verwerkt, zoals gegevens over godsdienst, gezondheid, politieke voorkeur of strafrechtelijke gegevens.
Een verwerkingsregister bevat per verwerking het doel en de aard van de verwerking, de getroffen beveiligingsmaatregelen en wie verantwoordelijk is.

2. Maatregelen in beveiliging - Artikel 32
Beveiliging van de bewerking

Pas technische en organisatorische maatregelen toe, zoals pseudonimering en versleuteling. Zorg ook voor een beschrijving van deze maatregelen zoals die zijn gerealiseerd. Hiermee waarborgt u de beveiliging van systemen en de daarmee verwerkte persoonsgegevens. Richt een managementcyclus (zoals de PDCA-cyclus) in waarbij zo nodig optimalisaties worden doorgevoerd.

3. Categorisering van persoonsgegevens - Artikel 9
Verwerking van bijzondere categorieën van persoonsgegevens

Geef aan wat de gevoeligheden van de verwerkte persoonsgegevens zijn en welke risico's hiermee gemoeid zijn voor de betrokkenen. Dit is van toepassing wanneer u persoonsgegevens verwerkt waaruit bijvoorbeeld geslacht, leeftijd, etniciteit of economisch welzijn blijken.

4. Data Protection Impact Assessment - Artikel 35
Gegevensbeschermingseffectbeoordeling

Voer een DPIA - een Data Protection Impact Assesment - uit. Bedrijven die een hoog privacyrisico lopen zijn zelfs verplicht om een DPIA uit te voeren en eventueel maatregelen te nemen. Een hoog risico loopt u onder meer als u op grote schaal gevoelige persoonsgegevens verwerkt, of individuen profileert, of als u in een publiek gebied cameratoezicht houdt.

Bij de risicoanalyse toetst u periodiek eventuele interne privacy problemen en brengt u deze in kaart. Beoordeel of de getroffen maatregelen nog in lijn zijn met de AVG en met alle privacy principes en risico's. Toets ook of de doelstelling van de verwerking behaald kan worden via andere wegen, of met minder persoonsgegevens. Voer bij gewijzigde omstandigheden of wijzigingen in systemen opnieuw een DPIA uit.

5. Privacy by Design of Privacy by Default - Artikel 25
Gegevensbescherming door ontwerp en door standaardinstellingen

Houd rekening met Privacy by Design en Privacy by Default.

Privacy by Design
Met Privacy by Design besteedt u bij de ontwikkeling van nieuwe informatiesystemen, maar ook bij wijzigingen, ten eerste aandacht aan privacy verhogende maatregelen. Ten tweede houdt u rekening met dataminimalisatie: u verwerkt zo min mogelijk persoonsgegevens, dat wil zeggen: alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Op deze manier kunt u een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen. Daarbij moeten systemen voor ingebruikname naar de laatste stand van de techniek zijn beveiligd.

Privacy by Default
Met Privacy by Default neemt u zowel technische als organisatorische maatregelen om ervoor te zorgen dat u alleen de persoonsgegevens bewaart die noodzakelijk zijn. Bijvoorbeeld door bij het laten abonneren op een nieuwsbrief niet meer gegevens vragen dan nodig is, of bij een app geen gebruik te maken van locatiegegevens als deze gegevens niets toevoegen.

6. Functionaris voor de gegevensbescherming / Data Protection Officer - Artikel 37
Aanwijzen van de functionaris voor de gegevensbescherming

Stel een functionaris voor de gegevensbescherming (FG) aan. Overheidsinstanties en publieke organisaties zijn altijd verplicht om dit te doen. Ook wanneer uw organisatie op grote schaal individuen volgt, bijvoorbeeld door profilering van mensen voor het inschatten van risico's, moet u een FG aanstellen.

7. Datalekken

Implementeer, passend bij uw organisatie, maatregelen om beveiligingsincidenten te detecteren en de gevolgen daarvan te beperken. Zorg voor documentatie van eventuele incidenten.

Melden datalek bij autoriteiten – Artikel 33
Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

De AVG stelt strengere eisen aan het melden van datalekken. Zo bent u als organisatie verplicht om alle datalekken te documenteren. Dus niet alleen de datalekken waar een melding van is gemaakt.

Richt een procedure Meldplicht datalekken in waarmee datalekken worden gedetecteerd en uiterlijk binnen 72 uur aan de Autoriteit Persoonsgegevens worden gemeld. Zorg ook voor documentatie van eventuele datalekken.

Melden datalek bij betrokkenen – Artikel 34
Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene

Pas een procedure toe waarmee betrokkenen - indien een datalek voor deze betrokkenen nadelige gevolgen heeft - direct geïnformeerd kunnen worden over een gesignaleerd datalek.

Tot slot

Bewustwording
Het traject begint met bewustwording. Welke medewerkers binnen de organisatie moeten op de hoogte zijn van de privacyregels? Wat is de impact op de organisatie en wat moet er binnen het bedrijf gebeuren om te voldoen aan de AVG? Maak verwerkingen en beschermingsmaatregelen transparant en overweeg om stakeholders gedurende, maar ook na afloop van het traject, periodiek te informeren over de gerealiseerde beveiliging van persoonsgegevens en de eventuele DPIA-rapportages.

Rechten van betrokkenen
De personen van wie uw bedrijf de persoonsgegevens verwerkt (de 'betrokkenen'), hebben vanaf 2018 verbeterde, maar ook meer rechten, zoals het recht op dataportabiliteit. Dit betekent dat zij het recht hebben om de persoonsgegevens te ontvangen die uw bedrijf van hen heeft. Hier kunt u uiteraard nu alvast rekening mee houden.

Verwerkersovereenkomsten
Besteedt uw organisatie de gegevensverwerking uit aan een derde partij, ofwel een verwerker? Bekijk in dat geval of de huidige contracten voldoen aan de eisen van de AVG. Zo niet, dan is het noodzakelijk om hier nieuwe afspraken over te maken en deze vast te leggen. In het geval dat uw bedrijf zelf verwerker of subverwerker is, zorgt u natuurlijk ook voor nieuwe contracten met de verwerkingsverantwoordelijke.

Leidende toezichthouder
Heeft uw organisatie vestigingen in meerdere lidstaten van de EU of is de gegevensverwerking van invloed op meerdere lidstaten? In dat geval hoeft u volgens de AVG maar met één privacytoezichthouder, de leidende toezichthouder, zaken te doen.

Toestemming
De AVG zorgt wat betreft persoonsgegevens voor strengere eisen aan het verkrijgen van toestemming van derden. Zo moet u verplicht aan kunnen tonen dat u toestemming hebt gekregen om deze gegevens te verwerken. Ook nieuw is dat betrokkenen deze toestemming net zo gemakkelijk weer kunnen intrekken.

Disclaimer: de inhoud van dit artikel dient enkel ter informatie en niet als juridisch advies

Bovenstaand overzicht geeft de belangrijkste eisen uit de AVG weer. Wilt u zeker zijn dat u voldoet aan de AVG? Neem dan gerust contact op voor advies.

Henk van Leussen
Specialist privacywetgeving

henk.vanleussen@mojarada.nl
+31 6 20 44 13 48

mojarada.nl