PRIVACY

Algemene Verordening Gegevensbescherming

BMGRIP

Een uitdaging voor iedereen

In een wereld die digitaliseert wordt privacy steeds belangrijker. Big data is big business. Tegenwoordig staan bijna alle gegevens digitaal opgeslagen. Ze worden zelfs regelmatig verhandeld en zijn volgens experts het nieuwe goud. Heeft u als burger eigenlijk nog wel controle over uw eigen data?

Van sommige zaken bent u zich bewust. De huisarts weet of u gezond bent en de bank ziet hoeveel geld er op uw rekening staat. Maar dagelijks staat u er waarschijnlijk niet bij stil dat de NS weet welke trein u neemt, de Albert Heijn ziet welke boodschappen u doet en dat uw telefoon aan apps doorgeeft waar u bent. De Europese Unie wil inwoners beter beschermen tegen de macht van dataverzamelaars en het misbruiken van data. En dus komt er een nieuwe wet: de Algemene Verordening Gegevensbescherming (AVG).

Voor wie geldt het?

Een ander groot verschil met de WBP is dat het begrip ‘persoonsgegevens’ is uitgebreid. Niet alleen een combinatie van naam, adres of telefoonnummer, maar ook computergegevens zoals IP-adressen en cookies ziet de AVG als persoonsgegevens. Met een bedrijfswebsite krijgt u dus al met de wetgeving te maken. Waarschijnlijk beschikt u als ondernemer ook over BSN-nummers en personeelsdossiers van medewerkers. Kortom, er zijn wel degelijk een aantal punten af te vinken voordat een organisatie AVG-proof is. Nu al nieuwsgierig hoe goed u bent voorbereid? Vul dan meteen de checklist in.

Wat is de AVG?

De AVG is de nieuwe privacywet die op 25 mei 2018 de huidige Wet Bescherming Persoonsgegevens (WBP) vervangt. De AVG is in vergelijking met de WBP een stuk strenger voor organisaties. Ook zijn de boetes hoger. Die kunnen oplopen tot 20 miljoen of 4% van de omzet.

De nieuwe wet is lastig in een paar zinnen samen te vatten. Dit zijn de belangrijkste veranderingen:

- De reden waarom u gegevens vastlegt moet helder zijn.
- De burger moet actief en ondubbelzinnig toestemming geven voor de vastlegging
- De burger heeft veel meer rechten, o.a. inzage, wijzigen, overdragen en verwijderen
- Alles wat u doet met persoonsgegevens moet aantoonbaar vastgelegd zijn
- U mag alleen maar gegevens vastleggen en bewaren die u actief nodig heeft
- De informatiebeveiliging moet up-to-date zijn én blijven.
- Actieve interne communicatie over de omgang met persoonsgegevens is van belang
- Wanneer externe partijen persoonsgegevens verwerken waar u verantwoordelijk voor bent moet dat worden vastgelegd in een overeenkomst

Er verandert dus veel. Met name de wijze van verkrijging, registratie van het gebruik en de beveiliging van gegevens hebben een stevige impact op een organisatie.

Wat zegt de AVG nog meer?

Naast de expliciete toestemming voor het opslaan van informatie is er nog een aantal belangrijke to-do's voor ondernemers. De verzamelde informatie dient het doel van de organisatie direct te ondersteunen. Oftewel, als organisatie moet u kunnen uitleggen waarom u naar informatie vraagt en waar u dat voor gebruikt. Bovendien wijst u de burger daarbij altijd expliciet op zijn rechten.

Informatiebeveiliging

Tevens dient u de informatie goed te beschermen, bijvoorbeeld via encryptie en twee-factor-authenticatie. Bij zowel de huidige als toekomstige ICT-systemen dienen de begrippen privacy by default en privacy by design centraal staan. Kortgezegd betekent dit dat de ICT-omgeving standaard is ingericht om persoonsgegevens op de juiste wijze vast te leggen én te beschermen.

Verwerkingsregister

Naast het secuur vastleggen en beveiligen van gegevens dienen sommige organisaties overzichtelijk te hebben wat voor soort persoonsgegevens ze verwerken. Ze leggen dat vast in een speciaal register. Het zogeheten verwerkingsregister. Wat dat precies inhoudt hebben we uitgelegd in het stappenplan. Organisaties met meer dan 250 werknemers én organisaties die structureel bijzondere persoonsgegevens verwerken dienen zo'n register op te stellen.

Verwerkingsovereenkomst

Afspraken met klanten en leveranciers over de persoons-gegevens dienen ook zwart op wit te staan in een zogenaamde verwerkersovereenkomst. Daarin dient onder andere te worden vastgelegd wat er wordt verwerkt, met welk doel, hoe de beveiliging is geregeld, wat er na afloop gebeurt met de gegevens en wie er eindverantwoordelijk is en wie slechts verwerker.

Datalek

De registratie van datalekken gaat verder dan voorheen. Alle situaties waarbij persoonsgegevens op verkeerde plaatsen terecht is gekomen moeten geregistreerd worden. Tevens dienen de incidenten altijd intern gecommuniceerd te worden.

Privacy officer

Wanneer u als organisatie op grote schaal bijzondere persoonsgegevens verwerkt, dient u een privacy officer aan te stellen. Dit is het interne aanspreekpunt voor alle vragen rondom persoonsgegevens. De privacy officer ziet toe op naleving van de AVG. Het is iemand die bijvoorbeeld jaarlijks een privacy impact assessment (PIA) uitvoert. De PIA is een uitgebreide privacychecklist die helpt om in kaart te brengen hoe er binnen de organisatie wordt omgegaan met persoonsgegevens.

Niks doen is geen optie

Met niks doen riskeert een organisatie hoge boetes. De Autoriteit Persoonsgegevens (AP), de Nederlandse toezichthouder op de AVG, heeft aangegeven strenger te gaan toezien op al het bovenstaande. Bovendien zijn de boetes verhoogd. Zoals eerder aangegeven kunnen deze oplopen tot 20 miljoen of 4% van de jaaromzet: het hoogste bedrag telt.

Goed voorbereid zijn op de AVG betekent:

- Organisatorisch een aantal maatregelen nemen en zaken uitgebreid vastleggen
- Juridisch verschillende documenten en processen checken,
- EN technische aanpassingen doorvoeren op het gebied van informatiebeveiliging

Voldoen aan de AVG is impactvol voor veel organisaties. Aan de andere kant zien we ook dat wanneer de organisatie een gestructureerde aanpak volgt en de juiste tools en templates gebruikt, het binnen afzienbare tijd goed en duurzaam te regelen is.

Aan de slag?

Wilt u weten wat u moet doen om AVG-proof te worden?
Download hier onze toolbox. Met een aanpak, diverse templates en to-do-lijsten.

Samen oppakken

Mocht u het liever samen willen doen, vul dan onze checklist in. Met die informatie kunnen we u binnen één werkdag een vrijblijvende offerte toesturen met informatie en een aanpak die aansluit op uw specifieke situatie.

BMGRIP heeft uitgebreide ervaring, kennis en systemen om hierbij te helpen. Daarbij is onze ervaring dat we veel organisaties binnen twee maanden en een beperkte inzet van ons AVG-proof kunnen krijgen.

BMGRIP
Computerweg 22
3542 DR Utrecht
030 - 755 53 55

info@bmgrip.nl,
www.bmgrip.nl

Versie juni 2022