HOUTHOFF

STAPPEN OP WEG NAAR COMPLIANCE MET DE AVG

DE AVG

Sinds 25 mei 2018 is de Europese Algemene Verordening Gegevensbescherming (Verordening 2016/679, "AVG") van toepassing. De AVG is inwerking getreden in plaats van de Europese Privacyrichtlijn uit 1995 en heeft grotendeels de wettelijke kaders van nationale lidstaten voor het verwerken van persoonsgegevens vervangen. Hoewel de AVG deels overeenstemt met de Privacyrichtlijn, zijn er een aantal belangrijke nieuwe onderwerpen. Deze brochure behandelt de belangrijkste nieuwe onderwerpen in de AVG, de beginselen voor het verwerken van persoonsgegevens en de verschillende stappen die een organisatie moet nemen om te kunnen voldoen aan de AVG.

NIEUWE BELANGRIJKE ONDERWERPEN

- Boetes voor overtredingen, oplopend tot 20 miljoen euro of 4% van de jaarlijkse wereldwijde omzet
- Nieuwe rechten voor betrokkenen, zoals het 'recht op vergetelheid' en 'dataportabiliteit'
- Meldplicht datalekken (een variant hierop bestond reeds in Nederland sinds 2016)
- Gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment)
- Aanvullende eisen voor het inschakelen van verwerkers
- Aanvullende eisen aan privacyverklaringen
- Meer uitgebreide eisen aan transparantie richting betrokkenen
- Verantwoordingsplicht: vereiste om aan te tonen dat wordt voldaan aan de AVG

TOEPASSELIJKHEID OP ORGANISATIES BUITEN DE EU

Het territoriale toepassingsbereik van de AVG is uitgebreid ten opzichte van de Privacyrichtlijn. Net zoals de Privacyrichtlijn is de AVG van toepassing op de verwerking van persoonsgegevens die plaatsvindt in het kader van de vestiging van een verwerkingsverantwoordelijke in de EU. In aanvulling hierop is de AVG is nu ook van toepassing op organisaties die buiten de EU zijn gevestigd, en die persoonsgegevens verwerken in verband met het aanbieden van goederen of diensten aan betrokkenen in de EU of het monitoren van hun gedrag.

BEGINSELEN VOOR DE VERWERKING VAN PERSOONSGEGEVENS

Aan de AVG liggen aan aantal kernbeginselen ten grondslag, die uiteenzetten wat organisaties moeten doen bij het verwerken van persoonsgegevens.

1. Rechtmatigheid, behoorlijkheid en transparantie
2. Doelbinding
3. Minimale gegevensverwerking
4. Juistheid
5. Opslagbeperking
6. Integriteit en vertrouwelijkheid

1. Rechtmatigheid, behoorlijkheid en transparantie
Persoonsgegevens worden verwerkt op een wijze die ten aanzien van betrokkene rechtmatig, behoorlijk en transparant is.

2. Doelbinding
Persoonsgegevens worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen niet op een daarmee onverenigbare wijze verder worden verwerkt.

3. Minimale gegevensverwerking
Persoonsgegevens dienen te worden verwerkt op een wijze die toereikend, ter zake dienend en beperkt is tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

4. Juistheid
Persoonsgegevens dienen juist te zijn en zo nodig te worden geactualiseerd.

5. Opslagbeperking
Persoonsgegevens zullen zo worden bewaard dat de betrokkenen niet langer kunnen worden geïdentificeerd, tenzij identificatie voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.

6. Integriteit en vertrouwelijkheid
Persoonsgegevens moeten middels passende technische en organisatorische maatregelen worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

VERANTWOORDINGSPLICHT

De verwerkingsverantwoordelijke moet ervoor zorgen dat de hierboven omschreven kernbeginselen worden nageleefd, en dat deze naleving kan worden aangetoond. Dit betekent dat van organisaties wordt verwacht dat deze passende technische en organisatorische maatregelen nemen, zoals bijvoorbeeld het opstellen van intern beleid voor gegevensbescherming, interne audits van verwerkingsactiviteiten en protocollen voor het herkennen en afhandelen van datalekken.

IN 12 STAPPEN OP WEG NAAR COMPLIANCE MET DE AVG

De AVG omschrijft hoe organisaties moeten voldoen aan de beginselen. Wij adviseren organisaties om de volgende stappen te nemen om te kunnen voldoen aan de AVG.

1

Data mapping
Breng de datastromen van, naar en binnen uw organisatie in kaart om zo een overzicht te verkrijgen van de verwerkingsactiviteiten binnen uw organisatie.

2

Houd een verwerkingsregister bij
De AVG vereist dat de meeste organisaties een register bijhouden van verwerkingsactiviteiten. Dit betekent dat uw organisatie moet documenteren welke persoonsgegevens worden verwerkt, met welk doel dit gebeurt, wat u doet met de gegevens, en met wie u deze deelt.

3

Stel bewaartermijnen vast
Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor de doeleinden waarvoor ze worden verwerkt. De bewaartermijn kan verschillen per categorie persoons-gegevens. Voor het bewaren van persoonsgegevens van sollicitanten zal doorgaans een andere bewaartermijn gelden dan voor persoonsgegevens in belastingaangiftes. Wij adviseren organisaties om bewaartermijnen-beleid op te stellen.

4

Voer een DPIA uit (waar nodig)
Organisaties kunnen verplicht zijn onder de AVG om een gegevensbeschermings-effectbeoordeling (Data Protection Impact Assessment, of "DPIA") uit te voeren voordat zij een bepaalde verwerking starten, indien de verwerking gelet op de aard, omvang, context en doel daarvan een hoog privacyrisico met zich meebrengt.

5

Sluit verwerkerovereenkomsten en werk deze bij
Als een organisatie als verwerkings-verantwoordelijke een derde partij inschakelt om diensten te verlenen (zoals bijvoorbeeld hosting- of payrolldiensten), zal zo'n derde partij vaak handelen in de hoedanigheid van 'verwerker'. De AVG vereist dat de verwerkingverantwoordelijke bepaalde schriftelijke afspraken maakt met die verwerker over hoe de verwerking wordt uitgevoerd.

6

Implementeer een datalekkenprotocol
De AVG verplicht organisaties om datalekken binnen 72 uur na ontdekking te melden aan de bevoegde privacy-toezichthouder, tenzij het niet waarschijnlijk is dat de inbreuk in verband met de persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Het is raadzaam om een datalekkenprotocol te implementeren waarmee datalekken effectief kunnen worden herkend, onderzocht en indien nodig gemeld.

7

Privacy by design & privacy by default
Bij het ontwerpen van producten en diensten waarbij persoonsgegevens worden verwerkt, moeten organisaties al rekening houden met de beginselen van de AVG voor het verwerken van persoonsgegevens. De standaard-instellingen van nieuwe producten moeten uitgaan van privacyvriendelijke instellingen, waarbij enkel persoons-gegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

8

Stel een Functionaris Gegevens-bescherming (FG) aan (indien nodig)
In bepaalde gevallen verplicht de AVG organisaties tot het aanstellen van een FG. Een FG moet in ieder geval worden aangesteld indien (i) de verwerking van persoonsgegevens wordt verricht door een overheidsinstantie of overheids-orgaan; (ii) de betrokkenen regelmatig en stelselmatig worden geobserveerd; (iii) een grootschalige verwerking van bijzondere categorieën persoons-gegevens plaatsvindt.

9

Pas privacyverklaringen en -kennisgevingen aan
Organisaties zijn verplicht om betrokkenen – meestal vooraf – te informeren over de verwerking van hun persoonsgegevens. Doorgaans gebeurt dit door middel van privacyverklaringen. De AVG bevat een uitgebreide lijst van informatie die moet worden verstrekt aan de betrokkenen.

10

Check of toestemming op juiste wijze wordt verkregen
Bekijk hoe uw organisatie toestemming verkrijgt van betrokkenen. Onder de AVG moet deze vrijelijk, voldoende geïnformeerd, specifiek en ondubbel-zinnig zijn om geldig te zijn. Daarnaast moeten betrokkenen te allen tijde in staat zijn om hun toestemming in te trekken en moet de verwerkings-verantwoordelijke kunnen aantonen dat er geldige toestemming is verkregen.

11

Rechten van betrokkenen
Organisaties moeten technische en organisatorische maatregelen nemen om te kunnen voldoen aan de verzoeken van betrokkenen, zoals het recht om vergeten te worden, het recht op gegevensoverdraagbaarheid en het recht op inzage en correctie. Organisaties doen er goed aan om hun interne procedures te herzien en waar nodig aan te passen om te kunnen voldoen aan de verzoeken van betrokkenen.

12

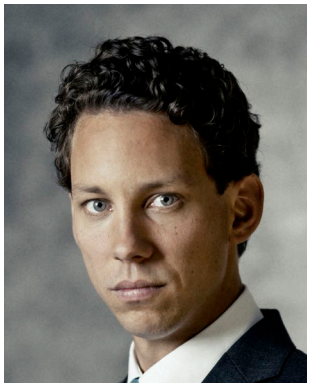
Stel vast wie de leidende privacy-toezichthouder is
Als een organisatie in meer dan één EU lidstaat vestigingen heeft of grensoverschrijdende verwerking verricht, zou deze profijt kunnen hebben van het 'one-stop-shop'-mechanisme van de AVG. Dit betekent dat er voor grens-overschrijdende verwerkingen één toezicht-houder bevoegd is. Organisaties zouden kunnen onderzoeken in hoeverre dit principe uit de AVG op hen betrekking heeft en welke toezichthouder bevoegd is.

CONTACT

Het Privacy & Data Protection Team van Houthoff heeft uitgebreide ervaring in het adviseren van cliënten over de AVG. Het team begeleidt AVG compliance-trajecten en voert privacy audits uit voor cliënten. Het team heeft specifieke ervaring met betrekking tot privacy-vraagstukken die zich voordoen in de sectoren automotive, e-commerce, retail, financiële dienstverlening en bouw.

THOMAS DE WEERD
ADVOCAAT | PARTNER

T +31 20 605 69 85 | M +31 6 5165 9208
t.de.weerd@houthoff.com



JURRE REUS
ADVOCAAT | ASSOCIATE

T +31 20 605 65 76 | M +31 6 8380 3239
j.reus@houthoff.com

@HouthoffPrivacy

Deze uitgave geeft een algemeen overzicht van de (mogelijke) gevolgen van de AVG voor uw onderneming. Als onafhankelijk advocatenkantoor, staat Houthoff haar cliënten bij met zeer specialistische juridische en marktkennis. De in deze uitgave gepresenteerde informatie is afkomstig van publieke bronnen en/of van derden. Houthoff is niet aansprakelijk voor eventuele foutieve en/of niet-volledige informatie, noch voor het gebruik van deze informatie door enige partij. Alvorens (delen van) deze informatie te gebruiken en/of te verspreiden, dient de ontvanger van deze uitgave op de hoogte te zijn van de lokale wet- en regelgeving, en overeenkomstig te handelen.