Europese Commissie

De AVG: nieuwe kansen en nieuwe verplichtingen

Wat ieder bedrijf moet weten over de algemene verordening gegevensbescherming van de EU

Justitie en Consumentenzaken

Printed by Bietlot in Belgium

Luxemburg: Bureau voor publicaties van de Europese Unie, 2018

Print	ISBN 978-92-79-79417-9	doi:10.2838/307738	DS-01-18-082-NL-C
PDF	ISBN 978-92-79-79424-7	doi:10.2838/23715	DS-01-18-082-NL-N

INHOUDSOPGAVE

HOOFDSTUK 1

EEN ZAKELIJKE KANS 2

HOOFDSTUK 2

INZICHT IN DE AVG 4

HOOFDSTUK 3

UW VERPLICHTINGEN IN HET KADER VAN DE AVG 8

HOOFDSTUK 4

VOLDOET U ER AL AAN? 18

HOOFDSTUK 1

EEN ZAKELIJKE KANS

De AVG regelt de manier waarop bedrijven persoonsgegevens verwerken en beheren. Deze verordening is vanaf 25 mei 2018 van toepassing op alle bedrijven en organisaties (bijv. ziekenhuizen, overheidsinstellingen enz.) en is de grootste wijziging van de Europese gegevensbeschermingsregels in meer dan twintig jaar.

De AVG geeft burgers niet alleen meer zeggenschap over de wijze waarop hun persoonsgegevens worden gebruikt, maar zorgt er ook voor dat de regelgeving voor bedrijven in aanzienlijke mate wordt gestroomlijnd door een uniform kader voor gegevensbeschermingswetgeving in de hele EU te scheppen. Met andere woorden, in plaats van dat ieder land zijn eigen wetten inzake gegevensbescherming hanteert, valt de hele EU nu onder één regelgevingskader. Bedrijven die in verschillende landen actief zijn, hoeven dus niet langer aan meerdere, vaak verschillende, regels te voldoen, maar slechts nog aan de AVG om hun diensten overal in de EU te kunnen aanbieden.

Hoe komt de AVG uw bedrijf ten goede?

- **Eén Unie, één wet**: een enkele reeks regels maakt het voor bedrijven eenvoudiger en goedkoper om in de EU zaken te doen.
- **Eén loket**: in de meeste gevallen krijgen bedrijven slechts met één gegevensbeschermingsautoriteit te maken.
- **Europese regels op Europese bodem**: buiten de EU gevestigde bedrijven moeten dezelfde regels toepassen als Europese bedrijven wanneer ze hun goederen of diensten aan personen in de EU aanbieden.
- **Risicogebaseerde benadering**: de AVG voorkomt een omslachtige verplichting die standaard voor iedereen gelijk is, maar stemt de verplichtingen af op de respectieve risico's.
- **Innovatievriendelijke regels**: de AVG is technologisch neutraal.

Alles draait om vertrouwen

Mensen maken zich veel zorgen om de bescherming van hun persoonsgegevens. Daarom hebben ze nog steeds weinig vertrouwen in digitale omgevingen. Volgens een Eurobarometerenquête:

- vinden acht op de tien mensen dat zij geen volledige zeggenschap over hun persoonsgegevens hebben;
- geven zes op de tien aan geen vertrouwen te hebben in onlinebedrijven;
- zegt meer dan 90 % van de Europeanen dat zij in alle EU-landen dezelfde gegevensbeschermingsrechten willen.

De AVG biedt uw bedrijf een nieuwe kans om het vertrouwen van de consument te vergroten door middel van risicogebaseerd beheer van persoonsgegevens.

"Bedrijven die er niet in slagen gegevens van personen adequaat te beschermen, lopen het risico het vertrouwen van de consument te verliezen, terwijl ze dat nodig hebben om mensen te stimuleren nieuwe producten en diensten te gebruiken."

HOOFDSTUK 2

INZICHT IN DE AVG

Geldt de AVG ook voor mij?

Kort gezegd, de AVG geldt voor ***ieder*** bedrijf dat:

persoonsgegevens verwerkt door middel van **geautomatiseerde** of **handmatige** verwerking (mits de gegevens volgens criteria zijn ingedeeld).

Zelfs als uw bedrijf slechts namens andere bedrijven gegevens verwerkt, moet u zich aan de regels houden.

De AVG is van toepassing wanneer:

- uw bedrijf persoonsgegevens verwerkt en in de EU is gevestigd, ongeacht waar de feitelijke gegevensverwerking plaatsvindt, of
- uw bedrijf buiten de EU gevestigd is, maar goederen of diensten aanbiedt aan of toezicht houdt op het gedrag van personen binnen de EU.

Wat zijn persoonsgegevens?

Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare en levende natuurlijke persoon, zoals:

- naam
- adres en telefoonnummer
- locatie
- medische dossiers
- inkomen en bankgegevens
- culturele voorkeuren
- ... enzovoort.

Persoonsgegevens waarbij de identiteitsgegevens zijn verwijderd of gepseudonimiseerd, maar die nog steeds kunnen worden gebruikt om iemand opnieuw te identificeren, vallen binnen het toepassingsgebied van de AVG. Persoonsgegevens die zodanig onomkeerbaar anoniem zijn gemaakt dat de betrokkene niet meer identificeerbaar is, worden niet als persoonsgegevens beschouwd en vallen dus niet onder de AVG.

De AVG is technologisch neutraal. Dit betekent dat het persoonsgegevens beschermt ongeacht de gebruikte technologie of de wijze waarop de persoonsgegevens worden opgeslagen. Ongeacht of uw bedrijf persoonsgegevens verwerkt en opslaat met behulp van een complex IT-systeem of via papieren bestanden, u valt altijd onder de AVG.

"Ongeacht of uw bedrijf persoonsgegevens verwerkt en opslaat met behulp van een complex IT-systeem of via papieren bestanden, u valt altijd onder de AVG."

Wees extra voorzichtig met speciale (gevoelige) categorieën persoonsgegevens

Als de persoonsgegevens die u verzamelt, informatie bevatten over iemands gezondheid, ras, seksuele geaardheid, religie, politieke overtuiging of vakbondslidmaatschap, worden ze als gevoelig beschouwd. Uw bedrijf mag deze gegevens alleen onder specifieke voorwaarden verwerken en u dient mogelijk extra beveiligingen in te voeren, zoals versleuteling.

Wat maakt iets tot verwerking van persoonsgegevens?

Volgens de AVG vallen alle handelingen, zoals het verzamelen, gebruiken en verwijderen van persoonsgegevens, onder de definitie van persoonsgegevens verwerken.

Bewaakt u uw pand met bewakingscamera's? Raadpleegt u een gegevensbank met persoonsgegevens voor zakelijke doeleinden? Verzendt u reclame-e-mails? Verwijdert u (digitale) werknemersdossiers of versnippert u documenten? Of plaatst u een foto van iemand op uw website of sociale-mediakanalen?Als u een van deze vragen met „ja" kunt beantwoorden, dan houdt uw bedrijf zich bezig met gegevensverwerking.

Hoe draagt de AVG bij aan kostenreductie?

De AVG houdt rekening met de behoeften van het bedrijfsleven. De verordening moet bijvoorbeeld administratieve verplichtingen afschaffen om de kosten te verminderen en de administratieve lasten tot een minimum te beperken:

- **Geen voorafgaande kennisgevingen meer**: de hervorming schrapt de meeste voorafgaande kennisgevingen aan toezichthoudende autoriteiten, samen met de daaraan verbonden kosten.
- **Functionaris voor gegevensbescherming**: bedrijven hoeven alleen een functionaris voor gegevensbescherming aan te stellen als hun hoofdactiviteiten betrekking hebben op de grootschalige verwerking van gevoelige gegevens of bestaan uit de grootschalige, regelmatige en systematische observatie van personen. Overheden zijn verplicht een functionaris voor gegevensbescherming aan te wijzen.
- **Effectbeoordeling gegevensbescherming**: bedrijven zijn alleen verplicht een effectbeoordeling gegevensbescherming uit te voeren als een voorgestelde gegevensverwerkingsactiviteit een groot risico inhoudt voor de rechten en vrijheden van personen.
- **Registratie**: bedrijven met minder dan 250 werknemers hoeven geen administratie bij te houden, tenzij de gegevensverwerking niet incidenteel is of gevoelige informatie betreft.

“De verordening moet bijvoorbeeld administratieve verplichtingen afschaffen om de kosten te verminderen en de administratieve lasten tot een minimum te beperken.”

HOOFDSTUK 3

UW VERPLICHTINGEN IN HET KADER VAN DE AVG

De AVG legt bedrijven directe verplichtingen inzake gegevensverwerking op EU-niveau op. Volgens de AVG mogen bedrijven alleen onder bepaalde voorwaarden persoonsgegevens verwerken. Zo moet de verwerking bijvoorbeeld eerlijk en transparant zijn, een bepaald en gerechtvaardigd doel dienen en zich beperken tot de gegevens die nodig zijn om dat doel te bereiken. Ook moet de verwerking gebaseerd zijn op een van de volgende rechtsgronden:

- **toestemming** van de betrokkene;
- een **contractuele verplichting** tussen u en de betrokkene;
- voldoen aan een **wettelijke verplichting**;
- de **vitale belangen** van de betrokkene beschermen;
- een **taak in het algemeen belang** uitvoeren;
- voor de **gerechtvaardigde belangen** van uw bedrijf, maar pas nadat u hebt gecontroleerd of de grondrechten en fundamentele vrijheden van de persoon wiens gegevens u verwerkt, niet ernstig worden aangetast. Als de rechten van de persoon zwaarder wegen dan uw belang, mag u de gegevens niet verwerken.

In focus: toestemming krijgen om persoonsgegevens te gebruiken

De AVG hanteert strikte regels voor de verwerking van gegevens op basis van toestemming. Deze regels moeten ervoor zorgen dat betrokkenen begrijpen waar zij toestemming voor geven. Dit betekent dat toestemming **vrijelijk**, **specifiek**, **geïnformeerd** en **ondubbelzinnig** wordt gegeven op een verzoek in duidelijke en eenvoudige taal. Bovendien moet de toestemming door middel van een **bevestigende handeling** worden gegeven, zoals het online aanvinken van een vakje of het ondertekenen van een formulier.

Als u op basis van toestemming de persoonsgegevens van een **kind** verwerkt, hebt u ouderlijke toestemming nodig. Aangezien de leeftijdsgrens in verschillende landen echter tussen de 13 en 16 jaar kan variëren, wordt u geadviseerd de nationale wetgeving te raadplegen.

Let op! Wanneer iemand met de verwerking van zijn persoonsgegevens instemt, mag u die alleen verwerken voor de doeleinden waarvoor toestemming is gegeven. Bovendien moet u betrokkenen de gelegenheid bieden hun toestemming in te trekken.

Uw rol en verantwoordelijkheid bepalen

Zodra u hebt vastgesteld dat de AVG op uw bedrijf van toepassing is en dat er persoonsgegevens worden verwerkt, is de volgende stap bepalen wat uw rol is.

De regels inzake gegevensbescherming maken een onderscheid tussen de verwerkingsverantwoordelijke en de gegevensverwerker, waarbij elk van hen andere verplichtingen heeft. Waar de verwerkingsverantwoordelijke de doeleinden en middelen van de verwerking van persoonsgegevens bepaalt, verwerkt de gegevensverwerker de persoonsgegevens enkel namens de verwerkingsverantwoordelijke. Dit betekent echter niet dat de verwerker zich achter de verwerkingsverantwoordelijke kan verschuilen.

Volgens de AVG mag de verwerkingsverantwoordelijke alleen gegevensverwerkers inschakelen die voldoende garanties bieden. Deze garanties moeten worden opgenomen in een schriftelijke overeenkomst tussen de verantwoordelijke en de verwerker. De overeenkomst moet ook een aantal bindende bepalingen bevatten, zoals een bepaling dat de gegevensverwerker alleen persoonsgegevens verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke.

Verplichtingen ter bescherming van individuele rechten

De AVG bevat een aantal verplichtingen ter bescherming van het recht van personen op zeggenschap over hun persoonsgegevens.

Uw verplichting: transparante informatie verstrekken

Bedrijven moeten personen informeren over wie wat verwerkt en waarom. In deze informatie moet ten minste duidelijk worden vermeld:

- wie u bent;
- waarom u de gegevens verwerkt;
- wat de rechtsgrond is;
- wie de gegevens ontvangt (indien van toepassing).

In sommige gevallen moet de informatie ook het volgende vermelden:

- contactgegevens van de functionaris voor gegevensbescherming;
- gerechtvaardigd belang (wanneer het gerechtvaardigd belang de rechtsgrond voor de verwerking is);
- basis voor de gegevensoverdracht naar een land buiten de EU;
- hoe lang de gegevens worden opgeslagen;
- welke rechten inzake gegevensbescherming de betrokkene heeft (d.w.z. het recht op inzage, correctie, verwijdering, beperking, bezwaar, overdraagbaarheid enz.);
- hoe toestemming kan worden ingetrokken (wanneer toestemming de rechtsgrond voor de verwerking is);
- of er een wettelijke of contractuele verplichting bestaat om de gegevens te verstrekken;
- bij geautomatiseerde besluitvorming, informatie over de logica achter en de betekenis en gevolgen van de besluitvorming.

“Bedrijven moeten personen informeren over wie wat verwerkt en waarom.”

Uw verplichting: recht op inzage en recht op gegevensoverdraagbaarheid

Personen hebben het recht om kosteloos inzage te vragen in hun persoonsgegevens in een toegankelijke vorm. Als u een dergelijk verzoek ontvangt, moet u:

- betrokkenen vertellen of u hun persoonsgegevens verwerkt;
- hen over de verwerking informeren (zoals het doeleinde van de verwerking, de categorieën persoonsgegevens in kwestie, wie hun gegevens ontvangen enz.);
- een kopie verstrekken van de verwerkte persoonsgegevens.

Wanneer de verwerking gebaseerd is op toestemming of een overeenkomst, mag de betrokkene bovendien verzoeken om zijn persoonsgegevens terug te sturen of door te geven aan een ander bedrijf. Dit staat bekend als het recht op gegevensoverdraagbaarheid. De gegevens moeten worden verstrekt in een algemeen gebruikte en machineleesbare vorm.

Hoewel deze twee rechten nauw met elkaar zijn verbonden, gaat het hier toch om twee verschillende rechten. U moet u er dus voor zorgen dat er geen verwarring bestaat tussen de twee rechten, en u moet de betrokkene hierover informeren.

Uw verplichting: recht op verwijdering (recht op vergetelheid)

In sommige gevallen kan een persoon de verwerkingsverantwoordelijke verzoeken om zijn persoonsgegevens te wissen, bijvoorbeeld wanneer de gegevens niet langer nodig zijn om het doeleinde van de verwerking uit te voeren. Uw bedrijf is echter niet verplicht om een individueel verzoek in te willigen indien:

- de verwerking noodzakelijk is om de vrijheid van meningsuiting en informatie te eerbiedigen;
- u de persoonsgegevens moet bewaren om aan een wettelijke verplichting te voldoen;
- er andere redenen van algemeen belang zijn om de persoonsgegevens te bewaren, zoals volksgezondheid of wetenschappelijke en historische onderzoeksdoeleinden;
- u de persoonsgegevens moet bewaren om een rechtsvordering vast te stellen.

Uw verplichting: recht op correctie en bezwaar

Indien betrokkenen van mening zijn dat hun persoonsgegevens onjuist, onvolledig of onnauwkeurig zijn, hebben ze het recht om deze zonder onnodige vertraging te laten corrigeren of aanvullen.

Betrokkenen mogen ook te allen tijde bezwaar maken tegen de verwerking voor een bepaald gebruik wanneer uw bedrijf hun persoonsgegevens verwerkt op basis van uw gerechtvaardigd belang of voor de uitvoering van een taak van algemeen belang. Tenzij u een gerechtvaardigd belang heeft dat zwaarder weegt dan het belang van de persoon, moet u het verwerken van de persoonsgegevens staken. Iemand mag ook vragen om de verwerking van zijn persoonsgegevens te beperken, terwijl wordt vastgesteld of uw gerechtvaardigd belang al dan niet opweegt tegen zijn belang. Bij direct marketing bent u echter altijd verplicht de verwerking van de persoonsgegevens op verzoek van de betrokkene te staken.

Een kleine waarschuwing over geautomatiseerde besluitvorming en profilering

Personen hebben het recht niet onderworpen te worden aan besluitvorming die uitsluitend op geautomatiseerde verwerking is gebaseerd. Er zijn echter enkele uitzonderingen op deze regel, bijvoorbeeld wanneer de betrokkene uitdrukkelijk toestemming heeft gegeven voor geautomatiseerde besluitvorming. Behalve wanneer geautomatiseerde besluitvorming op een wet is gebaseerd, moet uw bedrijf:

- de betrokkene informeren over de geautomatiseerde besluitvorming;
- de betrokkene het recht geven om de geautomatiseerde besluitvorming door een persoon te laten beoordelen;
- de betrokkene de mogelijkheid bieden om de geautomatiseerde besluitvorming te betwisten.

Indien een bank bijvoorbeeld haar besluitvorming automatiseert om al dan niet een lening aan bepaalde personen toe te kennen, moeten ze van de geautomatiseerde besluitvorming op de hoogte worden gebracht en de mogelijkheid krijgen de besluitvorming te betwisten en om menselijke tussenkomst te verzoeken.

Risicogebaseerde verplichtingen

Naast de verplichtingen ter bescherming van individuele rechten bevat de AVG ook een aantal verplichtingen waarvan de toepassing afhankelijk is van het risico.

Uw verplichting: een functionaris voor gegevensbescherming benoemen

Een functionaris voor gegevensbescherming is verantwoordelijk voor het toezicht op de naleving van de AVG. Een van de hoofdtaken van de functionaris voor gegevensbescherming is werknemers die de eigenlijke verwerking van persoonsgegevens uitvoeren, informeren en adviseren over hun verplichtingen. De functionaris voor gegevensbescherming werkt ook samen met de gegevensbeschermingsautoriteit en fungeert zowel voor hen als voor personen als aanspreekpunt.

Uw bedrijf is verplicht een functionaris voor gegevensbescherming aan te wijzen wanneer:

- u regelmatig of systematisch personen observeert of speciale categorieën gegevens verwerkt;
- deze verwerking een hoofdtaak is, en
- u dit op grote schaal doet.

Als u bijvoorbeeld persoonsgegevens verwerkt om reclame via zoekmachines te richten op basis van het onlinegedrag van personen, dan moet u volgens de AVG een functionaris voor gegevensbescherming hebben. Als u uw klanten echter slechts één keer per jaar promotiemateriaal stuurt, hebt u geen functionaris voor gegevensbescherming nodig. Ook als u een arts bent die gegevens over de gezondheid van patiënten verzamelt, hebt u waarschijnlijk geen functionaris voor gegevensbescherming nodig. Zo'n functionaris voor gegevensbescherming is wel nodig als u persoonsgegevens over genetica en gezondheid voor een ziekenhuis verwerkt.

Uw verplichting: gegevensbescherming door ontwerp endoor standaardinstellingen

De AVG introduceert twee nieuwe beginselen: gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen.

Gegevensbescherming door ontwerp draagt ertoe bij dat bedrijven in een vroeg stadium van de planning voor een nieuwe manier om persoonsgegevens te verwerken, rekening houden met gegevensbescherming. Volgens dit beginsel moet een verwerkingsverantwoordelijke alle nodige technische en organisatorische maatregelen treffen om de beginselen voor gegevensbescherming te implementeren en de rechten van personen te beschermen. Deze stappen kunnen bijvoorbeeld bestaan uit het gebruik van pseudonimisering.

Gegevensbescherming door ontwerp minimaliseert privacyrisico's en zorgt voor meer vertrouwen. Door gegevensbescherming vooraan in de ontwikkeling van nieuwe goederen of diensten te plaatsen, kunnen eventuele problemen op het gebied van gegevensbescherming in een vroeg stadium worden vermeden. Bovendien draagt deze praktijk bij aan meer bewustzijn over gegevensbescherming in alle afdelingen en op alle niveaus van een bedrijf.

Gegevensbescherming door standaardinstellingen betekent dat u ervoor zorgt dat uw bedrijf altijd de meest privacyvriendelijke instelling tot standaardinstelling maakt. Als er bijvoorbeeld twee privacyinstellingen mogelijk zijn en een van de instellingen voorkomt dat anderen inzage krijgen in persoonsgegevens, moet deze als standaardinstelling worden gebruikt.

"Gegevensbescherming door ontwerp minimaliseert privacyrisico's en zorgt voor meer vertrouwen."

"Gegevensbescherming door standaardinstellingen betekent dat u ervoor zorgt dat uw bedrijf altijd de meest privacyvriendelijke instelling tot standaardinstelling maakt."

Uw verplichting: correcte kennisgeving in geval van gegevensinbreuk

Er is sprake van gegevensinbreuk wanneer persoonsgegevens waarvoor u verantwoordelijk bent, per ongeluk of onrechtmatig aan onbevoegde ontvangers worden geopenbaard, tijdelijk niet beschikbaar zijn of worden gewijzigd.

Voor een bedrijf is het van vitaal belang om passende technische en organisatorische maatregelen te treffen om gegevensinbreuken te voorkomen. Als er echter toch een gegevensinbreuk plaatsvindt die een risico vormt voor rechten en vrijheden van personen, moet u dit uiterlijk binnen 72 uur nadat u kennis heeft genomen van de inbreuk, aan de gegevensbeschermingsautoriteit melden.

Afhankelijk van het feit of de gegevensinbreuk een *hoog* risico voor de betrokkenen inhoudt, moet een bedrijf eventueel alle personen die door de gegevensinbreuk worden getroffen, op de hoogte brengen.

Draagt u gegevens over buiten de EU?

De AVG is van toepassing op de Europese Economische Ruimte (EER), die alle EU-landen plus IJsland, Liechtenstein en Noorwegen omvat. Wanneer persoonsgegevens buiten de EER worden overgedragen, moet de bescherming die door de AVG wordt geboden, met de gegevens meegaan. Dit betekent dat bedrijven ervoor moeten zorgen dat er bepaalde waarborgen zijn om gegevens te mogen exporteren.

De AVG biedt een gediversifieerd instrumentarium aan mechanismen om gegevens aan derde landen te kunnen overdragen. Volgens de AVG mogen gegevens worden overgedragen wanneer:

1. de bescherming van het land door de EU toereikend wordt geacht, of
2. uw bedrijf bijvoorbeeld de nodige maatregelen treft om passende waarborgen te bieden, zoals specifieke bepalingen in de overeenkomst die met de niet-Europese importeur van de persoonsgegevens wordt gesloten, of
3. uw bedrijf zich bijvoorbeeld beroept op bepaalde gronden voor overdracht (de zogenaamde „afwijkingen“), zoals toestemming van betrokkenen.

Voor meer informatie over de regels die van toepassing zijn op internationale gegevensoverdrachten, kunt de mededeling van de Europese Commissie raadplegen over de uitwisseling en bescherming van persoonsgegevens in een geglobaliseerde wereld: http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52017DC0007&from=NL

Moet u een effectbeoordeling gegevensbescherming uitvoeren?

Een effectbeoordeling gegevensbescherming (Data Protection Impact Assessment of DPIA) is verplicht wanneer de beoogde verwerking een hoog risico voor de rechten en vrijheden van personen vormt. Dit kan bijvoorbeeld het geval zijn wanneer er nieuwe technologieën worden gebruikt.

Volgens de AVG bestaat er minstens zo'n groot risico wanneer:

- geautomatiseerde verwerkings- en profileringsmechanismen worden gebruikt om personen systematisch en uitgebreid te evalueren;
- er een voor het publiek toegankelijke gebied systematisch op grote schaal (bijvoorbeeld met bewakingscamera's) wordt geobserveerd;
- er op grote schaal gevoelige gegevens (bijv. gezondheidsgegevens) worden verwerkt.

Met een DPIA moeten potentiële risico's voor de rechten en vrijheden van personen worden vastgesteld voordat de verwerking van persoonsgegevens begint en voordat het risico werkelijkheid wordt. Door het risico vooraf te beperken, kan schade worden voorkomen en kunnen kosten worden geminimaliseerd.

Indien maatregelen uit de DPIA niet alle geïdentificeerde hoge risico's kunnen wegnemen, moet de gegevensbeschermingsautoriteit worden geraadpleegd voordat de beoogde gegevensverwerking plaatsvindt.

"Een effectbeoordeling gegevensbescherming (Data Protection Impact Assessment of DPIA) is verplicht wanneer de beoogde verwerking een hoog risico voor de rechten en vrijheden van personen vormt."

Wat u moet doen

Reageren op verzoeken

Als uw bedrijf een verzoek ontvangt van iemand die zijn rechten wil uitoefenen, moet u zonder onnodige vertraging en in elk geval binnen één maand na ontvangst van het verzoek reageren. Deze reactietijd kan echter met twee maanden worden verlengd voor complexe of meervoudige verzoeken, mits de betrokkene over de verlenging wordt geïnformeerd. Bovendien moeten verzoeken **kosteloos** worden behandeld. Indien een verzoek wordt afgewezen, moet u de betrokkene in kennis stellen van de redenen daarvoor en hem informeren over zijn recht om een klacht in te dienen bij de gegevensbeschermingsautoriteit.

Naleving aantonen en een administratie bijhouden!

Een van de belangrijkste beginselen die aan de AVG ten grondslag liggen, is ervoor zorgen dat bedrijven naleving kunnen aantonen. U moet dus kunnen aantonen dat uw bedrijf conform de AVG handelt en aan alle toepasselijke verplichtingen voldoet, in het bijzonder op verzoek van of na inspectie door de gegevensbeschermingsautoriteit.

Een manier om dit te doen is het bijhouden van een uitgebreide administratie over zaken als:

- naam en contactgegevens van uw bedrijf dat betrokken is bij de gegevensverwerking;
- reden(en) voor de verwerking van persoonsgegevens;
- beschrijving van de categorieën personen die persoonsgegevens verstrekken;
- categorieën organisaties die de persoonsgegevens ontvangen;
- doorgifte van persoonsgegevens aan een ander land of een andere organisatie;
- opslagperiodes van de persoonsgegevens;
- beschrijving van de veiligheidsmaatregelen die bij de verwerking worden gebruikt.

Daarnaast moet uw bedrijf ook schriftelijke procedures en richtlijnen bijhouden en regelmatig bijwerken en met uw medewerkers delen.

HOOFDSTUK 4

VOLDOET U ER AL AAN?

Als het gaat om de verwerking van persoonsgegevens, legt de AVG de bal bij u. De eerste stap is uw huidige gegevensverwerkingsactiviteiten in kaart brengen en uw interne bedrijfsprocessen opnieuw evalueren. In het bijzonder moet u:

- bepalen welke gegevens u voor welk doeleinde in uw bezit hebt en op welke rechtsgrond u die bezit;
- alle bestaande overeenkomsten beoordelen, met name die tussen verwerkingsverantwoordelijken en verwerkers;
- alle beschikbare opties voor internationale overdrachten evalueren, en
- het algemene toezicht binnen uw bedrijf beoordelen (d.w.z. welke IT- en organisatorische maatregelen u hebt getroffen), met inbegrip van de vraag of u al dan niet een functionaris voor gegevensbescherming moet of wilt benoemen.

Een essentieel element in dit proces is ervoor zorgen dat het hoogste managementniveau in uw bedrijf bij dergelijke beoordelingen wordt betrokken, input levert en regelmatig op de hoogte wordt gehouden van en wordt geraadpleegd over wijzigingen in het gegevensbeleid.

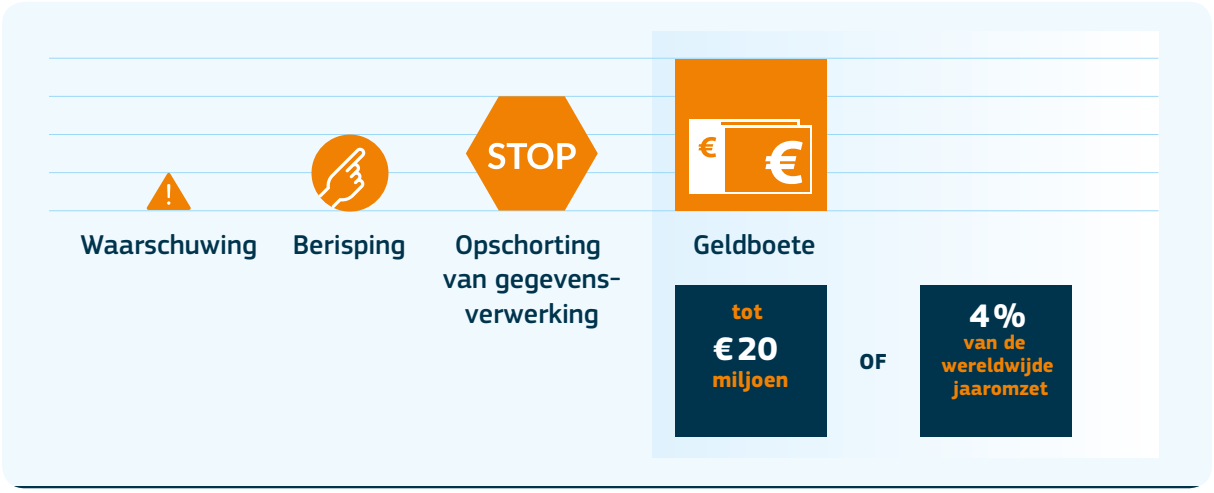
Verwerkt u gegevens in meer dan één land?

In geval van grensoverschrijdende verwerking kan een toezichthoudende autoriteit van een ander land de bevoegde autoriteit zijn in plaats van uw nationale gegevensbeschermingsautoriteit. Meestal is dit de gegevensbeschermingsautoriteit van het land waar het hoofdkantoor van uw bedrijf in de EU is gevestigd (waar beslissingen worden genomen over de middelen en doeleinden van verwerking).

De risico's van niet-naleving

Niet-naleving van de AVG kan leiden tot aanzienlijke boetes; voor sommige inbreuken kan dit zelfs oplopen tot 20 miljoen EUR of 4 % van de totale bedrijfsomzet. De gegevensbeschermingsautoriteit kan extra corrigerende maatregelen opleggen en bijvoorbeeld opdragen de verwerking van persoonsgegevens te staken. Ook moet u rekening houden met de reputatieschade die eventuele niet-naleving kan veroorzaken.

Het is duidelijk dat niet-naleving van de AVG veel meer kost dan alle investeringen die nodig zijn om eraan te voldoen.



Vragen? Opmerkingen? Neem contact op met uw nationale gegevensbeschermingsautoriteit.

Online uw nationale gegevensbeschermingsautoriteit opzoeken, kan op

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

BELANGRIJKE MEDEDELING

De informatie en adviezen in deze brochure zijn uitsluitend bedoeld om meer inzicht in de EU-regels voor gegevensbescherming te geven.

Ze zijn zuiver bedoeld als een adviesinstrument. Alleen de tekst van de algemene verordening gegevensbescherming (AVG) is rechtsgeldig. Daardoor kunnen natuurlijke personen hun rechten en verplichtingen alleen ontlenen aan de algemene verordening gegevensbescherming. Met deze adviezen worden geen afdwingbare rechten of verwachtingen gecreëerd.

Bindende interpretatie van EU-wetgeving is de exclusieve bevoegdheid van het Hof van Justitie van de Europese Unie. De in deze adviezen tot uitdrukking gebrachte opvattingen laten het standpunt dat de Commissie mogelijk inneemt bij het Hof van Justitie, onverlet.

Noch de Europese Commissie, noch enig persoon handelend namens de Europese Commissie is verantwoordelijk voor het gebruik dat van de informatie in de brochure zou kunnen worden gemaakt.

Omdat deze brochure een weerspiegeling is van de stand van zaken op het moment dat die werd opgesteld, moet de brochure worden gezien als een „dynamisch document" dat openstaat voor verbetering. De inhoud van deze adviezen kan zonder voorafgaande aankondiging worden gewijzigd.

Hoe neemt u contact op met de EU?

Kom langs

Er zijn honderden Europe Direct-informatiecentra overal in de Europese Unie. U vindt het adres van het dichtstbijzijnde informatiecentrum op: https://europa.eu/european-union/contact_nl

Bel of mail

Europe Direct is een dienst die uw vragen over de Europese Unie beantwoordt. U kunt met deze dienst contact opnemen door:

– te bellen naar het gratis nummer: 00 800 6 7 8 9 10 11 (bepaalde telecomaanbieders kunnen wel kosten in rekening brengen),
– te bellen naar het gewone nummer: +32 22999696, of
– een e mail te sturen via: https://europa.eu/european-union/contact_nl

Waar vindt u informatie over de EU?

Online

Informatie over de Europese Unie in alle officiële talen van de EU is beschikbaar op de Europa-website op: https://europa.eu/european-union/index_nl

EU-publicaties

U kunt publicaties van de EU downloaden of bestellen bij EU Bookshop op: https://publications.europa.eu/bookshop (sommige zijn gratis, andere niet). Als u meerdere exemplaren van gratis publicaties wenst, neem dan contact op met Europe Direct of uw plaatselijke informatiecentrum (zie https://europa.eu/european-union/contact_nl).

EU-wetgeving en aanverwante documenten

Toegang tot juridische informatie van de EU, waaronder alle EU-wetgeving sinds 1952 in alle officiële talen, krijgt u op EUR Lex op: http://eur-lex.europa.eu

Open data van de EU

Het opendataportaal van de EU (http://data.europa.eu/euodp/nl) biedt toegang tot datasets uit de EU. Deze gegevens kunnen gratis worden gedownload en hergebruikt, zowel voor commerciële als voor niet-commerciële doeleinden.

DS-01-18-082-NL-C

De algemene verordening gegevensbescherming (AVG) regelt de manier waarop bedrijven persoonsgegevens verwerken en beheren. Met één enkele Europese wet voor de bescherming van persoonsgegevens hoeft uw bedrijf zich nu in principe maar aan één gegevensbeschermingswet te houden wanneer het goederen en diensten in heel Europa aanbiedt.

Door de regelgeving voor bedrijven te vereenvoudigen, biedt de AVG uw bedrijf een nieuwe kans om het beheer van persoonsgegevens te verbeteren en er zo voor te zorgen dat de consument meer vertrouwen in uw bedrijf krijgt.

Deze brochure geeft een overzicht van de verplichtingen voor uw bedrijf in het kader van de AVG.

europa.eu/dataprotection/nl

Publicatiebureau

ISBN 978-92-79-79417-9