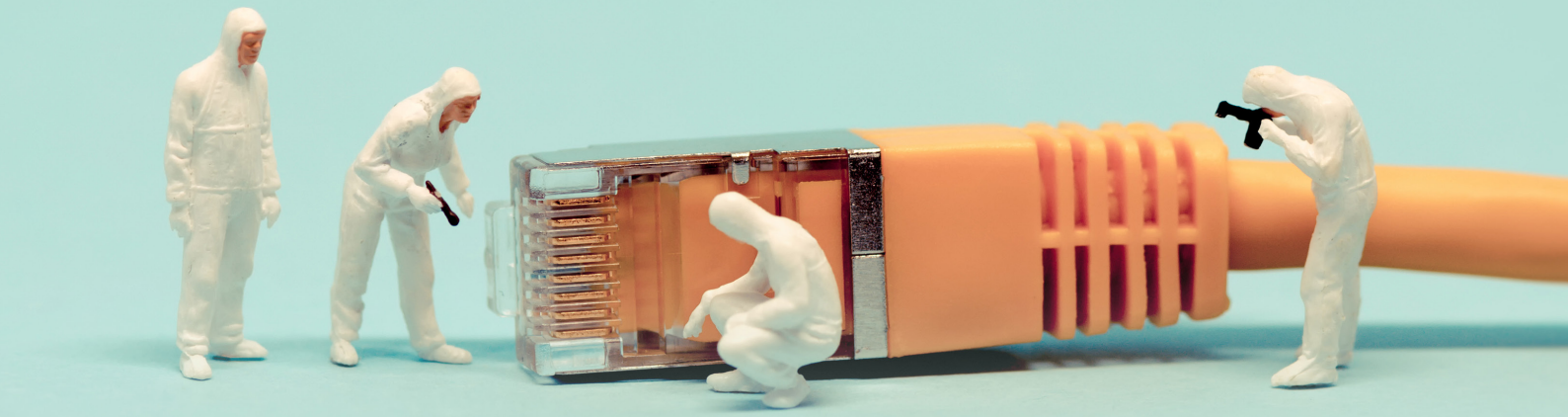
Your World First

C/M/S/
Law.Tax

Algemene verordening gegevensbescherming



2018

Inhoud

Inleiding

Het landschap voor privacyregelgeving, in het bijzonder de bescherming van persoonsgegevens, is grotendeels ongewijzigd gebleven sinds 1995. Dit landschap verandert binnenkort ingrijpend. Na uitgebreide onderhandelingen werd namelijk op 4 mei 2016 de Algemene verordening gegevensbescherming (AVG) formeel vastgesteld. De AVG vervangt richtlijn 95/46/EG en daarmee een groot deel van de huidige EU-wetgeving betreffende persoonsgegevensbescherming (hierna spreken wij voor het gemak dikwijls alleen nog van gegevensbescherming).

De AVG is rechtstreeks van toepassing in alle EU-lidstaten zonder dat omzetting in nationale wetgeving nodig is. Dit in tegenstelling tot richtlijn 95/46/EG (de Richtlijn bescherming persoonsgegevens, hierna: de Richtlijn), die in Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens. Met ingang van 25 mei 2018 vervangt de AVG dus een groot deel van de nationale wetgeving van de lidstaten op het gebied van gegevensbescherming.

De AVG introduceert nieuwe concepten in de regelgeving, zoals het recht op vergetelheid. Zij bevat uitgebreide nieuwe verplichtingen voor het bedrijfsleven en verandert de rol van de functionaris gegevensbescherming in een onderneming ingrijpend. De rechten voor particulieren zijn aanzienlijk versterkt en de maximale boetes die opgelegd kunnen worden bij niet-naleving zijn exponentieel gestegen tot € 20.000.000 of 4% van de jaarlijkse wereldwijde omzet van een onderneming.

Deze brochure is bedoeld om de belangrijkste verschillen tussen de Richtlijn en de AVG te verklaren. We hebben thema-iconen gebruikt voor het categoriseren van de veranderingen, zodat u in één oogopslag kunt zien welke impact een verandering op uw bedrijf heeft.

Zie onze Woordenlijst op pagina 21 voor een uitleg van termen en afkortingen die we hebben gebruikt in deze brochure.

Als u meer informatie wenst over de AVG of de Richtlijn, neem dan contact op met een van de leden van ons Data Protection & Privacy team:

Edmon Oude Elferink
Partner, Head of Data Protection & Privacy team
T: +32 26 5004 54
E: edmon.oudeelferink@cms-dsb.com

Simon Sanders
Advocaat, Data Protection & Privacy team
T: +31 20 3016 371
E: simon.sanders@cms-dsb.com

Stephanie Dekker
Advocaat, Data Protection & Privacy team
T: +31 20 3016 238
E: stephanie.dekker@cms-dsb.com

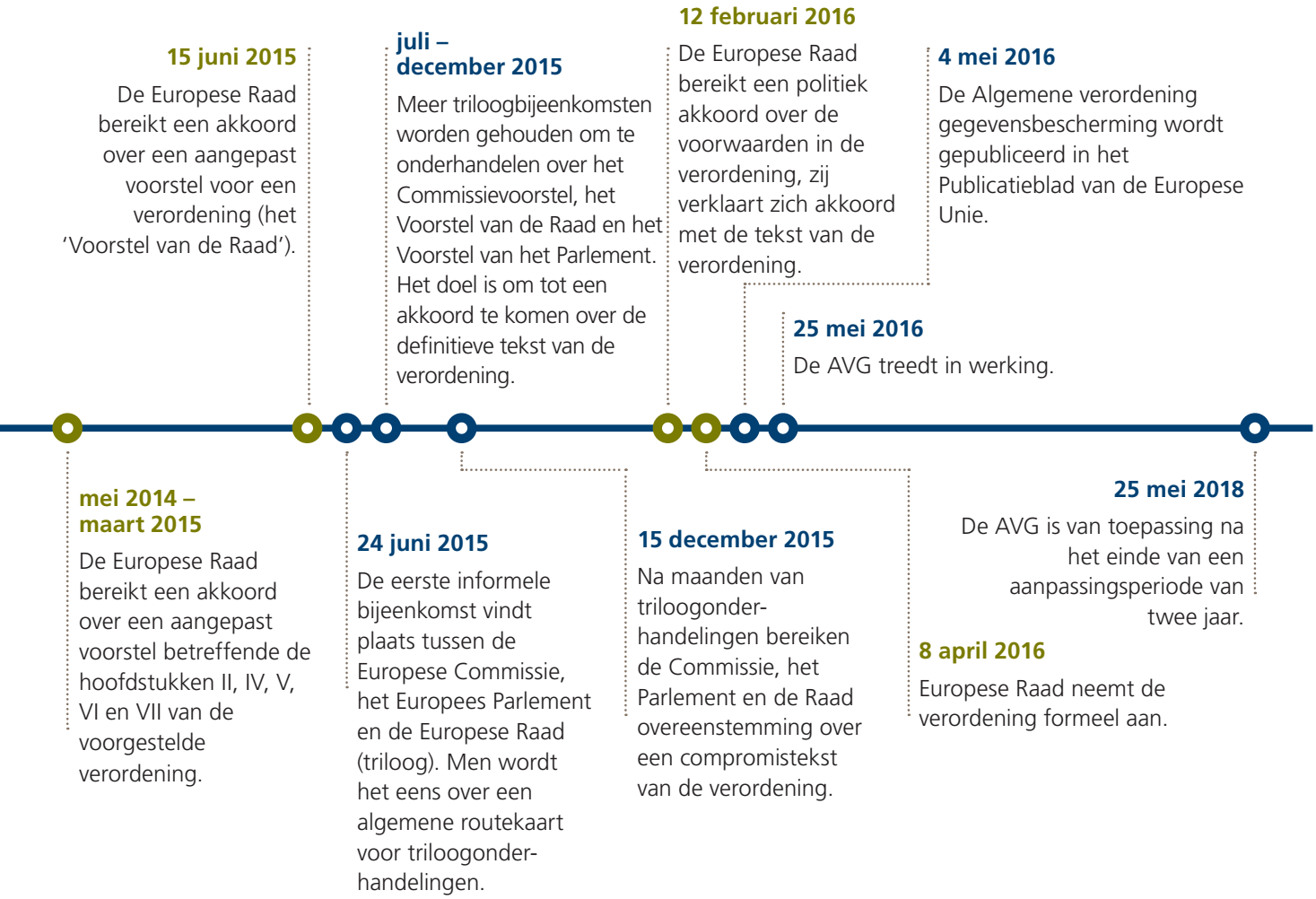
Erik Jonkman
Advocaat, Data Protection & Privacy team
T: +31 20 3016 379
E: erik.jonkman@cms-dsb.com

Tijdlijn Algemene verordening gegevensbescherming

Publicatie van de Europese Commissie

Publicatie van het Europees Parlement

Publicatie van de Europese Raad


mei 2014 – maart 2015
De Europese Raad bereikt een akkoord over een aangepast voorstel betreffende de hoofdstukken II, IV, V, VI en VII van de voorgestelde verordening.
15 juni 2015
De Europese Raad bereikt een akkoord over een aangepast voorstel voor een verordening (het 'Voorstel van de Raad').
24 juni 2015
De eerste informele bijeenkomst vindt plaats tussen de Europese Commissie, het Europees Parlement en de Europese Raad (triloog). Men wordt het eens over een algemene routekaart voor triloogonder-handelingen.
juli – december 2015
Meer triloogbijeenkomsten worden gehouden om te onderhandelen over het Commissievoorstel, het Voorstel van de Raad en het Voorstel van het Parlement. Het doel is om tot een akkoord te komen over de definitieve tekst van de verordening.
15 december 2015
Na maanden van triloogonder-handelingen bereiken de Commissie, het Parlement en de Raad overeenstemming over een compromistekst van de verordening.
12 februari 2016
De Europese Raad bereikt een politiek akkoord over de voorwaarden in de verordening, zij verklaart zich akkoord met de tekst van de verordening.
8 april 2016
Europese Raad neemt de verordening formeel aan.
25 mei 2016
De AVG treedt in werking.
4 mei 2016
De Algemene verordening gegevensbescherming wordt gepubliceerd in het Publicatieblad van de Europese Unie.
25 mei 2018
De AVG is van toepassing na het einde van een aanpassingsperiode van twee jaar.


North Sea
The Hague
London
Brussels
English Channel
Le Havre
Paris
FRANCE
Geneva (Genève)
Lyon
Strasbourg
Basel (Basle)
Brest
Nantes
Bordeaux
Toulouse
Bay of Biscay

Juridische reikwijdte

Personen en rechtspersonen (verantwoordelijken) die zijn gevestigd binnen de EU en verantwoordelijk zijn voor het verwerken van persoonsgegevens voor ondernemingen of organisaties zijn onderworpen aan de Richtlijn. Deze personen vallen nog steeds onder de AVG. De AVG heeft echter een ruimere reikwijdte. De AVG is in een aantal gevallen ook rechtstreeks van toepassing op zogeheten verwerkers van persoonsgegevens (voorheen: bewerkers). In de Richtlijn is dat niet het geval.

Voor verantwoordelijken die buiten de EU zijn gevestigd worden, in vergelijking met de Richtlijn, de criteria om te bepalen of de AVG van toepassing is ingrijpend veranderd.

Onder de huidige regelgeving zijn verantwoordelijken indien zij buiten de Europese Economische Ruimte zijn gevestigd maar in een EU-lidstaat wel apparatuur of middelen gebruiken voor de verwerking van persoonsgegevens onderworpen aan de Richtlijn (tenzij die middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens).

De reikwijdte van de AVG is breder. Verantwoordelijken en verwerkers die zijn gevestigd buiten de EU moeten voldoen aan de regels van de AVG indien de verwerking van persoonsgegevens betrekking heeft op:

— het aanbieden van goederen of diensten (gratis of betaald) aan particulieren in de EU; of

— het monitoren van gedrag van individuen in de EU.

In de overwegingen van de AVG staat dat websites die een taal of een munteenheid gebruiken van een lidstaat van de EU en de mogelijkheid bieden om goederen of diensten in die taal of valuta bestellen, of die uitdrukkelijk vermelden dat zij in EU gevestigde klanten of gebruikers hebben, binnen deze definitie kunnen vallen.

Om uit te maken of er sprake is van het monitoren van gedrag van individuen in de EU moet, volgens de overwegingen van de AVG, worden vastgesteld of er sprake is van online tracking of profilering, voornamelijk met het oog op het analyseren en voorspellen van persoonlijke voorkeuren en gedragingen.

Verantwoordelijken en verwerkers die buiten de EU zijn gevestigd, maar die zich richten op personen in de EU, kunnen dus onder de reikwijdte van Europees recht vallen. Als dit het geval is, moeten ook zij de verplichtingen die zijn opgenomen in de AVG analyseren om ervoor te zorgen dat zij in staat zijn te voldoen aan deze verplichtingen. De meeste bedrijven die in deze categorie vallen moeten ook een in de EU gevestigde vertegenwoordiger aanwijzen.

Te nemen stappen ter voorbereiding: Niet in de EU gevestigde verantwoordelijken en verwerkers moeten controleren of de AVG op hun onderneming van toepassing is.
Als de verwerking van persoonsgegevens valt onder bovenstaande criteria, moeten zij voldoen aan de regels in de AVG. Het is in dat geval aan te raden om zich bij voorbaat voor te bereiden op het van toepassing worden van deze regelgeving. Overweeg of het noodzakelijk is om een vertegenwoordiger in een EU-lidstaat aan te wijzen.

Boetes / Handhaving

Onder de huidige wetgeving in de EU-lidstaten verschillen de boetes die kunnen worden opgelegd voor overtredingen van regels voor het verwerken van persoonsgegevens nogal. In Nederland bijvoorbeeld, kan de Autoriteit Persoonsgegevens sinds 1 januari 2016 voor overtredingen van de privacyregelgeving, in het geval van een ernstige schending van de privacy door een verantwoordelijke of bewerker, een bestuurlijke boete opleggen van maximaal € 820.000 of 10% van de omzet in het vorige boekjaar. Onder de AVG kunnen de geldboetes voor verantwoordelijken en verwerkers nog hoger zijn.

De AVG introduceert zowel voor verantwoordelijken als verwerkers een tweeledig systeem van bestuurlijke boetes. Op sommige overtredingen, bijvoorbeeld overtredingen die verband houden met verplichtingen tot het inrichten van geautomatiseerde systemen, staat een boete van maximaal € 10.000.000, of voor een onderneming tot 2% van de wereldwijde omzet in het vorige boekjaar. Andere overtredingen, zoals schendingen van de basisprincipes voor de verwerking van persoonsgegevens of voorwaarden voor het verkrijgen van toestemming voor het verwerken van persoonsgegevens, worden bestraft met hogere boetes tot maximaal € 20.000.000, voor een onderneming, tot 4% van de wereldwijde omzet in het vorige boekjaar, als dit een hoger bedrag is. Nota bene: nationale wetgevers kunnen zelf bepalen of dergelijke boetes al dan niet kunnen worden opgelegd aan overheidsorganen.

Zie de bijlage op pagina 23 voor een overzicht van de maximale boete die voor een bepaalde overtreding kan worden opgelegd en de factoren die bij de vaststelling van de hoogte van de boete in aanmerking moeten worden genomen.

Op dit moment verschilt de handhaving van de richtlijn 95/46/EG door de nationale toezichthouders nog aanzienlijk. Op grond van de Richtlijn hebben toezichthouders de bevoegdheid tot interventie, zoals het uitbrengen van adviezen voordat gegevens worden verwerkt of de bevoegdheid tot blokkeren, wissen of vernietigen van gegevens. Toezichthouders kunnen ook audits uitvoeren en tot handhaving overgaan indien sprake is van overtreding van de Richtlijn. Over het algemeen zullen in de toekomst onder de AVG de handhavingsbevoegdheden worden geharmoniseerd. Let wel: de strafrechtelijke handhaving is niet geharmoniseerd maar nog steeds gedelegeerd aan de EU-lidstaten. Sommige common-law-lidstaten kennen namelijk geen bestuursrecht, en zullen de AVG dus alleen met strafrechtelijke middelen kunnen handhaven. Op basis van de nieuwe handhavingsbevoegdheden kunnen verantwoordelijken en verwerkers waarschuwingen, berispingen en bevelen krijgen. Verder kan een tijdelijk of definitief verbod op verwerking van gegevens worden opgelegd, de gegevensstroom naar het buitenland worden opgeschort en de rectificatie of verwijdering van persoonsgegevens worden bevolen.

Ook de rechten van individuen worden versterkt in de AVG. Deze rechten zijn bijvoorbeeld: (i) het vorderen van schadevergoeding voor schade veroorzaakt door een overtreding van de AVG; (ii) het recht tot het indienen van een klacht betreffende niet-conforme verwerking van persoonsgegevens door verantwoordelijken en verwerkers; (iii) de mogelijkheid om een klacht bij een toezichthouder in te dienen; en (iv) het recht op een effectief rechtsmiddel tegen een toezichthouder die een klacht niet correct heeft afgehandeld.

Te nemen stappen ter voorbereiding: Organisaties kunnen zich voorbereiden op de invoering van bovenstaande verplichtingen door het identificeren en aanpakken van hiaten in hun gegevensbescherming, ook als die op dit moment nog worden gezien als een laag risico. Als de AVG van toepassing is, kan het risico veel groter worden. Het is verder raadzaam om de nieuwe verplichtingen die worden opgelegd door de AVG te identificeren en een praktisch plan te ontwikkelen en te implementeren om compliant te zijn vóór 25 mei 2018.


BCE ECB EZB EKT EK
100 EURO

Informatieverplichtingen

Op basis van de AVG moeten verantwoordelijken hun betrokkenen informatie geven over de verwerking van persoonsgegevens. Deze informatie moet in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm worden verstrekt en bovendien in een duidelijke en eenvoudige taal zijn gesteld. Dit is extra belangrijk indien de informatie is gericht op kinderen.

Op basis van de Richtlijn hebben organisaties momenteel een verplichting om personen op de hoogte te stellen van de manier waarop persoonsgegevens worden verwerkt. Dit wordt vaak gedaan door middel van een privacy policy. De informatieverplichting wordt in de AVG belangrijker doordat ten opzichte van de Richtlijn meer informatie moet worden verstrekt. Die informatie betreft bijvoorbeeld: de periode waarin gegevens zullen worden opgeslagen, de rechten van de betrokkene, wat de bron is van de gegevens in het geval dat deze niet rechtstreeks door de betrokkene worden verstrekt, de juridische grondslag voor de verwerking van deze gegevens, indien van toepassing: of gegevens buiten de EER worden opgeslagen en, indien van toepassing, welk gerechtvaardigd belang van de verantwoordelijke is gediend met de verwerking.

Bovenstaande informatie hoeft niet te worden verstrekt indien de betrokkene de relevante informatie al heeft of indien een vrijstelling van toepassing is. Wanneer de gegevens niet rechtstreeks van de betrokkene worden verkregen hoeft bovenstaande informatie ook niet te worden verstrekt indien de verstrekking van deze informatie onmogelijk is, onevenredig veel moeite kost, een wettelijke verplichting tot de verwerking van de gegevens bestaat of wanneer de gegevens vertrouwelijk moeten blijven omdat zij vallen onder een beroepsgeheim.

De AVG voorziet in het toekomstig gebruik van gestandaardiseerde pictogrammen om consumenten in een vereenvoudigde vorm over de procedures met betrekking tot de verwerking van persoonsgegevens te informeren.

Te nemen stappen ter voorbereiding: Hoewel de AVG uitgebreidere informatieverplichtingen introduceert is het voordeel voor organisaties dat de AVG uitgaat van een gestandaardiseerde aanpak. Eén set bepaalde standaardinformatie is waarschijnlijk voldoende om in alle lidstaten aan de wettelijke informatieverplichtingen te voldoen. Voordat de AVG in werking treedt, moeten organisaties hun privacybeleid herzien en actualiseren om de aanvullende informatieverplichtingen die de AVG introduceert te implementeren.

Toestemming

In de AVG wordt de definitie 'toestemming' ten opzichte van de Richtlijn aangescherpt. De toestemming van betrokkene tot verwerking van persoonsgegevens moet zonder dwang 'vrij' geïnformeerd, specifiek en ondubbelzinnig door middel van een verklaring of een actieve handeling worden gegeven.

Indien 'bijzondere categorieën van persoonsgegevens' worden verwerkt en toestemming vereist is, moet de toestemming uitdrukkelijk zijn. Over het algemeen zijn 'bijzondere categorieën persoonsgegevens' gevoelige persoonsgegevens zoals ras, gezondheid en politieke opvattingen, maar ook de nieuwe genetische en biometrische gegevens. Indien de verwerking is gebaseerd op de toestemming van de betrokkene ligt de bewijslast om aan te tonen dat toestemming is gegeven bij de verantwoordelijke. Betrokkenen hebben het recht om de gegeven toestemming te allen tijde in te trekken. Voordat betrokkenen toestemming geven moeten zij in kennis worden gesteld van dit recht, anders is de toestemming ongeldig.

Bij het bezoeken van een website kan toestemming worden gegeven door een vakje aan te klikken, het kiezen van bepaalde technische instellingen of door een andere verklaring of gedraging die duidelijk aangeeft dat de verwerking van persoonsgegevens wordt aanvaard. Het automatisch, impliciet aannemen van toestemming of het gebruik van vooraf ingevulde vakjes is echter onvoldoende.

Toestemming is ook niet vrij gegeven als de betrokkene geen echt vrije keuze heeft, als hij niet in staat is om te weigeren of indien het nadelig is om de toestemming in te trekken. De toestemming wordt bijvoorbeeld niet geacht vrij te zijn gegeven, als het sluiten van een overeenkomst, of het ontvangen van een dienst wordt 'gekoppeld' aan de toestemming van betrokkene om persoonsgegevens te verwerken die niet noodzakelijk zijn voor de uitvoering van de opdracht.

Waar online diensten (zoals e-maildiensten en social-media-accounts) rechtstreeks worden aangeboden aan kinderen, is toestemming van de ouders nodig voor de verwerking van persoonsgegevens. Dit geldt voor kinderen onder de 16 jaar. Afzonderlijke lidstaten kunnen wetgeving aannemen waarbij een lagere leeftijdsgrens wordt gehanteerd. Deze leeftijdsgrens mag echter niet lager dan 13 jaar zijn. Bij het afnemen van online diensten kunnen kinderen ouder dan 16 dus altijd toestemming geven om persoonsgegevens te verwerken, terwijl de kinderen onder de 13 jaar nooit dergelijke toestemming kunnen geven. Voor de leeftijden daartussen beslissen de lidstaten zelf.

Te nemen stappen ter voorbereiding: De nieuwe bepalingen over toestemming betekenen dat in de praktijk toestemming moeilijker te verkrijgen zal zijn. Organisaties die momenteel afhankelijk zijn van impliciete toestemming voor de verwerking van persoonsgegevens zullen hun activiteiten moeten herzien en hun bestaande praktijken moeten aanpassen. Het is nu duidelijk dat stilzitten, door bijvoorbeeld het niet verwijderen van een het vinkje in een aangevinkt vakje, geen geldige toestemming vormt.

Rechten van betrokkenen

De rechten die betrokkenen op basis van de Richtlijn hebben blijven gehandhaafd in de AVG. In de AVG worden echter ook nog andere rechten geïntroduceerd.

Volgens de Richtlijn hebben natuurlijke personen recht op:

- het ontvangen van bepaalde informatie (zie de hoofdstukken Informatieverplichtingen / Toestemming op de pagina's 10-11);
- inzage in persoonlijke gegevens;
- het verhinderen van het verwerken van persoonsgegevens indien er zwaarwegende en gerechtvaardigde redenen bestaan;
- bezwaar maken tegen geautomatiseerde besluitvorming;
- compensatie in geval van schade; en
- een nationale rechtsgang waarin een betrokkene kan opkomen tegen de schending van zijn rechten.

Over het algemeen zijn al deze rechten opgenomen in de AVG, maar er zijn ook nieuwe rechten bijgekomen, bijvoorbeeld:

- een 'recht om persoonsgegevens te laten wissen'. Dit recht is toepasselijk onder een groot aantal omstandigheden. Het is niet nodig om eerst een gerechtelijk bevel te krijgen;
- natuurlijke personen krijgen ruimere mogelijkheden om de verwerking van hun persoonsgegevens te beperken; en
- natuurlijke personen krijgen het recht om informatie te ontvangen via een kosteloos verzoek, tenzij het verzoek 'kennelijk ongegrond of buitensporig' is.

In de AVG is ook een nieuw 'recht op dataportabiliteit' opgenomen. Onder bepaalde omstandigheden heeft een betrokkene het recht om van de verantwoordelijke zijn gegevens in een gestructureerd, gebruikelijk en leesbaar formaat te ontvangen. Indien het technisch mogelijk is kan de betrokkene ook eisen dat deze gegevens worden overgedragen aan een andere verantwoordelijke.

Te nemen stappen ter voorbereiding: De AVG bouwt voort op de bestaande rechten die natuurlijke personen al hebben op basis van de Richtlijn. Ter voorbereiding zullen organisaties eerst hun bestaande procedures moeten nagaan om ervoor te zorgen dat die toereikend zijn om alle bestaande rechten aan te pakken. De volgende stap is dan om de nieuwe rechten, die worden geïntroduceerd door de AVG, te implementeren. Verder zal er gekeken moeten worden naar de formats waarin persoonsgegevens aan particulieren worden verstrekt. Deze moeten voldoen aan het nieuwe recht op dataportabiliteit.

Meldplicht datalekken

De Richtlijn voorziet niet in een verplichting voor verantwoordelijken om datalekken te melden aan hun nationale toezichthouder of aan betrokkenen die worden geraakt door deze inbreuk. In Nederland geldt sinds 1 januari 2016 wel een dergelijke wettelijke verplichting om datalekken te melden. De AVG introduceert een systeem van verplichte melding voor datalekken voor alle EU-lidstaten.

Op grond van de Wet bescherming persoonsgegevens moet de verantwoordelijke – zo spoedig mogelijk, doch uiterlijk binnen 72 uur – de Autoriteit Persoonsgegevens op de hoogte stellen van een datalek dat resulteert in een aanzienlijke kans op, of ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Als het datalek waarschijnlijk ongunstige gevolgen heeft voor de privacy van betrokkenen moet de verantwoordelijke ook de betrokkenen direct op de hoogte stellen. Deze informatieverplichting ten opzichte van de betrokkenen geldt niet als de voor de verwerking verantwoordelijke passende technische beschermingsmaatregelen heeft genomen die de persoonsgegevens onbegrijpelijk of ontoegankelijk maken voor iedereen die geen recht op toegang tot die gegevens heeft. De verantwoordelijke is verplicht om een overzicht van alle datalekken bij te houden. Bovenstaande meldplichten gelden niet voor telecomproviders; zij hebben op basis van de Telecommunicatiewet een eigen meldplicht. De verplichting om betrokkenen te informeren geldt niet voor financiële instellingen.

De AVG introduceert ook een meldplicht voor datalekken. Op grond van de AVG zijn verantwoordelijken verplicht om inbreuken op persoonsgegevens onverwijld te melden aan toezichthouders, waar mogelijk binnen 72 uur nadat zij

zich bewust worden van het datalek. Kennisgeving aan toezichthouders is niet vereist indien het onwaarschijnlijk is dat de inbreuk zal leiden tot een hoog risico voor de rechten en vrijheden van natuurlijke personen.

Verantwoordelijken moeten ook, zonder onnodige vertraging, datalekken aan betrokkenen melden. Deze meldplicht is alleen vereist indien de inbreuk waarschijnlijk zal resulteren in een groot risico voor de rechten en vrijheden van individuen. Betrokkenen hoeven dus, zo lijkt het, doorgaans minder snel te worden geïnformeerd over een datalek dan op grond van het huidige Nederlands regime het geval is.

Te nemen stappen ter voorbereiding: Organisaties die zich nog niet hebben ingesteld op de Nederlandse meldplicht datalekken moeten actieplannen ontwikkelen, testen en implementeren betreffende hun optreden in het geval van datalekken en crisissituaties. Organisaties moeten een duidelijk beeld hebben van deze regels, zij moeten de verschillende verantwoordelijkheden in hun organisatie duidelijk in beeld hebben, en ervoor zorgen dat er flexibele processen zijn geïmplementeerd om de naleving van deze regels te garanderen.

Functionaris voor gegevensbescherming

De AVG introduceert nieuwe eisen met betrekking tot de functionaris voor gegevensbescherming (Data Protection Officer, hierna: DPO). De Richtlijn bevat geen verplichting om een DPO te benoemen. Op basis van de AVG moeten sommige verantwoordelijken en sommige verwerkers verplicht een DPO aanstellen.

Deze eis geldt voor:

— overheidsinstanties of organen (behalve rechtbanken wanneer zij hun rechtsprekende taak uitoefenen);

— degenen die krachtens een nationale wet een DPO moeten aanstellen; en

— verantwoordelijken en verwerkers die als kernactiviteit hebben:

  - de reguliere, systematische en grootschalige controle van personen (bijvoorbeeld door middel van camera's, het monitoren van e-mail van werknemers of voertuigvolgsystemen); of
  - de grootschalige verwerking van 'bijzondere categorieën gegevens' en/of 'strafrechtelijke gegevens'. Hieronder vallen ook de nieuwe categorieën persoonsgegevens: genetische en biometrische gegevens.

De taken van een DPO zijn onder meer het adviseren van collega's, het toezicht houden op de gegevensbescherming in hun organisatie, compliance, het geven van trainingen, het uitvoeren van audits, het adviseren over privacyeffectbeoordelingen en het contact onderhouden met toezichthouders.

Te nemen stappen ter voorbereiding: Organisaties die dat verplicht zijn te doen, moeten zo snel mogelijk een DPO aanstellen. Zij moeten deze persoon trainen en ondersteunen om ervoor te zorgen dat de DPO in staat is om zijn/haar rol effectief te vervullen wanneer de AVG in werking treedt.

Doorgifte van persoonsgegevens aan derde landen

Op basis van de Richtlijn mogen persoonsgegevens niet worden overgedragen aan een land buiten de Europese Economische Ruimte (EER), tenzij er sprake is van een 'passend beschermingsniveau' of er een vrijstelling van toepassing is. De verantwoordelijkheid voor de naleving van deze regel rust op de verantwoordelijke. Onder de AVG gelden dezelfde beperkingen, niet alleen voor verantwoordelijken maar ook voor verwerkers.

Bestaande methoden om vast te stellen of er een passend beschermingsniveau aanwezig is, en de vrijstellingen voor doorgifte, zijn in grote lijnen ongewijzigd gebleven onder de AVG.

In tegenstelling tot de Richtlijn is in de AVG uitdrukkelijk voorzien in het bestaan van bindende bedrijfsvoorschriften (Binding Corporate Rules, hierna: BCR). Het gebruik ervan wordt verruimd. Niet alleen een concern maar ook een 'groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen' kunnen BCR gebruiken. Het is nog steeds nodig dat de toezichthouder van de EU-lidstaat, van waaruit persoonsgegevens worden overgedragen, de BCR goedkeurt. Deze goedkeuring is echter een 'conformiteitstoetsing' die in de AVG is opgenomen om bij te dragen aan de consistente toepassing van de AVG. Als aan de in de AVG gestelde eisen wordt voldaan, moet goedkeuring worden verleend. Aanvullende eisen, die op dit moment bestaan in verschillende lidstaten, zijn niet meer mogelijk. Het moet zodoende makkelijker worden om goedkeuring voor een BCR van een nationale toezichthouder te krijgen.

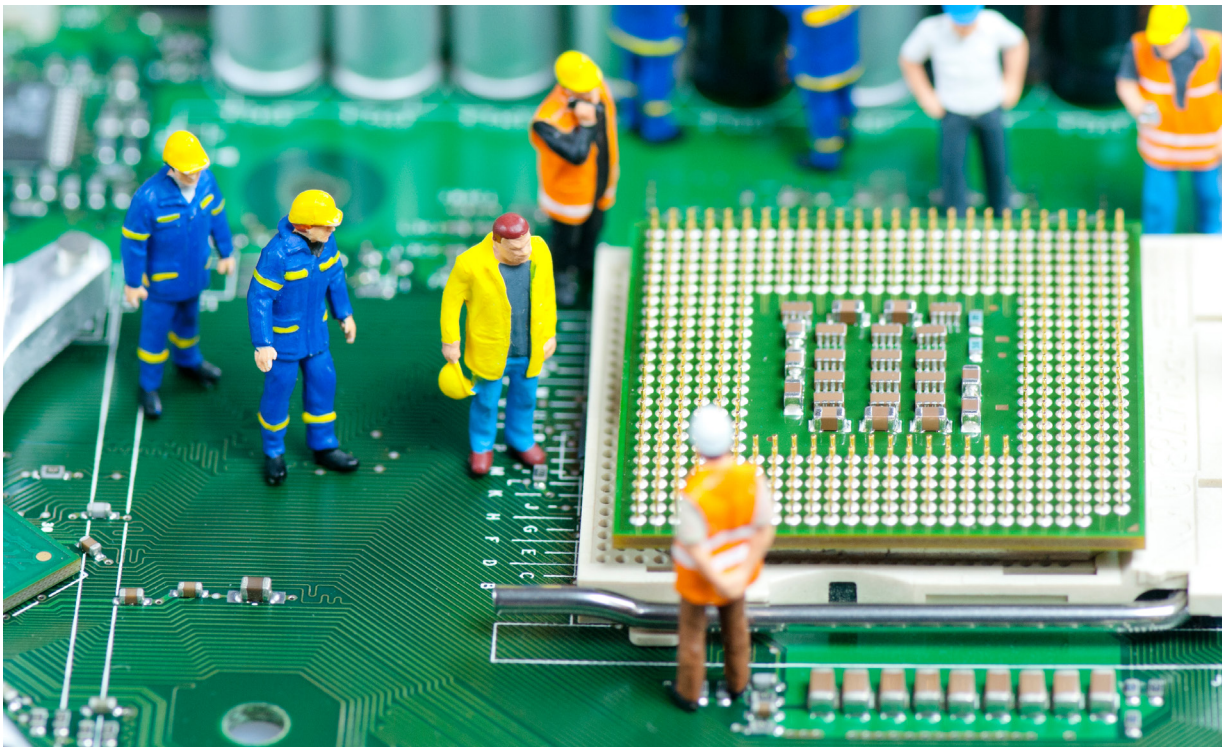
In sommige lidstaten bestaat op dit moment de mogelijkheid voor een verantwoordelijke om bij de doorgifte van persoonsgegevens aan derde landen zelf te

beslissen of er al dan niet een passend beschermingsniveau bestaat. Dit is niet meer mogelijk onder de AVG, behalve in specifieke situaties.

De AVG introduceert de mogelijkheid om persoonsgegevens door te geven indien er sprake is van een goedgekeurde gedragscode of een certificeringmechanisme tezamen met bindende en afdwingbare toezeggingen van de verantwoordelijke of de verwerker dat buiten de EER passende waarborgen bestaan. Deze mogelijkheid is opgenomen om het mogelijk te maken om naleving van de AVG aan te tonen.

Te nemen stappen ter voorbereiding: Organisaties moeten nagaan of er sprake is van internationale doorgifte van persoonsgegevens. Indien dat het geval is, moeten zij zorgen dat de doorgifte voldoet aan de wettelijke eisen van de AVG. Gezien het toenemend belang van BCR, kunnen organisaties die tot nu toe terughoudend geweest op de invoering hiervan, overwegen om BCR in te voeren binnen hun organisatie of concern.

Gegevensbescherming door ontwerp en door standaardinstellingen, anonimisering en pseudonimisering



De AVG verheft bestaande vormen van ‘best practices’ tot wettelijke verplichtingen.

Gegevensbescherming door ontwerp en door standaardinstellingen *(privacy by design and by default)*
De AVG vereist dat de verantwoordelijke passende technische en organisatorische maatregelen treft om het door de AVG vereiste beschermingsniveau te bewerkstelligen. Bij de bepaling in hoeverre sprake is van een ‘passend’ beschermingsniveau dient onder meer rekening te worden gehouden met de stand van de techniek, de implementatiekosten van de maatregel, de aard en context van de verwerking en de risico’s die met de verwerking gepaard gaan.

Welke maatregelen passend zijn dient mede te worden vastgesteld aan de hand van door de verantwoordelijke uitgevoerde risicobeoordelingen, ook wel aangeduid als ‘privacy impact assessments’.

De verantwoordelijke wordt geacht om een verwerking zodanig te organiseren (door ontwerp en standaardinstellingen) dat slechts noodzakelijke persoonsgegevens worden verwerkt. Ook dienen persoonsgegevens slechts te worden verwerkt voor het beoogde doel en niet langer te worden bewaard dan noodzakelijk is.

Gegevensbeschermingseffectbeoordeling *(privacy impact assessment)*
De AVG verplicht de verantwoordelijke tot het uitvoeren van een gegevensbeschermingseffectbeoordeling (privacy impact assessment) voor zover een verwerking gelet op haar aard, omvang, context en doel een hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen. De verantwoordelijke dient een

dergelijke beoordeling vóór aanvang van de verwerking uit te voeren. De beoordeling bevat in ieder geval een beschrijving en het doel van de verwerking, evenals een beoordeling van de noodzaak en proportionaliteit van de verwerking, een inventarisatie van de betrokken risico's en de maatregelen die zullen worden getroffen om met deze risico's om te gaan.

De AVG bevat daarnaast specifieke gevallen waarin privacy impact assessments moeten worden uitgevoerd. Toezichthouders worden bovendien geacht een lijst te publiceren met verwerkingen waarvoor het uitvoeren van een privacy impact assessment verplicht is.

Anonimisering en pseudonimisering
Anonieme gegevens (die dus niet tot een identificeerbaar individu kunnen worden herleid) vallen buiten de werkingssfeer van de AVG. In tegenstelling tot de Richtlijn erkent de AVG echter het concept 'pseudonimisering'. Dit betekent dat een persoonsgegeven zodanig wordt verwerkt dat deze niet langer tot een individu kan worden herleid zonder dat gebruik wordt gemaakt van aanvullende, afzonderlijk opgeslagen informatie. Pseudonimisering wordt door de AVG beschouwd als een technische en organisatorische maatregel om persoonsgegevens te beschermen tegen onrechtmatige verwerkingen.

Te nemen stappen ter voorbereiding: Organisaties dienen te inventariseren welke verwerkingen momenteel in de organisatie plaatsvinden en of deze verwerkingen al dan niet noodzakelijk zijn. Daarnaast dient men oog te houden voor verwerkingen die volgens de toezichthouder een privacy impact assessment vereisen. Organisaties dienen tevens te onderzoeken in hoeverre zij risicobeperkende maatregelen kunnen treffen in de vorm van anonimisering en pseudonimisering van persoonsgegevens. Bij nieuwe verwerkingen van persoonsgegevens die gepaard gaan met bovengemiddelde risico's adviseren wij om steeds een privacy impact assessment uit te voeren.

Verantwoording

De AVG introduceert verplichtingen voor organisaties om duidelijke en volledige verantwoording en rekenschap af te leggen over de wijze waarop met persoonsgegevens wordt omgegaan. Uitgangspunt hierbij is dat toezichthouders hierdoor beter kunnen controleren of verplichtingen in de praktijk daadwerkelijk worden nageleefd.

Het afleggen van verantwoording binnen het huidig regelgevend kader bestaat voornamelijk uit het melden aan de bevoegde autoriteiten van een voorgenomen verwerking. Deze verplichting, die in de praktijk vaak wordt gezien als een bureaucratische formaliteit, komt te vervallen met de inwerkingtreding van de AVG. Tegelijkertijd vereist de AVG echter dat een verantwoordelijke (en eventuele verwerker) de verwerkingsprocessen nauwkeurig administreert. Toezichthouders kunnen bovendien verzoeken om inzage in dergelijke administratie. Deze administratieplicht geldt overigens niet voor organisaties waarbinnen minder dan 250 personen werkzaam zijn, tenzij sprake is van een verwerking met een hoog risico of verwerking van bijzondere, biometrische of strafrechtelijke persoonsgegevens.

De AVG vereist tevens dat de verantwoordelijke kan aantonen dat verwerkingen geschieden in overeenstemming met de vereisten die de AVG daaraan stelt. De implicatie hiervan kan zijn dat specifiek beleid moet worden ontwikkeld en geïmplementeerd. Denk hierbij ook aan de implementatie van (al dan niet officiële) gedragscodes.

Het verantwoordingsvereiste van de AVG blijkt tot slot ook uit de verplichting om een DPO aan te stellen (zie pagina 14), het hanteren van gegevensbescherming door ontwerp en door standaardinstellingen (zie pagina 16) en het uitvoeren van privacy impact assessments (zie pagina 16).

Te nemen stappen ter voorbereiding: Organisaties dienen, voor zover zij daar niet al over beschikken, systemen te implementeren waarmee verwerkingen kunnen worden gedocumenteerd. Daarnaast raden wij organisaties aan om zoveel mogelijk aansluiting te zoeken bij gedragscodes die door toezichthouders worden gepubliceerd.

Verplichtingen voor verwerkers

De huidige Richtlijn bevat slechts een beperkt aantal zelfstandige verplichtingen voor de verwerker (daar nog bewerker genoemd) van persoonsgegevens. Met de inwerkingtreding van de AVG neemt het aantal verplichtingen voor de verwerker aanzienlijk toe.

Onder het huidige stelsel van de Richtlijn is vooral de "verantwoordelijke" degene die rekening moet houden met bestuursrechtelijke handhaving. Verwerkers kunnen veelal slechts civiel in rechte worden aangesproken voor het schenden van verplichtingen (meestal vastgelegd in bewerkersovereenkomsten). De AVG schept voor de verwerker echter een reeks directe verplichtingen, waarvan de overtreding kan resulteren in significante sancties (zie tevens pagina 23).

Enkele voorbeelden van zelfstandige verplichtingen voor de verwerker:

— het documenteren van verwerkingen;
— het aanstellen van een functionaris gegevensbescherming;
— het verkrijgen van toestemming van de verantwoordelijke alvorens een sub-verwerker in te schakelen;
— het melden van een datalek aan de verantwoordelijke;
— het treffen van passende technische en organisatorische maatregelen ter beveiliging en ter voorkoming van onrechtmatige verwerkingen;
— het verlenen van medewerking aan de bevoegde toezichthouder;
— het handelen in overeenstemming met de eisen voor doorgifte van persoonsgegevens naar derde landen buiten de EER; en
— het uitvoeren van *privacy impact assessments.*

De AVG beschrijft daarnaast een reeks contractuele waarborgen die de verantwoordelijke dient te treffen alvorens een verwerker in te schakelen. Deze waarborgen zien onder meer op geheimhouding, teruggave en/of vernietiging van persoonsgegevens en de uitvoering van audits.

Te nemen stappen ter voorbereiding: Organisaties die in hoedanigheid van verantwoordelijke of verwerker persoonsgegevens (laten) verwerken dienen hun bewerkersovereenkomsten te controleren en eventueel tot heronderhandeling over te gaan. Verwerkers dienen zich bovendien te vergewissen van hun nieuwe verplichtingen en de praktische uitvoering daarvan.

Toezicht

Lidstaten dienen reeds op grond van de huidige Richtlijn autoriteiten aan te wijzen die toezicht houden op de regels die voortvloeien uit de Richtlijn. Deze verplichting blijft in stand onder de AVG.

Een eerste vernieuwing onder de AVG is het beginsel van de 'one-stop-shop'. Dit betekent dat organisaties met vestigingen in meerdere lidstaten voortaan worden onderworpen aan het toezicht van één toezichthouder; de 'leidende toezichthouder' (de toezichthouder in de jurisdictie waar de organisatie zijn hoofdzetel heeft). Uitgangspunt is dat deze leidende toezichthouder tevens bevoegd is te handhaven ten aanzien van grensoverschrijdende verwerkingen van een dergelijke organisatie. Vindt een verwerking uitsluitend plaats in een andere lidstaat dan die van de leidende toezichthouder of heeft een verwerking substantiële invloed op betrokkenen in een andere lidstaat, dan schrijft de AVG tevens voor hoe de leidende en overige toezichthouders onderling moeten samenwerken.

Ten tweede voorziet de AVG in de oprichting van een zogeheten Europees Comité voor Gegevensbescherming (Comité), bestaande uit de voorzitters van toezichthoudende instanties van de lidstaten. Toezichthouders van de lidstaten kunnen aan het

Comité vragen om juridische opinies uit te vaardigen over vraagstukken die voor meerdere lidstaten van belang zijn, een taak die tot dusver was toebedeeld aan de zogeheten Artikel 29-Werkgroep. Daarnaast is het Comité bevoegd tot geschilbeslechting tussen toezichthouders en kan het zelfs, op verzoek van een toezichthouder, beslissingen verwerpen die zijn genomen door de leidende toezichthouder.

Te nemen stappen ter voorbereiding: Grensoverschrijdende organisaties dienen zich te realiseren in welke jurisdictie hun hoofdzetel zich bevindt. Op basis daarvan kan worden vastgesteld welke toezichthouder voor hen als 'leidend' fungeert vanaf de inwerkingtreding van de AVG in 2018.

Woordenlijst

AVG: de Algemene verordening gegevensbescherming.

Betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon van wie Persoonsgegevens worden verwerkt.

Lidstaat: een land dat is aangesloten bij de Europese Unie.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

Richtlijn 95/46/EG (ook: Richtlijn): Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Toezichthouder: een door een lidstaat ingestelde onafhankelijke overheidsinstantie.

Verantwoordelijke/Verwerkingsverantwoordelijke: de natuurlijke persoon of rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerker: de natuurlijke persoon of rechtspersoon die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt.

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Wbp: Wet bescherming persoonsgegevens.

Bijlage: bestuurlijke boetes

Relevante factoren waarmee rekening moet worden gehouden bij het bepalen van de hoogte van de boete (artikel 83 (2) AVG)

Relevante factoren	Actiepunten
De aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade.	— Voer regelmatig audits uit om potentiële risicogebieden te onderkennen en doeltreffende oplossingen te implementeren. — Wees proactief, voorkomen is altijd beter dan 'damage control'.
De opzettelijke of nalatige aard van de inbreuk.	— Ontwikkel en implementeer een duidelijk intern beleid voor de bescherming van persoonsgegevens, voer regelmatig controles uit op de naleving ervan. — Definieer privacygevoelige processen, leg de verantwoordelijkheid hiervoor bij bepaalde stakeholders, zorg ervoor dat privacy op de agenda van het bestuur komt te staan.
De door de verwerkingsverantwoordelijke of de verwerker genomen maatregelen om de door betrokkenen geleden schade te beperken.	— Reageer snel om de gevolgen van de inbreuk te beperken en om grotere schade te voorkomen.
De mate waarin de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd in het kader van gegevensbescherming door ontwerp (artikel 25) en de beveiliging van de verwerking (artikel 32).	— Zorg ervoor dat bewerkersovereenkomsten de verantwoordelijkheid en de aansprakelijkheid duidelijk verdelen tussen de verwerkingsverantwoordelijke en de verwerker.
Eerdere relevante inbreuken door de verwerkingsverantwoordelijke of de verwerker.	— Neem maatregelen om ervoor te zorgen dat een inbreuk snel wordt opgelost en zorg ervoor dat het geen terugkerend thema wordt.
De mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken.	— Wees coöperatief en werk mee met de toezichthouder, geen vertraging bij het aanpakken van inbreuken en het beperken van de gevolgen. — Wees proactief, stel zelf oplossingen voor met betrekking tot inbreuken, stel de belangen van betrokkenen voorop. — Gebruik een "front foot" benadering in de relatie met de toezichthouder.
De categorieën van persoonsgegevens waarop de inbreuk betrekking heeft.	— Zorg ervoor dat er extra beveiligingen bestaan voor bijzondere categorieën persoonsgegevens waar een hoger risico bij de verwerking bestaat.
De wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke of de verwerker de inbreuk heeft gemeld.	— Meld datalekken zo snel mogelijk aan de toezichthouder, verstrek regelmatig updates.
De naleving van de door de toezichthoudende autoriteit genomen maatregelen (artikel 58, lid 2), voor zover die al eerder ten aanzien van eenzelfde kwestie zijn genomen.	— Neem stappen om alle bezwaren van de toezichthouder aan te pakken, zorg ervoor dat het niet weer gebeurt, wees in staat om aan te tonen dat aanzienlijke inspanningen zijn gemaakt om te voldoen aan de opgelegde maatregelen.
Het aansluiten bij goedgekeurde gedragscodes (artikel 40) of van goedgekeurde certificeringsmechanismen (artikel 42).	— Houd in de gaten of er gedragscodes of een certificatiemechanisme in uw branche wordt goedgekeurd door een toezichthouder.
Elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor, zoals gemaakte financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien.	— Weeg zorgvuldig de risico's van niet-naleving af. — Zorg ervoor dat de technische en organisatorische maatregelen zo robuust maar ook zo flexibel zijn als maar mogelijk is.

Categorie 1 inbreuken Maximale hoogte boete: € 20 miljoen of 4% van de totale wereldwijde jaaromzet (indien dit hoger is) * ^
Niet voldoen aan de basisbeginselen inzake verwerking: rechtmatigheid, de voorwaarden voor toestemming, de verwerking van bijzondere categorieën van persoonsgegevens (artikelen 5, 6, 7 en 9).
Niet naleven van de rechten van de betrokkenen (artikelen 12 tot en met 22).
Doorgeven van persoonsgegevens aan derde landen zonder dat een passend beschermingsniveau bestaat en zonder dat er een vrijstelling van toepassing is (artikelen 44 tot en met 49).
Het niet naleven van specifieke wetten van de lidstaten inzake gegevensverwerking, met inbegrip van wetten betreffende de vrijheid van meningsuiting, wetten in het kader van de arbeidsverhouding, wetten betreffende toegang van het publiek tot officiële documenten, wetten inzake archivering in het algemeen belang, wetenschappelijke of historisch onderzoek of statistische doeleinden en geheimhoudingverplichtingen (hoofdstuk *IX*).
Niet-naleving van de maatregelen en bevelen van toezichthouders opgelegd in het kader van hun corrigerende en/of onderzoeksbevoegdheden (artikel 58(2) en artikel 58(1)).
Categorie 2 inbreuken Maximale hoogte boete: € 10 miljoen of 2% van de totale wereldwijde jaaromzet (indien dit hoger is) * ^
Niet naleving van de voorwaarden met betrekking tot toestemming van kinderen voor de verwerking van persoonsgegevens (artikel 8).
Niet naleven van de rechten van betrokkene indien aanvullende informatie is verkregen, waardoor de verwerkingsverantwoordelijke in staat is om betrokkene te kunnen identificeren (artikel 11).
Niet implementeren van technische en organisatorische maatregelen betreffende privacy by design (artikel 25).
Niet transparant zijn over de gezamenlijke verplichtingen van gezamenlijke verwerkingsverantwoordelijken (artikel 26).
Niet aanwijzen van een vertegenwoordiger in de EU door een verwerkingsverantwoordelijke of verwerker die niet in de EU is gevestigd (artikel 27).
Niet door de verwerkingsverantwoordelijke gebruik maken van verwerkers die voldoende garanties bieden inzake de passende technische en organisatorische maatregelen om de naleving van de AVG te waarborgen (artikel 28).
Uitbesteding van verwerking van persoonsgegevens door een verwerker zonder de voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke (artikel 28).
Niet uitsluitend in opdracht van de verwerkingsverantwoordelijke, door de verwerker persoonsgegevens verwerken (*artikel 29*).
Niet bijhouden door de verwerkingsverantwoordelijke of verwerker van een register van de verwerkingsactiviteiten (*artikel 30*).
Niet meewerken door de verwerkingsverantwoordelijke of verwerker met de toezichthouder (artikel 31).
Niet nemen van passende technische en organisatorische maatregelen door de verwerkingsverantwoordelijke of verwerker waardoor een op het risico afgestemd beveiligingsniveau is gewaarborgd (artikel 32).
Niet melden van een datalek door de verwerkingsverantwoordelijke aan de toezichthouder (artikel 33).
Niet melden van een datalek door de verwerkingsverantwoordelijke aan betrokkenen (artikel 34).
Niet verrichten van een gegevensbeschermingseffectbeoordeling door de verwerkingsverantwoordelijke en het niet voorafgaand raadplegen hierover van de toezichthouder indien noodzakelijk (artikelen 35 en 36).
Niet aanwijzen van een functionaris voor gegevensbescherming indien verplicht (artikelen 37-39).
Niet nakomen door de verwerkingsverantwoordelijke of verwerker van de verplichtingen van een gedragscode indien die van toepassing zijn (artikel 42).
Niet optreden van een toezichthoudend orgaan, dat toezicht houdt op de gedragscode, indien de verwerkingsverantwoordelijke of verwerker inbreuk pleegt op de gedragscode (artikel 41(4)).
Niet nakomen van een certificeringsinstituut van zijn verplichtingen (artikel 43).

* De lidstaten kunnen bepalen dat strafrechtelijke sanctie worden opgelegd voor overtredingen van de AVG. Ook ontneming van behaalde winsten is mogelijk. Deze sancties kunnen echter alleen worden opgelegd in plaats van, niet in aanvulling op eventuele bestuurlijke boetes of andere sancties *(overweging 149)*.

^ Wanneer bestuurlijke boetes worden opgelegd aan personen die geen onderneming zijn (dat wil zeggen organisaties die zich niet bezighouden met een economische activiteit, bijvoorbeeld overheidsinstanties) moet een toezichthouder bij het bepalen van de hoogte van de boete rekening houden met het inkomensniveau van de betreffende lidstaat, alsmede met de economische situatie van de persoon. Verder kunnen de lidstaten zelf bepalen of en in welke mate overheden moeten worden onderworpen aan administratieve boetes (*overweging 150).*

Contactpersonen

ALBANIA

Marco Lacaita
E marco.lacaita@cms-aacs.com
T +355 (0)4 430 2123

ALGERIA

Amine Sator
E amine.sator@cms-bfl.com
T +213 (7)21 69 3234

ARGENTINA

Ted Rhodes
E ted.rhodes@cms-cmck.com
T +55 21 3722 9831

AUSTRIA

Dr. Johannes Juranek
E johannes.juranek@cms-rrh.com
T +43 1 40443 2450

BELGIUM

Tom De Cordier
E tom.decordier@cms-db.com
T +32 2 743 69 13

BOSNIA AND HERZEGOVINA

Nedžida Salihović-Whalen
E nedzida.salihovic-whalen@cms-rrh.com
T +387 33 94 4610

BRAZIL

Ted Rhodes
E ted.rhodes@cms-cmck.com
T +55 21 3722 9831

BULGARIA

Nevena Radlova
E nevena.radlova@cms-cmno.com
T +359 2 923 4866

CHINA

Nick Beckett
E nick.beckett@cms-cmno.com
T +86 10 8527 0287

CROATIA

Dr. Gregor Famira
E gregor.famira@cms-rrh.com
T +385 1 4825 600

CZECH REPUBLIC

Tomas Matejovsky
E tomas.matejovsky@cms-cmno.com
T +420 296 798 852

FRANCE

Anne-Laure Villedieu
E anne-laure.villedieu@cms-bfl.com
T +33 1 47 38 55 00

GERMANY

Christian Runte
E christian.runte@cms-hs.com
T +49 89 23807 163

Michael Kamps
E michael.kamps@cms-hs.com
T +49 221 7716 372

Reemt Matthiesen
E reemt.matthiesen@cms-hs.com
T +49 89 23807 248

HUNGARY

Dora Petranyi
E dora.petranyi@cms-cmno.com
T +36 1 483 4820

ITALY

Fabrizio Spagnolo
E fabrizio.spagnolo@cms-aacs.com
T +39 06 478151

LUXEMBOURG

Julien Leclère
E julien.leclere@cms-dblux.com
T +352 26 27 53 28

MEXICO

Derek Woodhouse
E dwoodhouse@wll.com.mx
T +52 (55) 2623.0552

MONTENEGRO

Radivoje Petrikić
E radivoje.petrikic@cms-rrh.com
T +381 11 3208900

MOROCCO

Marc Veuillot
E marc.veuillot@cms-bfl.com
T +212 522 22 86 86

NETHERLANDS

Edmon Oude Elferink
E: edmon.oudeelferink@cms-dsb.com
T: +32 26 5004 54

OMAN

Ben Ewing
E ben.ewing@cms-cmno.com
T +968 2439 9905

POLAND

Tomasz Koryzma
E tomasz.koryzma@cms-cmno.com
T +48 22 520 8479

PORTUGAL

José Luís Arnaut
E joseluis.arnaut@cms-rpa.com
T +351 210 958 100

ROMANIA

Marius Petroiu
E marius.petroiu@cms-cmck.com
T +40 (0)21 407 3889

RUSSIA

Maxim Boulba
E maxim.boulba@cmslegal.ru
T +7 495 786 40 23

SERBIA

Radivoje Petrikić
E radivoje.petrikic@cms-rrh.com
T +381 11 3208900

SLOVAKIA

Ian Parker
E Ian.parker@cms-cmno.com
T +420 296 798 815

SLOVENIA

Luka Fabiani
E luka.fabiani@cms-rrh.com
T +396 (0)1 620 5210

SPAIN

Blanca Cortés Fernández
E blanca.cortes@cms-asl.com
T +34 91 451 9284

SWITZERLAND

Dr Robert G. Briner
E robert.briner@cms-vep.com
T +41 44 285 11 11

TURKEY

John Fitzpatrick
E john.fitzpatrick@cms-cmck.com
T +44 7515 787 228

UKRAINE

Olexander Martinenko
E olexander.martinenko@cms-cmno.com
T +380 44 391 33 77

Olga Belyakova
E olga.belyakova@cms-cmno.com
T +380 44 391 3377

UK

John Armstrong
E john.armstrong@cms-cmno.com
T +44 20 7367 2701

Emma Burnett
E emma.burnett@cms-cmno.com
T +44 20 7367 3565

Alan Nelson
E alan.nelson@cms-cmno.com
T +44 141 304 6006

Tom Scourfield
E tom.scourfield@cms-cmno.com
T +44 20 7367 2707

Ian Stevens
E ian.stevens@cms-cmno.com
T +44 20 7367 2597

Loretta Pugh
E Loretta.Pugh@cms-cmno.com
T +44 20 7367 2730

UNITED ARAB EMIRATES

Matthew Culver
E matthew.culver@cms-cmck.com
T +971 4 374 2805


Africa


Europe
Middle East
Asia-Pacific