

AVG EN DE IMPACT OP UW BUSINESS

AVG

De AVG, de Algemene Verordening Gegevensbescherming of de Europese Privacy Verordening, hanteert dezelfde principes en kernbegrippen als haar voorganger de Europese Privacy Richtlijn uit 1995.

In de afgelopen 20 jaar hebben technologische ontwikkelingen een vlucht hebben genomen en is de mogelijkheid om gebruik van persoonsgegevens te maken onbegrensd geworden (“big data”). De rechten en vrijheden van de betrokkene (degene over wie de gegevens gaan) zijn daarmee in het gedrang gekomen.

Vandaar dat de AVG nog meer aandacht geeft aan het herstellen van de balans tussen enerzijds het gebruik van persoonsgegevens en anderzijds de rechten en vrijheden van de betrokkene. Concreet betekent dit dat de AVG een gedetailleerder en strikter kader geeft voor het gebruik van persoonsgegevens. Deels betreft dit het vastleggen van “best practices” en jurisprudentie uit de afgelopen 20 jaar.

In onderstaand overzicht omschrijven we per artikel de verandering en de impact die dit op uw business als verantwoordelijke kan hebben. We hebben daarbij een indeling gemaakt naar “verplichtingen van de verantwoordelijke”, “rechten van de betrokkene” en “verplichtingen van de bewerker”. Deze impact hebben we direct vertaald naar actiepunten. Uiteraard met een samenvatting ter afsluiting.

Impact van de nieuwe verplichtingen voor u als verantwoordelijke

WAAR	WAT	ACTIE
Art 3	<u>Territoriale werking wordt uitgebreid.</u> Het aanknopingspunt was de vestigingsplaats van de verantwoordelijke. Onder de werking van de AVG vallen ook verantwoordelijke gevestigd buiten de EU die zich richten tot betrokkenen in de EU of hun gedrag monitoren.	• CHECK voor uw onderneming of de verwerking nu wél onder de Europese wetgeving valt, indien dit voorheen niet het geval was.
Art 5.1.e	<u>Opslag beperking.</u> In de beginselen van de gegevensverwerking is nu letterlijk omschreven dat de opslag bepaalde beperkingen moet kennen. O.a. moeten gegevens in een vorm worden opgeslagen die het mogelijk maakt de betrokkene niet langer te identificeren dan voor de doeleinden van verwerking noodzakelijk is.	• CHECK of de huidige systemen voldoen aan de vereisten voor opslag beperking (anonymisering, archiveren, beveiliging)
Art 5.2, 24, 30	<u>Aantoonbaar nakomen, documenteren verwerking en beleid.</u> De verantwoordelijke moet aantoonbaar de beginselen van verwerking nakomen. In artikel 30 wordt dit aangevuld met het bijhouden van een register alle verwerkingen door de verantwoordelijke en bewerker. Onder omstandigheden is het bijhouden van een register niet vereist (art 30 lid 5)	• MAAK BELEID waaruit blijkt dat u de beginselen nakomt. • VASTLEGGEN van de wijze waarop de beginselen van gegevensverwerking (en het beleid) worden nagekomen. Dit is het “accountability” vereiste. • CHECK of de uitzondering van art 30 lid 5 AVG voor u geldt.
Ov 32, 42, 43 Art 6, 7	<u>Grondslag toestemming wordt strikter:</u> toestemming is alleen een geldige grondslag indien dit aantoonbaar, expliciet is gegeven. In afhankelijk relaties kan niet met toestemming worden gewerkt. Indien een overeenkomst over meerdere onderwerpen gaat, dient toestemming voor een verwerking separaat te worden gevraagd, indien de overeenkomst ook zonder de toestemming kan worden uitgevoerd.	• CHECK de grondslag voor verwerking. • CHECK de wijze waarop toestemming wordt gevraagd en verkregen. • PAS zo nodig de wijze van toestemming vragen aan.
Art 6 (.1.f)	<u>Grondslag inzake gerechtvaardigd belang & kinderen wijzigt.</u> Het belang van kinderen wordt specifiek benoemd in het artikel over gerechtvaardigd belang, in die zin dat het belang van kinderen zwaarder weegt.	• CHECK of u persoonsgegevens van kinderen verwerkt, gebaseerd op de grondslag gerechtvaardigd belang, zo ja; • GA na of uw verwerking nog is toegestaan, zo nodig • STAAK de verwerking.

Art 6 (.1.f)	<u>Grondslag inzake gerechtvaardigd belang & overheid verval</u> . Overheidsinstanties kunnen in het kader van de uitoefening van hun taken geen beroep meer doen op gerechtvaardigd belang als grondslag.	• BEN U EEN OVERHEIDSINSTANTIE? Zorg dat al uw verwerkingen binnen de publieke taak vallen.
Art 8	<u>Toestemming van kinderen online</u> . Maken kinderen onder de 16 jaar gebruik van internetdiensten dan is de toestemming van ouders nodig. Dit stond op zich al in de Wbp, artikel 5.	• Als het goed is, vraagt u al om toestemming van ouders bij kinderen onder de 16 jaar. • CHECK indien u geen verantwoordelijke naar Nederlands recht bent of u aan dit vereiste voldoet. Pas het systeem zo nodig aan.
Art 9	<u>Genetische en biometrische gegevens zijn bijzondere gegevens</u> . Dus geldt een verwerkingsverbod, tenzij is voldaan aan specifieke voorwaarden.	• CHECK of u biometrische of genetische gegevens verwerkt; • PAS zo nodig de wijze van verwerken aan.
Art 10	<u>Strafbare feiten en strafrechtelijke veroordelingen vallen niet onder artikel 9</u> . Dit zijn geen bijzondere gegevens meer. Voor de verwerking van deze gegevens gelden wel specifieke eisen en voorwaarden.	• CHECK of uw verwerkingen van dit soort gegevens binnen de regels van artikel 10 AVG gebeurt (bijvoorbeeld onder toezicht van de overheid).
Art 12	<u>Termijn voor reactie op uitoefening rechten betrokkene 1 maand</u> . Dit is in de Wbp 4 weken.	• CHECK uw procedures voor de omgang met rechten van betrokkenen. • PAS zo nodig de protocollen aan op de termijn van 1 maand.
Art 12.5	<u>Verstreking van inzage is kosteloos</u> . Tenzij het verzoek buitensporig of ongegrond is. Onder de Wbp mochten wel kosten in rekening worden gebracht.	• PAS uw beleid aan. Er mogen – in principe - geen kosten meer in rekening worden gebracht voor het verstrekken van de informatie naar aanleiding van een inzageverzoek.
Art 13 en 14	<u>Informatieverstreking meer specifiek</u> . De informatieverstreking bij het verkrijgen van persoonsgegevens rechtstreeks van de betrokkene is specifieker en uitgebreider (13), maar ook indien de gegevens niet rechtstreeks van de betrokkene worden verkregen (14)	• PAS uw privacy statement, privacy policy of privacy verklaring tijdig aan; • CHECK uw informatieverstreking voor de gevallen dat u via een andere partij persoonsgegevens verkrijgt.
Art 25	<u>Implementeren privacy by design en privacy by default</u> . Dit was al een uitgangspunt onder de Wbp, maar nu is het een letterlijke verplichting in de AVG.	• PAS zo nodig de wijze waarop aankopen voor systemen worden gedaan (aanbesteding, offerte, opdracht) of de wijze waarop systemen worden ontwikkeld aan.

Art 26	<u>Gezamenlijke verantwoordelijken leggen rolverdeling vast.</u> Indien sprake is van gezamenlijke verantwoordelijkheid dan dienen de partijen een aantal zaken af te spreken en vast te leggen.	• CHECK of bij een van uw verwerkingen sprake is van gezamenlijke verantwoordelijkheid. • DOCUMENTEER de afspraken die u conform artikel 26 AVG moet maken.
Art 28	<u>Aanstelling bewerker strikter.</u> Er mag alleen een bewerker worden ingeschakeld als deze afdoende beveiligingsgarantie biedt en de bewerker mag alleen op basis van schriftelijke instructies verwerken. Ook wordt de inhoud van de bewerkersovereenkomst specifiek omschreven.	• CHECK de bestaande relaties met bewerkers en de bestaande bewerkersovereenkomsten aan de inhoud van dit artikel; • PAS dit artikel toe op de nieuwe relaties met bewerkers.
Art 33, 34	<u>Meldplicht datalekken.</u> Deze wijkt op bepaalde punten af van de in de Wbp ingevoerde meldplicht datalekken. Zo geldt de meldplicht in de AVG wel in zijn geheel voor instanties die onder de Wft vallen.	• CHECK uw draaiboek datalekken; • PAS zo nodig het draaiboek datalekken aan; • VALT U ONDER DE WFT? Dan bent u onder de AVG wel verplicht om onder omstandigheden te melden aan de betrokkene.
Art 35	<u>Privacy Impact Assessment.</u> In specifiek omschreven situaties is het uitvoeren van een PIA verplicht. Het artikel omvat meer verplichtingen en bepalingen over het vooraf inschatten van het effect van een verwerking dan alleen het uitvoeren van een PIA!	• CHECK of voor u de PIA verplichting geldt; • VOOR tijdig en correct een PIA uit; • CHECK uw beleid aan art 35, in dit artikel staan meer effect-beoordelingsverplichtingen dan het uitvoeren van een PIA;
Art 37, 38, 39	<u>Aanstellen DPO.</u> Indien sprake is van de specifieke situaties als omschreven in art 37 moet uw organisatie een data protection officer, een functionaris voor de gegevensbescherming, aanwijzen.	• CHECK of u verplicht bent een FG te aan te wijzen; • BENOEM zo nodig een FG.
Art 40, 41, 42, 43	<u>Gedragscodes en certificering.</u> Er zijn een aantal verplichtingen waaraan u kunt voldoen, of geacht wordt aan te voldoen, indien u zich aansluit bij een gedragscode of een certificering verkrijgt.	• CHECK of er gedragscodes of certificeringen zijn waarmee u aan verplichtingen uit de AVG kunt voldoen.
Art 83	<u>Hoge boetes.</u> De boetes voor overtreding van de AVG zijn hoog. Er kan maximaal een boetebedrag van EUR 20.000.000,00 of een bedrag gelijk aan 4% van de totale wereldwijde jaaromzet van het voorgaande boekjaar worden opgelegd.	• CHECK of u voldoet aan alle verplichtingen uit de AVG, de boetes op overtreding zijn hoog.

Impact van de nieuwe rechten van de betrokkene voor u als verantwoordelijke

WAAR	WAT	ACTIE
Art 17, 19, 23	<u>Recht om vergeten te worden</u> . “Het recht op vergetelheid” zoals het in de Nederlandse vertaling wordt genoemd. Artikel 17 en 19 bepalen wanneer dit recht terecht kan worden ingeroepen en hoe dit moet worden uitgevoerd.	• CHECK of het mogelijk is in uw systemen om de uitoefening van dit recht te effectueren; • PAS zo nodig uw systemen aan; • PAS uw beleid aan op dit nieuwe recht, de voorwaarden en de wijze waarop u dit dient te effectueren (“zonder onredelijke vertraging wissen”)
Art 20, 23	<u>Recht op dataportabiliteit</u> . “Het recht op overdraagbaarheid” zoals het in de Nederlandse tekst van de AVG staat. Artikel 20 bepaalt onder welke voorwaarden en hoe dit recht kan worden uitgeoefend en hoe dit door de verantwoordelijke wordt uitgevoerd.	• CHECK of het mogelijk is in uw systemen om de uitoefening van dit recht te effectueren; • PAS zo nodig uw systemen aan; • PAS uw beleid aan op dit nieuwe recht, de voorwaarden en de wijze waarop u dit dient te effectueren.
Art 21,22, 23	<u>Recht om bezwaar te maken tegen profiling</u> . De betrokkene mag tegen geautomatiseerde beslissingen, gebruik van gegevens voor direct marketing en tegen profilering bezwaar maken. De voorwaarden waaronder dit recht kan worden uitgeoefend en hoe dit moet worden gerespecteerd, staan op specifieke wijze omschreven in artikel 21 en 22.	• CHECK of het mogelijk is in uw systemen om de uitoefening van dit recht te effectueren; • PAS zo nodig uw systemen aan; • PAS uw beleid aan op dit nieuwe recht, de voorwaarden en de wijze waarop u dit dient te effectueren.

Impact van de rechtstreekse verplichtingen voor bewerkers voor u als verantwoordelijke

WAAR	WAT	ACTIE
	De bewerker had hooguit een verplichting tot beveiliging en geheimhouding op basis van de Wbp. Onder de AVG krijgt de bewerker een aantal specifieke verplichtingen. Dit verandert het proces van totstandkoming van een bewerkers-overeenkomst, omdat de financiële belangen en aansprakelijkheden van een bewerker veranderen. Dit verandert ook uw positie ten opzichte van de bewerker. Indien een bewerker de algemene verplichtingen uit de AVG niet nakomt, dan kan dit voor u een negatieve uitwerking hebben. U bent immers verantwoordelijk voor de keuze om met deze specifieke bewerker zaken te doen.	• BEGIN TIJDIG met onderhandelen indien u nieuwe bewerkersovereenkomsten gaat afsluiten. De positie van de bewerker is veranderd, de gesprekken zullen anders zijn; • HOUD REKENING met een veranderde onderhandelingspositie van de bewerker; • PAS TIJDIG de bestaande bewerkersovereenkomsten aan, voordat uw bewerker zijn positie gaat uit spelen; • NEEM de wettelijke verplichtingen voor de bewerker op in de bewerkersovereenkomst! Dan is een overtreding niet alleen onrechtmatig, maar kunt u op grond van de overeenkomst wellicht aanspraak maken op boetbedragen, korte verzuimtermijnen, beëindiging van de overeenkomst. • ASSISTEER zo nodig uw bewerker bij het nakomen van de nieuwe verplichtingen. U heeft een soort onderzoeksplicht naar de bewerker, artikel 28.1 AVG, dus kan het voor u nadelig zijn als uw bewerker de hoofdverplichtingen uit de AVG niet nakomt. Al is het maar omdat hierdoor rechten en vrijheden van betrokkene in het gedrang kunnen komen. En dat zijn úw klanten, werknemers, patiënten of leden.

Art 27	<u>Aanwijzen vertegenwoordiger</u> . Indien artikel 3 lid 2 van toepassing is (de bewerker is buiten de Europese Unie gevestigd) wijst de bewerker schriftelijk (!) een vertegenwoordiger aan in de Europese Unie.	• CHECK of uw bewerker aan deze verplichting voldoet.
Art 28	<u>Vastleggen afspraken met bewerker</u> . Dit gehele artikel gaat over de positie, taken en verplichtingen van de verwerker. In lid 2 staat dat enkel met voorafgaande specifieke of algemene toestemming van de verantwoordelijke een sub-bewerker mag worden ingeschakeld. In lid 3 staan de onderwerpen die tenminste in de bewerkersovereenkomst moeten staan.	• CHECK de bestaande bewerkersovereenkomsten; • PAS zo nodig de bestaande bewerkersovereenkomsten aan.
Art 29	<u>Vereiste van een opdracht en instructies</u> . De bewerker mag alleen in opdracht van de verantwoordelijke handelen en moet instructies krijgen. Nieuw is dat deze verplichting rechtstreeks aan de bewerker wordt opgelegd.	• CHECK of de inhoud van de bestaande bewerkersovereenkomst overeenkomt met de verwerkingen die de bewerker verricht; • PAS zo nodig de bestaande bewerkersovereenkomsten aan.
Art 30.2	<u>Bijhouden van register van verwerkingen</u> . de bewerker moet een overzicht bijhouden van alle categorieën persoonsgegevens die in opdracht van de verantwoordelijke worden verwerkt, tenzij lid 5 van toepassing is.	• CHECK of bij uw bewerkers sprake is van de uitzonderingssituatie als omschreven in art 30.5; • WIJS uw bewerkers op de verplichting van art 30; • ASSISTEER zo nodig uw bewerkers bij het nakomen van de verplichting van art 30 AVG.
Art 31	<u>Samenwerken met toezichthouder</u> . Ook de bewerker moet desgevraagd samenwerken met de toezichthouder.	• MAAK EEN AFSpraak met de bewerker dat u direct op de hoogte wordt gesteld zodra de bewerker een dergelijk verzoek ontvangt. Een onderzoek kan zich namelijk ook uitbreiden naar uw activiteiten.

Art 32	<u>Beveiligingsverplichting.</u> de beveiligingsverplichting geldt ook voor de bewerker. Wordt gebruik gemaakt van sub-bewerker dan gelden er extra eisen.	• CHECK de bewerkersovereenkomst op afspraken over de beveiliging. Als het goed is, is dit al geregeld; • PAS zo nodig de bewerkersovereenkomst aan.
Art 33	<u>Melding datalek.</u> bewerkers moeten onverwijld de verantwoordelijke op de hoogte stellen van een datalek.	• PAS de bewerkersovereenkomst aan. Als het goed is heeft u dit in het kader van artikel 34a Wbp al gedaan.
Art 35	<u>PIA.</u> Onder omstandigheden heeft de bewerker de verplichting om een PIA uit te voeren.	• PAS de bewerkersovereenkomst aan. Overtreding van een wettelijke verplichting door de bewerker kan onrechtmatig zijn jegens u. Voor u is het praktischer als dit op grond van de bewerkersovereenkomst ook een overtreding is, zodat gefixeerde boetes uit de overeenkomst geldig zijn of beëindiging mogelijk is.
Art 37	<u>Aanstellen DPO.</u> De bewerker is in bepaalde gevallen verplicht om zelf een DPO, data privacy officer, aan te stellen.	• CHECK of deze verplichting voor uw bewerker geldt; • PAS zo nodig de bewerkersovereenkomst aan.

ACTIEPUNTEN SAMENGEVAT

- **DOCUMENTEER:** de AVG bevat een omvangrijke documentatieverplichting. Beoordeel of u onder de uitzonderingen valt. Zo niet, zorg dat u alle registers behoudt.
- **MAAK BELEID:** stel een privacybeleid op wat van toepassing is op alle soorten verwerkingen die u binnen uw organisatie doet.
- **VOER AUDITS UIT EN LEG DE UITKOMSTEN VAST:** u moet aantoonbaar voldoen aan diverse verplichtingen. Een beleid opstellen is een goede eerste stap. Dit beleid moet in de praktijk ook worden nageleefd. Dit controleert u door een audit, quickscan of uitgebreide PIA.
- **BEVEILIG:** neem technische beveiligingsmaatregelen en houd deze up to date. Neem ook organisatorische beveiligingsmaatregelen en train uw medewerkers met regelmaat. Dit was al een verplichting. De hoge boetes uit de AVG maken dat dit onderwerp extra aandacht verdient. Ook omdat gebrek aan beveiliging en/of datalekken vaak aanleiding is voor de start van een onderzoek door een toezichthouder.
- **PIA:** ga na of voor u of uw bewerker de verplichting geldt om een privacy impact assessment uit te voeren. Zo ja, begin hier tijdig mee, voer de PIA zorgvuldig uit en neem actief actie aan de hand van de uitkomsten.
- **PRIVACY OFFICER:** ga na of de verplichting tot het aanstellen van een data protection officer, een functionaris voor de gegevensbescherming, voor u en/of uw bewerker geldt. Zo ja, stel deze persoon aan.
- **PAS SYSTEMEN AAN:** de betrokkenen krijgen nieuwe rechten. Sommige bestaande rechten veranderen. U dient ervoor te zorgen dat de betrokkenen deze rechten kan uitoefenen. Hiervoor zijn soms aanpassingen aan systemen nodig.
- **PAS BEWERKERSOVEREENKOMSTEN AAN:** De positie van de bewerker verandert. Neem in ieder geval de rechtstreekse verplichtingen voor de bewerker uit de AVG ook op in de bewerkersovereenkomst. Maak de bewerker onderdeel van uw nieuwe verplichtingen uit de AVG.
- **PAS PRIVACY STATEMENT AAN:** De informatieverschaffing aan betrokkenen is essentiëler en gedetailleerder geworden. Pas tijdig uw privacyverklaring aan.
- **GRONDSLAG CHECK:** In ieder geval de mogelijkheid om gebruik te maken van de grondslag toestemming verandert sterk. Ga na welke grondslagen u gebruikt en of deze conform de AVG op een geldige wijze worden gebruikt.
- **PAS PROCEDURES VOOR AANSCHAF ICT-SYSTEMEN AAN:** Naast de verplichte PIA wordt het toepassen van de principes van privacy by design en default een verplichting. Neem deze verplichting mee in de afspraken met opdrachtnemers.

Wij voeren en Privacy Quickscan uit voor Euro 850,00 ex BTW
Of bel gerust voor vrijblijvend overleg: 06 – 50 54 20 66

Alle informatie van www.privacy-advocaat.nl is met zorg samengesteld, maar wij garanderen niet dat deze juist of volledig is en ook niet dat de informatie voor uw situatie passend is. De interpretatie van privacywetgeving is aan verandering onderhevig en hangt af van feiten en omstandigheden. Voor een passend en actueel advies verzoeken wij u contact op te nemen.