25-5-2017

WHITEPAPER ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

Nog één jaar te gaan: wat moet u weten? | Privacy team - Köster Advocaten

Wetgeving

Huidige wetgeving

Op dit moment geldt in Europa nog de Privacyrichtlijn 95/46/EG van 24 oktober 1995 (hierna: de ñ**Privacyrichtlijn**ò). Deze Privacyrichtlijn legt op dit moment aan iedere lidstaat van de EU de verplichting op om de nationale wetgeving aan te passen zodat deze minimaal voldoet aan de vereisten van de richtlijn (*minimumharmonisatie)*. In alle lidstaten van Europa is de nationale wetgeving ten aanzien van de bescherming van persoonsgegevens met deze richtlijn als uitgangspunt opgesteld. In Nederland is dat gebeurd in de Wet bescherming persoonsgegevens (ñ**Wbp**ò).

Dit heeft ervoor gezorgd dat de wetgeving in de EU uiteenloopt. Ook heeft ieder land een eigen handhavende instantie, met een eigen beleid. In Nederland is dat de Autoriteit Persoonsgegevens (tot 2015: College bescherming persoonsgegevens).

Nieuwe wetgeving: de Algemene Verordening Gegevensbescherming

Sinds 1995 (de inwerkingtreding van de Privacyrichtlijn) is er nogal wat veranderd op het gebied van digitale verwerking van (persoons)gegevens. Er worden op dit moment meer persoonsgegevens dan ooit verzameld en verwerkt door organisaties. De Privacyrichtlijn voldeed niet meer aan de eisen die de huidige tijd stelt.

De Privacyrichtlijn gaat zoals gezegd uit van het principe van minimumharmonisatie. De AVG neemt afstand van dit principe.

Of dit daadwerkelijk voor uniforme regels en handhaving binnen de EU gaat zorgen, is overigens nog de vraag. De AVG staat, net als de Wbp, bol van de óvage normenô en óopen begrippenôdie door de nationale toezichthouders en nationale rechters moeten worden uitgelegd en toegepast. Dat is ook de reden dat op dit moment nog veel vragen zijn over de uitleg en toepassing van de AVG. De verschillen normen en waarden in de diverse lidstaten zullen zo binnen de EU in de loop der tijd worden uitgekristalliseerd, dat onvermijdelijk zal leiden tot een verschillende uitwerking van dezelfde regels in de verschillende landen.

1. Mogen wij de persoonsgegevens (nog) wel verwerken?

De AVG formuleert zes basisbeginselen waaraan alle verwerkingen van persoonsgegevens moeten voldoen, als de gegevensverwerking van uw organisatie aan deze beginselen voldoet, is verwerking in principe toegestaan.

U kunt via een Privacy Impact Assessment (laten) nagaan of bepaalde gegevens verwerkingen in overeenstemming zijn met deze basisbeginselen.

De basisbeginselen zijn:

a. **Rechtmatigheid, behoorlijkheid en transparantie**: informatie over de verwerking moet eenvoudig toegankelijk en begrijpelijk zijn, in heldere (niet-juridische) taal. Dit heeft betrekking op alle communicatie, uw privacy statement en het afhandelen van inzageverzoeken en bezwaren.
b. **Doelbindingsprincipe**: u dient welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te formuleren voor het verwerken van persoonsgegevens. Verwerken voor ñbedrijfsdoeleindenò is niet specifiek genoeg. De persoonsgegevens die rechtmatig zijn verkregen voor bepaalde doeleinden, mogen niet voor andere doeleinden worden gebruikt.
c. **Dataminimalisatie**: u kunt alleen de noodzakelijke gegevens verzamelen (gelet op het doel waarvoor u deze verzamelt). Persoonsgegevens moeten zo snel mogelijk worden vernietigd zodra ze niet meer relevant zijn. Zo mogen gegevens van een sollicitant na afwijzing niet zonder toestemming langer bewaard worden dan gedurende de sollicitatieprocedure.
d. **Juistheidsprincipe**: u bent verplicht om ervoor te zorgen dat de gegevens niet onjuist of achterhaald zijn.
e. **Opslagbeperking**: bewaar de persoonsgegevens niet langer dan noodzakelijk. De AVG bevat, net als de Wbp, geen specifieke bewaartermijnen maar alleen algemene normen. Daarvoor geldt: documenteer duidelijk welke bewaartermijnen worden gehanteerd en waarom. Let op dat de bewaartermijnen wel in andere wetten kunnen zijn vastgelegd. Fiscale wetgeving eist bijvoorbeeld dat de administratie gedurende 7 jaar wordt bewaard. Hiermee worden de bewaartermijnen voor u ingevuld.
f. **Integriteit en vertrouwelijkheid**: de verantwoordelijke moet passende technische en organisatorische maatregelen nemen om te voorkomen dat er ongeoorloofde toegang of ongeoorloofd gebruik van de persoonsgegevens mogelijk is. Een inbreuk moet worden gemeld (meldplicht datalekken) Hierover later nog meer.
g. **Verantwoordingsplicht**: de verantwoordelijke moet kunnen aantonen dat zij zich houdt aan de AVG. Dit betekent in feite een documentatieplicht. Uit de documentatie dient te blijken op welke manier de naleving is gewaarborgd. Hoe zijn de systemen beveiligd, op welke manier worden gegevens verkregen en verwerkt? Wie heeft daar toegang toe? Waarom worden deze gegevens verwerkt? Is dat noodzakelijk? Hoe wordt aan het dataminimalisatieprincipe voldaan? Welke bewaartermijnen worden gehanteerd? En is vernietiging na afloop van de termijn geautomatiseerd? Etc. Als de toezichthouder een vermoeden heeft dat uw organisatie de verplichtingen niet naleeft, dan moet uw organisatie kunnen aantonen dat zij dat wel doet. Lukt dat niet, dan staat vast dat uw organisatie de wet overtreden heeft.

2. Moet er een bewerkersovereenkomst worden gesloten?

Een bewerker is de partij die uw organisatie als verantwoordelijke inschakelt, om persoonsgegevens te verwerken. Zo is bijvoorbeeld een SAAS-dienstverlener in de meeste gevallen een bewerker, omdat zij de database waarin de persoonsgegevens van uw klanten staan, beheert en host.

De AVG stelt het verplicht om een bewerkersovereenkomst te sluiten met partijen aan wie uw organisatie de opdracht geeft om persoonsgegevens te verwerken. De AVG noemt het overigens een verwerker en dus ook een ñverwerkersovereenkomstò

De AVG bepaalt dat ook de bewerker hoofdelijk aansprakelijk is voor schade van de betrokkenen, indien de schade is veroorzaakt doordat de bewerker onvoldoende technische en organisatorische maatregelen heeft getroffen. Let er dus op dat uw organisatie vanaf volgend jaar dus ook als bewerker rechtstreeks aansprakelijk kan worden gesteld op basis van de wet! Belangrijk is in dat kader dat de AVG de bewerker letterlijk verbiedt om een sub-bewerker in te schakelen, zonder toestemming van de verantwoordelijke. Doet u dat wel, dan is uw organisatie dus aansprakelijk voor alle schade. Zo kan uw bedrijf bijvoorbeeld een partij inhuren die de webshop bouwt en onderhoudt (dat is de bewerker). De webshop bouwer zal weer de webshop en de database met persoonsgegevens van uw klanten laten hosten door een hostingpartij / datacenter. Dat datacenter is dan een sub-bewerker.

De AVG bepaalt dat de verwerkersovereenkomst op schrift moet staan (elektronisch is ook mogelijk). Mondelinge afspraken zijn dus niet voldoende. Het is toegestaan om deze overeenkomst in de algemene (inkoop)voorwaarden te integreren. De AVG stelt een behoorlijk aantal inhoudelijke eisen aan de verwerkersovereenkomst, zoals: de verwerker verwerkt persoonsgegevens uitsluitend op basis van schriftelijke instructies van de verwerkingsverantwoordelijke; de bewerker heeft een geheimhoudingsverplichting opgelegd aan werknemers, de bewerker neemt alle vereiste technische en organisatorische maatregelen en de verwerker werkt mee aan een audit van de verantwoordelijke.

Het is aan te raden om in de verwerkersovereenkomst alvast afspraken te maken over de audits (wie draagt de kosten, en wanneer? Bijvoorbeeld alleen indien sprake is van een niet-naleving van de afspraken?) en aansprakelijkheid in geval van klachten of boetes.

Daarnaast geldt dat de verwerker ook een register bijhoudt van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit register heeft dezelfde inhoudelijke eisen als het register van de verantwoordelijke zelf (zie hiervoor bij vraag 6).

3. Hebben wij toestemming nodig van de betrokkenen om de gegevens te verwerken?

Toestemming is alleen nodig, als er geen andere wettelijke grondslag is aan te wijzen. De AVG biedt de volgende grondslagen:

- Als het noodzakelijk is ter uitvoering van een overeenkomst waarbij de betrokkenen partij zijn. Daarbij geldt de norm dat zonder verwerking van persoonsgegevens de overeenkomst niet kan worden uitgevoerd[1]. Denk bijvoorbeeld aan adresgegevens die nodig zijn voor levering van een besteld product.
- Noodzakelijk om te voldoen aan een wettelijke verplichting. Vb. verstrekken gegevens van betrokkenen aan de belastingdienst of de Politie (in sommige gevallen).
- Noodzakelijk voor de vitale belangen van de betrokkenen. Vb. medische gegevens bij een ongeval.
- Noodzakelijk voor de uitvoering van een taak van algemeen belang of openbaar gezag (geldt m.n. voor overheidsinstanties en andere instanties die het algemeen belang behartigen).
- Noodzakelijk voor de behartiging van gerechtvaardigde belangen van uw organisatie of van een derde. Hierbij dient een belangenafweging te worden gemaakt, en deze dient u te documenteren (gezien op het verantwoordingsprincipe zie hiervoor). Gerechtvaardigde belangen kunnen zijn: fraudepreventie, direct marketing, doorzending binnen een concern, of als het nodig is met het oog op netwerk- en informatiebeveiliging (denk aan overheidsinstanties en computer security incident response teams).

Biedt bovenstaande onvoldoende grondslag voor uw activiteiten met persoonsgegevens, dan is toestemming nodig. Let op dat het vragen van toestemming ook aan regels gebonden is. De AVG is zeer expliciet over de wijze waarop geldige toestemming verkregen moet worden.

[1] Rb. Utrecht 21/3/2012, OV-chipkaart studenten

Daarnaast gelden er aanvullende regels voor bijzondere persoonsgegevens (zoals medische gegevens, ras, het BSN en strafrechtelijke gegevens). Bij het verwerken van een kopie ID en een pasfoto zal er altijd sprake zijn van het verwerken van bijzondere persoonsgegevens. In dat geval is het te allen tijde aan te raden juridisch advies in te schakelen.

4. Wij zijn een vestiging of dochter van een Amerikaans bedrijf, is de AVG wel op ons van toepassing?

Jazeker, als de organisatie (of een vestiging) in de EU gevestigd is, zelfs als de activiteit van de vestiging gering is, is de AVG van toepassing[2]. Daarbij is van belang dat ook een handelsagent kan kwalificeren als vestiging. Deze agent verzamelt de gegevens immers ten behoeve van de onderneming. Veel Amerikaanse bedrijven (Facebook, Microsoft) hebben Europese dochterondernemingen.

5. Wij pseudonimiseren alle gegevens, is dat voldoende om onder de verplichtingen uit te komen? En hoe zit het met anonimiseren?

Er is sprake van een persoonsgegeven, als een natuurlijk persoon identificeerbaar is aan de hand van de gegevens die beschikbaar zijn. Daarvoor geldt dat identificatie niet noodzakelijk *direct* mogelijk hoeft te zijn, maar het kan ook *indirect*, door het inzetten van (redelijke) middelen. Ook door enkel locatiegegevens en kenmerken kan iemand te identificeren zijn.

Daarnaast hoeft het ook niet zo te zijn dat uw organisatie de personen zelf kan identificeren. Als een andere organisatie dat wél kan, dan is er ook sprake van persoonsgegevens. Bijvoorbeeld: een kenteken van een auto is een persoonsgegeven, ook al is het niet voor iedereen mogelijk de eigenaar te achterhalen. Het RDW kan namelijk wél de personen aan deze auto koppelen.

Is het **pseudonimiseren** voldoende om onder de AVG uit te komen?

Pseudonimisatie maakt identificatie lastiger, maar vaak niet onmogelijk. Daarom is de AVG wel van toepassing, maar wordt pseudonimiseren aangemerkt als een mogelijk passende waarborg (artikel 6 AVG) en beveiligingsmaatregel (art. 33 AVG). Het automatisch inbouwen van pseudonimiseren van persoonsgegevens is aan te merken als een onderdeel van privacy-by-design (25 AVG) en wordt door de Europese en Nederlandse instanties toegejuicht.

Hoe ziet het met **anonimiseren**?

Het weglaten van naam en contactgegevens is niet voldoende. Een klantnummer koppelen aan bepaalde transactiedata zal zeer waarschijnlijk toch nog tot een herleidbaar persoon leiden en dat betekent dat er toch sprake is van persoonsgegevens. **Aggregatie** of **randomiseren** van gegevens kan wél leiden tot anonieme gegevens waarop de AVG niet van toepassing is. Vraag uw dataspecialist hoe u dit kunt realiseren.

6. Wij slaan gegevens alleen maar op, maar doen er verder niets mee. Is de AVG dan wel van toepassing?

Iedere denkbare handeling met persoonsgegevens is het verwerken daarvan. Zelfs het opslaan, wissen en vernietigen.

De AVG definieert: *een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, als dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending,*

[2] HvJ Weltimmo

verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Sinds het Costeja-arrest (Google arrest, HvJ EU 13 mei 2014, C-131/12) is ook duidelijk dat indexatie en beschikbaarstelling door zoekmachines als verwerking wordt aangemerkt. En sinds het Lindqvist arrest (C-101/01) is duidelijk dat publiceren via internet ook als verwerking is aan te merken.

Het kan ook zo zijn dat uw organisatie de gegevens opslaat en bewaart voor een andere organisatie. In dat geval kwalificeert uw organisatie niet als verantwoordelijke, maar als bewerker (verwerker) van persoonsgegevens. Dat betekent niet dat u geen verplichtingen heeft op basis van de AVG. U dient beveiliging van de persoonsgegevens (de ñtechnische en organisatorische maatregelenò) op een goed niveau te houden. Daarbij mag rekening worden gehouden met de stand van de techniek, de gevoeligheid van de persoonsgegevens en de kosten die ermee gemoeid zijn. Ook zal u met de verantwoordelijke een bewerkersovereenkomst moeten sluiten (zie hieronder bij vraag 9).

7. Welke rechten hebben de personen waarvan wij persoonsgegevens verwerken?

De natuurlijk personen wiens persoonsgegevens worden verwerkt worden ñbetrokkenenò genoemd. De AVG beschermt de betrokkenen vergaand. Een aantal belangrijke rechten waar u rekening mee zal moeten houden zijn.

Inzagerecht en verzoeken ten aanzien van persoonsgegevens.

Uw organisatie is verplicht verzoeken van betrokkenen voortvarend af handelen. De AVG schrijft voor: onverwijld maar uiterlijk binnen een maand. Er dient in ieder geval binnen één maand een mededeling te worden gedaan waarom het verzoek zonder gevolg is gebleven en dat er een mogelijkheid is om een klacht in te dienen bij de toezichthoudende autoriteit en beroep bij de rechter. Dit alles dient kosteloos te gebeuren.

Recht op rectificatie

De betrokkene heeft een in de AVG verankerd recht om fouten te laten corrigeren. Hieronder valt ook een naamswijziging na het aangaan van een huwelijk.

Recht op dataportabiliteit

Dit recht wordt door de AVG nieuw geïntroduceerd. Dit recht geeft de betrokkene de mogelijkheid een kopie van zijn persoonsgegevens te eisen die bruikbaar is bij een andere vergelijkbare dienstverlener. Een voorbeeld daarvan is een lijst met de muziek die via een streamingdienst zijn beluisterd en de gezondheid- en hartslaggegevens die via een activity-tracker zijn verzameld van een gebruiker. Deze gegevens moeten in een gestructureerde, gangbare en machinaal leesbare vorm door de gebruiker direct kunnen worden gedownload.

Recht op vergetelheid

De uitspraak van het Hof van Justitie in de Costéja-zaak (het ñGoogle-arrestò), waarin een recht om vergeten te worden aan de orde was, staat op gespannen voet met vrijheid van meningsuiting en het beginsel dat de integriteit van archieven gewaarborgd moeten worden. De AVG stelt daarom beperkingen aan dit recht op vergetelheid. Zo dient er een belangenafweging gemaakt te worden.

Bij verwerking van persoonsgegevens voor ñdirect marketingò dient een bezwaar van een betrokkene in beginsel altijd gehonoreerd te worden. Als een betrokkene zijn of haar eerder gegeven toestemming intrekt, mag het verzoek tot wissen van de gegevens worden geweigerd als er ook nog een andere (wettelijke) grondslag is die de verwerking rechtvaardigt.

Voorbeeld: iemand heeft toestemming gegeven om persoonsgegevens te verwerken in het kader van het gebruik van een smartphone app voor het bijhouden van zijn of haar gezondheid en beweging. Voor het gebruik van de smartphone app is een abonnement afgesloten. Als die persoon vervolgens de toestemming op het gebruik van persoonsgegevens intrekt, maar het abonnement niet beëindigt, dan is verwerking van de persoonsgegevens alsnog gerechtvaardigd op grond van de uitvoering van de overeenkomst. Beëindigt hij ook het abonnement, dan dient de gegevensverwerking te stoppen.

8. Profiling is één van onze marketingspeerpunten, hoe zit het daarmee onder de AVG?

Van profileren is volgens de AVG sprake wanneer *langs geautomatiseerd weg bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd om zo voorspellingen te kunnen doen over bijvoorbeeld iemands economische situatie, persoonlijke voorkeuren of gedrag*.

Profileren is in principe toegestaan, maar als een betrokkene een bezwaar maakt tegen profiling, geldt dit bezwaar in principe altijd zal moeten worden gehonoreerd. Dat betekent dat profiling van deze persoon zal moeten stoppen.

Daarnaast geldt dat het nemen van een besluit op basis van de evaluatie van persoonsgegevens niet zomaar is toegestaan. Dat betekent dat u bijvoorbeeld een klant niet zomaar mag weigeren als hij of zij niet voldoet aan een bepaald profiel. Het uitgangspunt van de AVG is namelijk dat geautomatiseerde besluitvorming niet is toegestaan, tenzij één van de wettelijke uitzonderingen van toepassing zijn. Daarnaast geldt voor geautomatiseerde besluitvorming dat een Privacy Impact Assessment verplicht is.

9. Wat moet ik regelen als verantwoordelijke?

Verantwoordelijken (de organisaties die persoonsgegevens verwerken voor eigen geformuleerde doeleinden) hebben een verantwoordingsplicht. Zij moeten gedocumenteerd kunnen aantonen op welke wijze zij voldoen aan de AVG. Verplicht is:

Voldoende transparantie bieden aan betrokkenen, bijvoorbeeld via een privacy statement. Voor andere situaties kunnen ook brieven of andersoortige informatieberichten voldoende zijn. De AVG stelt inhoudelijke voorwaarden aan een privacy statement.

Het bijhouden van een register van de verwerkingsactiviteiten. In dit register moet bijgehouden worden (o.a.) wat de verwerkingsdoeleinden zijn, welke categorieën van betrokkenen er zijn, aan wie de persoonsgegevens zijn of zullen worden verstrekt (bewerkers!), bewaartermijnen en een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

10. Welke beveiligingsmaatregelen moet ik nemen?

De AVG schrijft geen specifieke beveiligingsmaatregelen voor. Wel geeft de AVG een norm, namelijk: ñDe technische en organisatorische maatregelen moeten, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, op het risico afgestemd beveiligingsniveau waarborgenò Wat passend is, is afhankelijk van uw organisatie, de aard van de persoonsgegevens en de omgang van de verwerking. Daarvoor kunnen in ieder geval de volgende maatregelen genomen worden:

a) de **pseudonimisering**
b) **hashing** en **versleuteling** van persoonsgegevens, zeker bij verzending en opslag in de cloud;
c) two-factor authenticatie
d) toegangscontrole/**autorisatieniveaus** voor medewerkers
e) wachtwoordbeleid
f) beveiligde verbinding

g) systeembeveiliging
h) bewerkersovereenkomsten
i) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
j) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.
k) Privacy-by-design
l) ISO-normeringen en certificaten

11. Wie is de toezichthouder?

Wanneer uw organisatie alleen binnen Nederland persoonsgegevens verwerkt, dan geldt dat de Autoriteit Persoonsgegevens de toezichthouder is.

Als uw organisatie de persoonsgegevens in meerdere EU lidstaten verwerkt, geldt de ñonestopshop-regelò Dit betekent dat die organisaties met nog maar met één privacytoezichthouder zaken hoeven te doen. Dit wordt de óleidende toezichthouderôgenoemd (lead supervisory authority). De hoofdregel is dat de toezichthouder van de EU-lidstaat waar de hoofdvestiging van een organisatie is gevestigd, de lead supervisory authority is. Deze lead supervisory authority stemt zijn optreden af met privacytoezichthouders in de andere EU-landen waar de gegevensverwerking impact heeft.

Onder grensoverschrijdende verwerking van persoonsgegevens wordt verstaan dat een organisatie gegevens verwerkt in verschillende EU-lidstaten óf dat de verwerkingen in meerdere lidstaten impact hebben.

12. Wat zijn de sancties op overtreding?

Overtreedt uw organisatie straks de AVG dan kan de Autoriteit Persoonsgegevens (of een andere lead supervisory authority, zie hiervoor bij vraag 12) een boete opleggen van maximaal 20 miljoen euro. Een boete wordt niet direct opgelegd, daar zal eerst een uitgebreid onderzoek aan vooraf gaan en organisaties krijgen in de meeste gevallen eerst een waarschuwing (die publiekelijk bekend wordt gemaakt). Daarnaast zijn er twee categorieën overtredingen en bijbehorende maximale boetes.

1. Boete van maximaal 10 miljoen euro

Komt een verantwoordelijke de specifieke verplichtingen voor verantwoordelijken niet na, zoals de documentatieplicht of de meldplicht datalekken? Dan kan de Autoriteit Persoonsgegevens een boete opleggen van maximaal 10 miljoen euro. Of een boete van 2% van de wereldwijde jaaromzet, mocht dat bedrag hoger zijn.

2. Boete van maximaal 20 miljoen euro

Overtreedt een verantwoordelijke de beginselen of grondslagen van de AVG? Of de privacyrechten van de betrokkenen? Of volgt een verantwoordelijke de bevelen van de Autoriteit Persoonsgegevens niet op?

Dan kan de Autoriteit Persoonsgegevens een boete opleggen van maximaal 20 miljoen euro. Of een boete van 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.

Al met al komt er veel op u af met de komst van de AVG. Wij denken graag met u mee over de stappen die uw organisatie moet en kan zetten. U kunt daarvoor contact opnemen met het team Privacy van Köster Advocaten (info@kadv.nl).

Iris Tuk
Linda Relouw