Tussen Wbp en Avg: over de invoering van de Avg

Inleiding

De Algemene verordening gegevensbescherming (hierna: de Avg) is op 25 mei 2016 van kracht geworden. Vanaf 25 mei 2018 kunnen de toezichthoudende autoriteiten van de verschillende lidstaten (in Nederland: de Autoriteit Persoonsgegevens, hierna: de AP) actief handhaven en maatregelen instellen, waaronder de veelbesproken astronomische boetebedragen. Deze 'grace period' van twee jaar is bedoeld om organisaties de gelegenheid te geven hun bedrijfsvoering in lijn te brengen met de voorschriften van de verordening. Op het moment van schrijven hebben zij nog een kleine 14 maanden te gaan. Dat lijkt veel, maar onderschatting ligt op de loer. Het CIP heeft door zijn opzet en structuur, als kenniscentrum voor informatiebeveiliging en privacybescherming, veel contacten in overheid en bedrijfsleven. Vanuit dat 'ervaringsveld' mag gezegd worden dat het CIP de implementatie van de Avg met zorg beschouwt. De Avg zorgt nu weliswaar voor een brede 'privacy awareness boost', maar de aanscherpingen en nieuwigheden van de Avg zijn ingrijpender dan ze wellicht lijken en we zien helaas nog te vaak een afwachtende houding.
Een deel van de verklaring voor deze onderschatting kan zijn dat de Avg, ten opzichte van de huidige Wbp (Wet Bescherming Persoonsgegevens) en verwante sectorale wet- en regelgeving, niet veel wezenlijk nieuws bevat. Er zijn accent- en definitieverschillen, transparantie is nadrukkelijker gedefinieerd, er zijn nieuwe details toegevoegd, het is EU-wetgeving geworden, maar het gedachtegoed van de Wbp (inclusief de Meldplicht datalekken) is er nog stevig in terug te vinden. Echter: dat organisaties nu nerveus worden zou ook wel eens kunnen komen doordat ze al die jaren eigenlijk de Wbp (van 6 juli 2000) teveel links hebben laten liggen. In die zin hebben ze dan het strengere karakter van de Avg als het ware over zichzelf afgeroepen en zou de Avg een awareness booster moeten zijn: het is nu hoog tijd voor reparatie. Afhankelijk van het achterstallige onderhoud kan dat wel eens een omvangrijke klus zijn.

CIP, 4 april 2017
[20170404 Tussen Wbp en Avg.pdf]

Inhoud

1. Algemeen: de burger voorop 3

2. Aan de slag! 3

3. Over de rol van CIP 4

Bijlage: Avg-topics nader beschouwd 5

Aanvullende literatuursuggesties 8

Leeswijzer

De Avg adresseert verwerkingsverantwoordelijken en verwerkers. Wij spreken gemakshalve van 'organisaties'. Deze notitie richt zich primair tot bestuurders/managers van organisaties die persoonsgegevens verwerken of dat laten doen.

- De eerste paragraaf bevat algemene observaties bij de Avg. De kern is een aansporing om de implementatiewerkzaamheden niet te onderschatten en vooral de implementatiedatum van 25 mei 2018 niet af te wachten.
- Er zijn genoeg zaken relatief eenvoudig nu al aan te pakken. De paragraaf 'Aan de slag' gaat daarop in.
- Na een korte afsluitende paragraaf over de rol van het CIP wordt in de bijlage nader ingegaan op de meest relevante Avg-topics.

Deze notitie adresseert belangrijke kenmerken van de Avg, maar heeft vooral een signalerende en beschouwende bedoeling. Volledig is zij niet. We laten bijvoorbeeld de problematiek van internationale gegevensuitwisseling voor wat zij is, en ook de bepalingen omtrent de, voor de grotere verwerkers verplicht gestelde, Functionaris voor de gegevensbescherming behandelen wij niet.
Er zijn inmiddels uitstekende publicaties verschenen die de verordening artikel voor artikel verduidelijken en becommentariëren. In de bijlage vindt u daarvan een klein overzicht.

Dit is een publicatie van het Centrum voor informatiebeveiliging en Privacy. Zij is tot stand gekomen met brede inbreng van de CIP Domeingroep Privacy. De aanzet voor deze notitie is gelegen in een verzoek van het BOCU (Bestuurlijk Overleg Compacte Uitvoering) een visie te geven op de invoering van de Avg.

1. Algemeen: de burger voorop

Eigenlijk is de Avg niet eens 'strenger' dan de Wbp. De Nederlandse wetgever heeft het met de Wbp en de Meldplicht datalekken eigenlijk heel goed gedaan en een geleidelijke opstap naar de Avg geboden. De veranderingen zitten in de sfeer van accountability (aantoonbaar in control zijn) en handhaving (de boetebedragen zijn naar het niveau van commerciële wereldspelers getild).
De Avg is evenwel meer uitgesproken en concreet gericht op verbetering van de rechtspositie van de 'betrokkenen' (burgers, consumenten, klanten). Betrokkenen kunnen onder de Avg gemakkelijker dan nu controleren wat er met hun persoonsgegevens wordt gedaan en door wie ze verwerkt worden. De Avg brengt een uitbreiding van het inzage- en correctierecht en introduceert formeel het recht op vergetelheid. Dit zijn geen ongeclausuleerde rechten. Zij kunnen slechts naar redelijkheid en billijkheid worden uitgeoefend. Het recht op vergetelheid is niet van toepassing bij verwerkingen op basis van een wettelijke taak.

De aandacht voor de positie van de burger gaat in de Avg gepaard met verplichtingen die organisaties moeten helpen om alvast op voorhand te regelen dat zij de bescherming van persoonsgegevens op orde hebben en daarover glashelder kunnen communiceren wanneer de burger bij hen aanklopt. De meest fundamentele en waarschijnlijk ook wel meest ingrijpende maatregelen in dit verband zijn 'privacy by default' en 'privacy by design'. In een tijd waarin juist de massale verwerking van big data een enorme vlucht neemt, vereist 'dataminimalisatie' een tegendraadse denksprong: vraagt en gebruikt een organisatie uitsluitend wat werkelijk nodig is voor haar (wettelijke) taak?
De Avg verordonneert ook expliciet transparantie. Dat vereist een precies en actueel zicht op alle verwerkingen van persoonsgegevens die plaatsvinden in de organisatie. In het bijbehorende verwerkingenregister moeten o.a. worden opgenomen: de grondslagen, de doelbinding en de uitbestede verwerkingen. Het betekent ook iets voor de communicatie naar betrokkenen: die moet eenvoudig toegankelijk en begrijpelijk zijn c.q. gemaakt worden.

2. Aan de slag!

De Avg is van kracht, dus in zoverre werpt hij zijn schaduw allang niet meer vooruit. Betrokkenen kunnen zich er al op beroepen. Hoewel op grond van de Avg nog niet beboetbaar, kunnen overtredingen zodoende toch al tot lelijke publiciteit leiden. Vice versa kunnen positieve acties als goede reclame worden benut.

Hoewel de kans te worden aangesproken op onrechtmatig verwerken reëel is, zitten veel organisaties nog in een ontkenningsfase. Mogelijk denkt men dat het allemaal wel zal loslopen of dat het melden van een datalek potentieel schadelijker is dan dat het risico betrapt te worden groot is. Maar ook onduidelijkheid kan een rol hebben gespeeld.
De verordening kan niet meer door nationale wetgeving worden aangepast, maar bevat nog wel in 22 artikelen open plekken die 'lidstatelijk' moeten of kunnen worden ingevuld. Hierop wachten is géén goed idee: de toelichting bij de concept Uitvoeringswet maakt duidelijk dat wordt gestreefd naar een 'beleidneutrale' invulling ten opzichte van de huidige nationale wet- en regelgeving, waaronder handhaving van vigerende sectorspecifieke regelgeving.

Er is geen overgangsrecht. Dat wil zeggen dat de Avg ook van toepassing is op verwerkingen van vóór mei 2018. De gewenningsperiode van twee jaar is bedoeld om je te kunnen instellen op de nieuwe wetgeving. Je bent laakbaar als je na mei 2018 naar aanleiding van een incident, een klacht of routinematig de aandacht trekt van de AP, terwijl je de voorafgaande twee jaren niets hebt gedaan ter verbetering.

Maatregelen waaruit blijkt dat je de Avg serieus neemt zijn bijvoorbeeld een datalekkenprotocol, beslissen of er een Functionaris Gegevensbescherming (FG) moet komen, het verduidelijken en toegankelijk maken van je privacybeleid en het uitvoeren van PIA's - die overigens GEB's[1] gaan heten - op mogelijk riskante verwerkingen.
Het zijn zaken waarmee je in ieder geval al gemakkelijk kunt beginnen. Zo ook het tegen het licht houden en eventueel aanpassen van leverancierscontracten en het instellen van een meld- en klachtenloket. Topprioriteit zou de inrichting van een complete, actuele verwerkingsadministratie moeten zijn. Veel werk wellicht, maar deze administratie en de voorzieningen die daarvoor nodig zijn heb je (ook nu al) nodig in geval van een datalek, wanneer de AP erom vraagt en in verband met de rechten van betrokkenen. Doe vast wat je kunt en wat je snel kunt realiseren.

De Avg biedt ook enige speelruimte: op basis van een risicoanalyse kunnen keuzes worden gemaakt, bijvoorbeeld wanneer maatregelen naar de mening van de verwerkingsverantwoordelijke onevenredig veel kosten en/of een te gering risico zouden verminderen. De AP beoordeelt of de verantwoordelijke zijn keuzes in dit verband in redelijkheid had mogen maken. Daar is geen harde maat voor en dat brengt organisaties die de grens opzoeken mogelijk in een riskante positie.

Misschien is het teveel om nog voor mei 2018 voor elkaar te krijgen; maak dan in ieder geval alvast risicoanalyses en bepaal aan de hand daarvan prioriteiten. Groei dan geleidelijk (houd het beheersbaar en haalbaar), maar gestaag en planmatig. Het voortdurend en gericht managen van de groei naar privacy-volwassenheid moet een centraal element in de bedrijfsvoering worden, beschouw de persoonsgegevens die je als verantwoordelijke of verwerker verwerkt als de kroonjuwelen van de organisatie. Bedenk dat het niet gaat om compliancy aan wetten, maar om respect voor de persoonlijke levenssfeer van anderen en een balans tussen deze privacy en de noodzaak om persoonsgegevens te verwerken. Juist overheidsorganisaties moeten op dit punt bij uitstek voorbeeldig gedrag ten toon spreiden.

Onderschat de waarde van compliancy evenwel niet. Een nauwgezette gegevensverwerkingsadministratie stelt je niet alleen in staat om accountable en transparant te zijn naar controlerende instanties en burgers; het zou ook wel eens heilzaam kunnen zijn voor de bedrijfsvoering en, naar mate het privacy-bewustzijn bij burgers en klanten groeit, een mooi marketinginstrument kunnen worden. En: let en passant dan bij procesaanpassingen en softwarebestellingen voortaan meteen ook op privacy by default en by design.

3. Over de rol van CIP

Voor alle aspecten die in de Avg aan de orde komen, en dan met name de uitvoeringsaspecten, probeert CIP in, voor en vanuit zijn omvangrijke netwerk voortdurend producten te maken en evenementen te organiseren die privacybewustzijn bevorderen en ondersteuning bieden bij het implementeren van privacybeschermende maatregelen. Het CIP voorziet dat privacy-thema's de komende jaren om verschillende redenen een belangrijke rol zullen blijven spelen in het maatschappelijk verkeer, de IT-economie, private organisaties en de overheid. Het CIP bevordert samenspraak en samenwerking tussen private specialisten en de uitvoeringsorganisaties bij de overheid en ziet daar mooie, maar nog relatief kleinschalige resultaten ontstaan. Wij houden graag de gedachte staande dat hier bij uitstek een voorbeeldrol is weggelegd voor overheidsorganisaties. Laten we de komst van de Avg aangrijpen om daar nog meer kracht en uitstraling aan te geven.

[1] GegevenbeschermingsEffectBeoordeling.

Bijlage: Avg-topics nader beschouwd

In grote lijnen blijven de beginselen onverkort van kracht zoals ze nu ook gelden voor de verwerking van persoonsgegevens (*rechtvaardigingsgrond*, *transparantie, doelbinding, doelmatigheid, beveiliging*). De belangrijkste veranderingen ten opzichte van de vigerende privacywetgeving doen zich voor als gevolg van de verplichte transparantie en de uitbreiding van sommige rechten en controlemogelijkheden voor de burger waar het de verwerking van zijn gegevens betreft. Dit betekent aangescherpte verplichtingen van de verantwoordelijken:

- De inrichting van de gegevenshuishouding moet op orde zijn. Aandachtspunten hierbij zijn ook de gegevensverwerking binnen de keten, afspraken over verantwoordelijkheden binnen de keten en duidelijkheid over wie de authentieke bron van specifieke gegevenselementen beheert.
- De wijze waarop de verantwoordelijke bijdraagt aan de uitoefening van de rechten door de burger. De gegevensverantwoordelijke moet - onder voorwaarden - kunnen voldoen aan verzoeken om inzage, correctie van gegevens of verwijdering van gegevens - tenzij wettelijk anders is bepaald. Hij moet tevens betrokkenen *actief* informeren over hun rechten en maat-regelen treffen om te borgen dat betrokkenen informatie over verwerkingen ontvangt (art. 13, art. 14);
- Meldplicht bij een gebleken 'inbreuk in verband met persoonsgegevens' waarbij de 'rechten en vrijheden van natuurlijke personen' een waarschijnlijk groot risico lopen (personal data breach, in het Nederlands doorgaans 'datalek' genoemd). Art. 33 en 34 zien op deze meldplicht: de opzet en het doel lijken op de Nederlandse versie in de Wbp, maar er zijn ook enkele significante verschillen.[2]
- Accountability voor het voldoen aan deze verplichtingen;
- Het in dienst nemen of inhuren van een Functionaris gegevensbescherming (FG) wanneer de verwerkingsverantwoordelijke een overheids- of bestuursorgaan is, dan wel een particuliere onderneming die verwerkingen van persoonsgegevens verricht die aan bepaalde kenmerken voldoen (qua omvang, gevoeligheid).

Op veel plaatsen vult de Avg concreet, expliciet in wat er precies onder een bepaald recht of een bepaalde plicht moet worden verstaan. Voorbeelden zijn:

- Voorwaarden voor transparantie (art. 13/14),
- Het uitgebreide recht op inzage (art. 15),
- De uitwerking van (mogelijke) uitzonderingen of beperkingen op de rechten en plichten, (bijv. art. 23 over uitzonderingen op basis van belangen die boven de belangen van betrokken gesteld kunnen worden),
- Eisen die aan verwerkers gesteld worden (art. 29; zie ook 28 en 32),
- De eisen die aan een verwerkersovereenkomst worden gesteld (art. 28).

De plicht om je als verwerkingsverantwoordelijke bij de AP te melden wanneer je persoonsgegevens verwerkt komt te vervallen. De Avg vervangt de huidige meldingsplicht door een verantwoordings-plicht. 'Op eigen kracht in control' is wellicht een sympathiek uitgangspunt, maar het betekent voor verantwoordelijken en verwerkers met achterstallig onderhoud op dit punt tevens een administratieve verzwaring en een implementatie-inspanning. Verwerkingsverantwoordelijke én verwerker(s) zijn gehouden om samen te werken met de toezichthoudende autoriteit.

[2] In de vigerende Nederlandse versie lijkt de nadruk te liggen op de melding bij de AP. In de Avg is het tijdig, volledig en behulpzaam informeren van de betrokkene(n) het zwaartepunt. Melden mag achterwege blijven als 'rechten en vrijheden van natuurlijke personen' geen groot risico lopen; dat geldt onder de Avg voor zowel de melding aan de autoriteit, als aan de betrokkene. Dit is ook het geval 'wanneer melding afbreuk zou doen aan een zwaarwegend belang'.

Je bent als gegevensverwerker verantwoordelijk en aansprakelijk (accountable) voor hoe je de verplichtingen hebt ingevuld en hoe je ermee omgaat. Dit moet volledig inzichtelijk zijn wanneer de AP erom vraagt. De verordening staat evenwel nadrukkelijk het opstellen van en/of aansluiten bij gedragscodes en certificeringen toe waarmee je, indien eenmaal goedgekeurd, kunt aantonen:

- hoe je als verwerker/verantwoordelijke aan de wettelijke eisen voldoet;
- hoe aan de beveiligingsverplichting is voldaan. (artikel 32 lid 3); voor overheden geldt dat in ieder geval moet worden voldaan aan BIR/BIG/BIWA.
- hoe je in algemene zin je verplichtingen als verwerker/verantwoordelijke naleeft.

Jurisprudentie zal nog moeten uitwijzen in hoeverre documenten die verantwoordelijken opstellen in het kader van de accountability openbaar moeten worden gemaakt.[3]

Artikel 6 van de Avg formuleert de toegestane verwerkingsgrondslagen, toestemming van de betrokkene is één daarvan. Als de verwerking kan plaatsvinden op basis van een van de andere wettelijke grondslagen, dan is toestemming (van de betrokkene) niet vereist.

Vindt een verwerking niet plaats ter uitoefening van *een wettelijke taak* en zijn ook de andere verwerkingsgrondslagen niet van toepassing, dan moet er aantoonbaar toestemming zijn. Een dergelijke toestemming moet voldoen aan de voorwaarden van art. 7 en 8 van de Avg. Daarin staat, geparafraseerd, dat 'opt in' de standaard modus operandi is bij het vragen en geven van de toestemming, dat het voor de betrokkene volstrekt duidelijk moet zijn waarvoor de toestemming wordt gevraagd en dat een toestemming even eenvoudig moet kunnen worden ingetrokken als verleend. Is de betrokkene een kind dan gelden aanvullende voorwaarden.
Bij reeds bestaande toestemmingen die niet aan de gestelde voorwaarden voldoen en niet op een van de overige toestemmingsgronden kan steunen, kan dit dus betekenen dat zij alsnog expliciet moeten worden opgehaald of als niet rechtsgeldig moeten worden bestempeld.

Betrokkenen krijgen het recht van verzet tegen commercieel gebruik van hun gegevens, profilering en tegen 'geautomatiseerde beslissingen', dat wil zeggen: waar geen beoordeling door een natuurlijke persoon meer aan te pas komt.

Betrokkenen moeten gemakkelijk informatie kunnen verkrijgen over hoe hun persoonsgegevens verwerkt worden en die informatie moet in begrijpelijke taal zijn opgeschreven. Er moet ook een klachtenformulier + procedure beschikbaar c.q. operationeel zijn.

Gegevensbescherming *by design* en *by default* zijn beide expliciet opgenomen in de Avg. Dit betekent twee dingen:

- Bij het ontwerpen van een nieuwe verwerking van persoonsgegevens en de processen daaromheen wordt het verplicht om bescherming van persoonsgegevens vanaf het begin in het ontwerpproces mee te nemen; vergeet de bestaande verwerkingen niet: ook daarvoor gelden deze gegevensbeschermingsprincipes.
- Voor de hoeveelheid verwerkte informatie wordt de standaard: zo weinig mogelijk. Alleen wat noodzakelijk is om het doel van de verwerking te kunnen bereiken kan nog worden opgevraagd of verder worden verwerkt. Dit kan dataminimalisering vereisen en maakt het noodzakelijk om alle verwerkingen - niet alleen nieuwe - goed tegen het licht te houden.

[3] Vooruitlopend op de invoering van de wet Open Overheid heeft het kabinet al besloten tot openbaarmaking van onderzoeksrapporten, waaronder ADR-rapportages.

Van ingestelde beveiligingsmaatregelen moet de doeltreffendheid zijn geborgd; je moet dat ook aantonen, bijvoorbeeld met periodieke testen. Het is zaak om het geheel van getroffen maatregelen (zoals: audits, pentesten, SSD-implementatie, ed.) door te lichten en waar nodig te verbeteren of aan te vullen.

De komst van de Avg is een mooie aanleiding om de informatiebeveiliging en privacybescherming stevig(er) aan elkaar te relateren. Informatiebeveiliging is een belangrijk instrument voor privacy-bescherming en de toename van cybercrime maakt dat bijna dagelijks duidelijk. CIP spreekt graag van 'informatieveiligheid' als de na te streven resultante van de twee disciplines in onderlinge samenhang en richt zijn adviezen en producten daarop. In dat licht geeft CIP het advies een goede symbiose van de FG/DPO[4] en de CISO/Security Officer te bevorderen. De FG of soortgelijke functionaris zou zich bovendien niet alleen moeten richten op de beleidsstaf of het bestuur, maar juist (ook) op het uitvoerend management.

Over uitbestede verwerkingen moeten afspraken worden gemaakt tussen de verwerkings-verantwoordelijke en de verwerker(s). Bestaande afspraken moeten worden getoetst en wellicht worden aangevuld met bepalingen die het mogelijk maken om als verantwoordelijke en verwerker aan de nieuwe bepalingen te kunnen voldoen.
Bovendien moet goed naar aansprakelijkheid in ketenverband worden gekeken: iedere actor in een verwerkingsketen kan aansprakelijk worden gesteld voor schade. Haal hier vooraf al juridische expertise bij en niet pas als er klachten of claims zijn. Een specifieke tip uit het veld hierbij: laat, in verband met aansprakelijkheid, een advocaat ernaar kijken - als nadere specificering van 'juridische expertise'.

Een laatste woord ten slotte over het veelbesproken boetebeleid. Het is aan de lidstaten gelaten om zelf invulling te geven aan een boetebeleid. En de hamvraag is daarbij tot nu toe: kunnen ook *overheidsinstanties* worden beboet voor overtredingen die worden geconstateerd bij het uitoefenen van de wettelijke taak? Het vigerende beleid onder de Wbp staat beboeting van overheden toe; de eerste conceptversie van de Uitvoeringswet Avg (die de Wbp zal vervangen en de discretionaire ruimte invult die de Avg de lidstaten toestaat) laat dat vooralsnog intact, inclusief de opties van last onder bestuursdwang en last onder dwangsom. Overigens wordt wel aangesloten bij de in de Avg gehanteerde (maximale) boetebedragen.

[4] Data Protection Officer

Aanvullende literatuursuggesties

Wie een goed overzichtsartikel over Avg zoekt kan terecht bij:

- https://www.recht.nl/vakliteratuur/privacy/artikel/413550/accountability-in-de-avg-betere-processen-en-een-sterkere-positie-van-betrokkenen/

NB: dit artikel is niet vrij verkrijgbaar en CIP - wij zijn van vrijelijk en onbekommerd delen voor het algemeen belang - betreurt dat.

Wil je iemand in 3 minuten op scherp zetten, verwijs hem dan naar het redactioneel openingsstuk van Peter Lievense op pagina 3 van *iBestuur*, januari 2017 (nr. 21):

- http://ibestuur.nl/file_download/281/iBestuur_21.pdf

De feitelijke tekst van de verordening, waarin de overwegingen en artikelen ongerelateerd achter elkaar worden neergezet, is nogal gebruikersonvriendelijk. Even zoeken op internet met "GDPR" levert inmiddels een reeks aan titels op die in dit opzicht soelaas bieden. Wij noemen er enkele uit eigen ervaring. Deze publicaties zijn eveneens niet vrijelijk te verkrijgen:

- http://www.bju.nl/juridisch/catalogus/tekstuitgave-privacyverordening-1
- https://www.managementboek.nl/boek/9789082083446/de-algemene-verordening-gegevensbescherming-editie-2017-arnoud-engelfriet
- http://www.nomos-shop.de/Albrecht-Jotzo-neue-Datenschutzrecht-EU/productview.aspx?product=27238

Handig, nuttig en gratis, maar nog niet helemaal af, is:

- https://wiki.surfnet.nl/display/privacy/De+privacyverordening+uitgewerkt

Tevens nog relevant is:

- https://www.wolterskluwer.nl/shop/boek/wet-bescherming-persoonsgegevens-in-europees-perspectief/NPWBPEUPE/