Perspectief op de AVG

Perspectief op de AVG

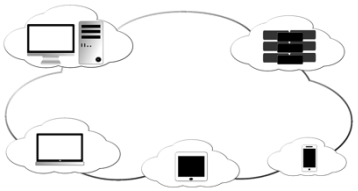
Van WBP naar AVG

Nederland had voor de AVG (Algemene Verordening Gegevensbescherming) al een wet die de bescherming van persoonsgegevens regelde. De AVG is weliswaar op een aantal punten een behoorlijke aanscherping van die wet, maar veel elementen uit de AVG staan ook in de WBP (Wet Bescherming Persoonsgegevens). Daarnaast is de WBP een Nederlandse wet, terwijl de AVG een Europese wet is[1]. Hiermee worden de regels voor gegevensbescherming over de volledige EU op een lijn gebracht. De AVG geldt niet alleen voor digitale gegevens, ook gegevens op papier vallen daar onder.

Om te voldoen aan de AVG moeten organisaties aan een aantal eisen voldoen. Welke die eisen zijn hangt deels samen met de mate waarin een organisatie persoonsgegevens verwerkt.

Gegevensverwerking

Het primaire doel van de AVG is het reguleren van het verwerken van persoonsgegevens ter bescherming van individuen. Er kan sprake zijn van gegevensverwerking zodra een partij die kan verzamelen, inzien, aanpassen, doorgeven, verwijderen of opslaan. Toegang hebben tot die gegevens is geen verwerking op zich, maar zodra de gegevens benaderd worden, is sprake van verwerking in de zin van de AVG. Het bekijken van gegevens is voor de AVG dus verwerken.



Ieder gegeven of iedere combinatie van gegevens die te herleiden is tot een individu is een persoonsgegeven. Gegevens als naam, BSN of mailadres zijn vaak direct terug te voeren naar een individu. Een combinatie van leeftijd en adres kan dat ook zijn. Dat kan ook gelden voor foto's waarop een individu herkenbaar is, zeker als die foto voor identificatie bedoeld is (zoals een pasfoto).

Verantwoordingsplicht

Voor ieder opgeslagen persoonsgegeven dient een helder doel geformuleerd te zijn, dat past binnen de kaders van de wetgeving. Deze doelbinding dient vooraf helder te zijn. Het verzamelen van gegevens omdat dat altijd handig is voor later is dus niet toegestaan. Het doel dient redelijk te zijn binnen de kaders van de wet. Vaak gaat een bewaartermijn gepaard met een doel; zo gelden er voor veel instellingen wettelijk vastgelegde bewaartermijnen waaraan voldaan moet worden.

Naast een heldere doelbinding, dient de verwerking ook te voldoen aan eisen van transparantie, rechtmatigheid en juistheid en de organisatie dient aan te kunnen tonen dat hieraan voldaan wordt. Bijzondere persoonsgegevens (gegevens over ras, religie, etniciteit, seksualiteit, strafblad) hebben hierin een speciale plaats.
De verantwoordingsplicht geldt voor alle verschillende vormen van persoonsgegevens-verwerking. Voor iedere verwerking dient apart een onderbouwing gegeven te worden.

[1] De AVG is Internationaal bekend als de GDPR (General Data Protection Regulation)

Grondslag

De AVG noemt een aantal toegestane grondslagen voor verwerking van persoonsgegevens:

a) **Toestemming**. Toestemming kan in principe gegeven worden voor iedere vorm van verwerking van persoonsgegevens en voor ieder doel.
b) **Uitvoering van een overeenkomst**. Bijvoorbeeld een onderwijsinstelling die een student registreert.
c) **Wettelijke verplichting**. Bijvoorbeeld een gemeente die een inwoner registreert.
d) **Vitale belangen**. Bijvoorbeeld als een arts op de eerste hulp een patiënt behandelt. Deze grondslag is gericht op het direct kunnen beschermen van iemands fysieke integriteit.
e) **Algemeen belang of uitoefening van openbaar gezag**. Deze grondslag kan alleen gebruikt worden indien sprake is van een wettelijke grondslag, waardoor deze eigenlijk gelijk valt met c).
f) **Gerechtvaardigde belangen**. Deze grondslag is bedoeld als verwerking niet toegestaan is op basis van de andere grondslagen. Een voorbeeld is registratie van id en wachtwoord voor geautomatiseerde omgevingen. Deze grondslag geeft meer ruimte dan de andere, maar verwacht kan worden dat het gebruik van deze grondslag een stevige onderbouwing vereist.

Het is aan de verwerkende organisatie te bepalen of voldaan wordt aan een van de zes grondslagen. Dit moet aangetoond kunnen worden aan de Autoriteit Persoonsgegevens.

Toestemming

Als een organisatie op basis van grondslagen b) tot en met f) gegevens verwerkt, dan kan dat zonder dat daarvoor toestemming gevraagd wordt aan de eigenaar van de persoonsgegevens. Als wel toestemming gevraagd moet worden voor het gebruik van persoonsgegevens, dan moet die vrij en in voldoende kennis verleend (geïnformeerd) worden. Ofwel: op zo'n manier gevraagd worden dat duidelijk is waarvoor toestemming gevraagd wordt (specifiek); verborgen regeltjes in een lang stuk tekst zijn niet afdoend, moeilijke teksten ook niet. Ook de vooraf aangevinkte toestemming is niet toegestaan, evenmin als toestemming onderstellen bij verder gebruik (bij bijvoorbeeld een website). Daarnaast mag het niet verlenen van toestemming geen negatieve gevolgen hebben voor de weigeraar.
Indien de gegevens van kinderen jonger dan zestien jaar verwerkt worden, moet toestemming verleend worden door de ouders of verzorgers van het kind.

Functionaris Gegevensbeheer (FG)

Organisaties die veel persoonlijke gegevens verwerken zijn verplicht een FG aan te stellen. Hierbij kun je denken aan overheden, onderwijsinstellingen en zorginstellingen, maar bijvoorbeeld ook verzekeringsmaatschappijen of banken. Daarnaast geldt de plicht voor organisaties die veel bijzondere persoonsgegevens verwerken vanuit hun bedrijfsdoel, zoals organisaties die zich bezighouden met profiling.
De FG moet voldoende kennis hebben om die rol bij diens organisatie in te vullen[2] en

[2] De AVG formuleert geen harde eisen aan de FG, maar noemt wel een aantal elementen:
- Kennis van wet- en regelgeving op gebied van privacy en gegevensverwerking
- Begrip van de gegevensverwerkingen die de organisatie uitvoert
- Begrip van IT en informatiebeveiliging
- Kennis van de organisatie en van de sector waarin die actief is
- Vaardigheden om een cultuur van gegevensbescherming te ontwikkelen binnen de organisatie

geregistreerd worden bij de Autoriteit Persoonsgegevens. De AVG laat ruimte om een externe partij aan te stellen als FG voor een organisatie, maar maakt daarbij wel de aantekening dat het wenselijk is dat een persoon aangewezen wordt als aanspreekpunt.

De FG wordt geacht de AVG en andere relevante wetgeving en praktijken op het gebied van gegevensbescherming te kennen. Daarnaast moet deze inzicht hebben in de gegevens en gegevensverwerking binnen de organisatie en in staat zijn de zorgvuldige behandeling van gegevens uit te dragen in een organisatie. Wat een passend niveau is, hangt af van de gevoeligheid van de verwerking(en) in de organisatie. Daarnaast moet de organisatie de FG de mogelijkheden geven diens taak (controle op naleving van wetgeving voor gegevensbescherming) naar behoren uit te voeren, door deze bekend te maken in de organisatie, te ondersteunen in bemensing, infrastructuur en financiën en dient deze door het hoger management ondersteund te worden en onafhankelijk te kunnen functioneren. Het aanstellen van een excuus-FG is dus nadrukkelijk niet voldoende om aan de AVG te voldoen. Dit vindt ook zijn weerslag in het feit dat ook na aanstellen van een FG de organisatie verantwoordelijk blijft voor het naleven van de AVG; deze verantwoordelijkheid verschuift niet naar de FG.

Verwerker vs verwerkingsverantwoordelijke

Veel organisaties besteden werkzaamheden uit waarvan de verwerking van persoonsgegevens deel uitmaakt, bijvoorbeeld aan een administratiekantoor, maar ook bij een facilitair dienstverlener of ICT-beheerder die persoonsgegevens kan inzien om calls af te handelen kan sprake zijn van een verwerkersrelatie. In zo'n situatie is het administratiekantoor de verwerker en de organisatie waarvoor de werkzaamheden worden verricht de verwerkingsverantwoordelijke. Dat de verwerking plaatsvindt ten behoeve van de verwerkingsverantwoordelijke is onderdeel van de verwerkersrelatie.
Voor beide partijen geldt dat ze zorgvuldig om moeten gaan met de gegevens. Het is aan de verwerkingsverantwoordelijke om te bepalen wat doelbinding is en -indien nodig- toestemming te verkrijgen van de eigenaar van de persoonsgegevens. De verwerker is een zelfstandige rechtspersoon die gedelegeerd uitvoerend is. Als er sprake is van een gezagsrelatie tussen verwerkingsverantwoordelijke en uitvoerende, is er geen sprake van een verwerker in de zin van de AVG. Een verwerker is een opdrachtnemer.
In gevallen waar sprake is van een verwerkersrelatie, moet deze worden bevestigd in een verwerkersovereenkomst. Hierin staan in ieder geval de duur van de overeenkomst, het soort gegevens dat verwerkt wordt en het doel en de aard daarvan, de categorieën van betrokkenen (bv. studenten, medewerkers) en de rechten en plichten van de verwerkingsverantwoordelijke.

Een voorbeeld: facebook kwam in het nieuws omdat een andere partij -Cambridge Analytica (CA)- persoonsgegevens gebruikte die bij facebook vandaan kwamen. Weliswaar is het zo dat hier geen sprake is van een gezagsverhouding en er duidelijk sprake is van verwerking van persoonsgegevens, maar aangezien de verwerking in het belang van CA gebeurde en niet in het belang van facebook, was hier geen sprake van een verwerkersrelatie. Dat laatste wil overigens niet zeggen dat facebook rechtmatig handelde.

Register

Organisaties met minstens 250 medewerkers en organisaties die structureel persoonsgegevens verwerken zijn verplicht een register te voeren van de verwerking van die gegevens. Het voeren van een personeelsadministratie is bijvoorbeeld een vorm van structureel persoonsgegevens verwerken. Vanwege de extra risico's met bijzondere persoonsgegevens zijn de eisen daar nog strenger.

Het staat een organisatie vrij te bepalen hoe het register opgesteld wordt, maar in ieder geval de volgende gegevens moeten hierin staan voor de verwerkingsverantwoordelijke:

- contactgegevens van de organisatie (of het aanspreekpunt), de gegevens van de FG en de contactgegevens van eventuele (internationale) organisaties waarmee gegevens gedeeld worden;
- de doelen waarvoor persoonsgegevens verwerkt worden;
- een categorisatie van de soorten personen van wie gegevens verwerkt worden (bijvoorbeeld: medewerkers, studenten, patiënten);
- de categorieën van de gegevens die opgeslagen worden (bijvoorbeeld: naam, adres, BSN);
- wat is de termijn waarvoor gegevens bewaard worden;
- met wie worden de gegevens gedeeld en voor welk doel gebeurt dit.

Voor de verwerker zijn de eisen minder streng; het register daar moet bevatten:

- contactgegevens van de organisatie (of het aanspreekpunt), de gegevens van de FG, een beschrijving van het soort verwerkingen dat toegepast wordt en de contactgegevens van eventuele (internationale) organisaties waarmee gegevens gedeeld worden.
- een algemene technische beschrijving van de technische en organisatorische maatregelen die zorgen voor een veilige verwerking van persoonsgegevens.

Let wel: iedere verwerking dient apart beschreven te worden in het register. Als bijvoorbeeld persooneelsgegevens geadministreerd worden in personeelssysteem A en die gegevens doorgegeven worden aan helpdesksysteem B voor het aanmaken van een netwerktoegang, dan is sprake van drie verwerkingen:

- Personeelsregistratie in A vanwege uitvoeren van arbeidsovereenkomst
- Doorgeven van persoonsgegevens naar systeem B
- Persoonsregistratie voor netwerktoegang in B

Afhandelen AVG-verzoeken

Ieder individu heeft bepaalde rechten op basis van de AVG en kan in het kader daarvan een verzoek indienen bij een organisatie. Er geldt een plicht om dat verzoek (mits redelijk) binnen dertig dagen af te handelen, daarbij niet alleen wettelijke kaders aanhoudend, maar ook het doel van de verwerking van persoonsgegevens. Dit zijn de rechten:

- **Dataportabiliteit**. Het recht om persoonsgegevens over te dragen aan een andere partij.
- **Vergetelheid**. Het recht om vergeten te worden, ofwel het recht om gegevens te laten verwijderen.
- **Inzage**. Het recht op inzage in welke gegevens hoe bewaard worden en op welke manier die verwerkt worden door de organisatie.
- **Rectificatie en wijziging**. Het recht om gegevens aan te (laten) passen.
- **Beperking van de verwerking**. Het recht op verwerking van minder gegevens.
- **Vrijstelling van geautomatiseerde besluitvorming en profilering**. Het recht om gegevens niet (alleen) geautomatiseerd te verwerken, maar ook door een mens beoordeeld te worden.
- **Bezwaar**. Het recht om bezwaar te maken tegen de verwerking van gegevens.
- **Duidelijke informatie**. Het recht op duidelijke informatie hoe gegevens verwerkt worden.

De eigenaar van de persoonsgegevens kan altijd een verzoek doen op basis van de AVG, maar dat wil niet zeggen dat organisaties daaraan altijd moeten voldoen. De verwerkingsverantwoordelijke moet hierbij steeds andere belangen afwegen tegen die van de verzoeker.

Ad Dataportabiliteit. Dit recht heeft alleen betrekking op digitale gegevens die met toestemming worden verwerkt of op basis van uitvoering van een overeenkomst. Die gegevens moeten goed bruikbaar opgeleverd worden. Het gebruik van een open standaard is aan te raden.
Ad Vergetelheid. Het recht op vergetelheid dwingt alleen als er (niet langer) een wettelijke grondslag is om gegevens te bewaren. Bijvoorbeeld doordat toestemming wordt ingetrokken, er niet langer sprake is van de uitvoering van een overeenkomst (uit dienst, afgestudeerd) of als de verwerking van de gegevens geen wettelijke grondslag had (in strijd met regelgeving verzameld zijn). Daarnaast kunnen bewaartermijnen een rol spelen (er geldt bijvoorbeeld een bewaartermijn voor diploma's en voor belastinggegevens. Dit recht overschrijdt het recht op vergetelheid).
Ad Inzage. Bij dit recht moet volledig inzicht gegeven worden in welke persoonsgegevens waar en met welk doel worden verwerkt, op welke wijze (inclusief al dan niet geautomatiseerde besluitvorming en onderbouwing daarvan), aan wie ze verstrekt zijn, hoelang die gegevens bewaard zullen worden en wat de herkomst van die gegevens is. Daarnaast moet de verzoeker van diens rechten met betrekking tot de gegevens op de hoogte gesteld worden.
Ad Rectificatie. Dit recht is bedoeld om fouten te corrigeren of incomplete gegevens aan te vullen. Hierbij moet aannemelijk zijn dat sprake is van een fout; onwelgevallige meningen vallen niet binnen het bereik.
Ad Beperking. Dit recht is bedoeld als de verwerker (mogelijk) foute gegevens heeft, of er geen grondslag is voor verwerking, maar als de eigenaar (nog) niet wil dat die verwijderd worden, bijvoorbeeld omdat die nog inzicht wil hebben in de gegevens. De verzoeker kan

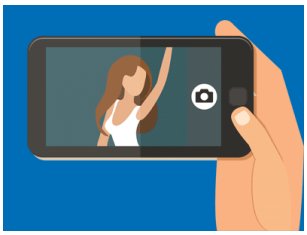
dan eisen dat de gegevens niet langer verwerkt worden.
Ad Vrijstelling geautomatiseerde verwerking. Als een organisatie geautomatiseerd gegevens verwerkt en op basis hiervan besluiten neemt die gevolgen hebben, dan kan hiervan vrijstelling worden gevraagd.
Ad Bezwaar. Indien gegevens verwerkt worden op basis van algemeen belang of een gerechtvaardigd belang, dan kan hiertegen bezwaar gemaakt worden. Hierbij worden vooral het recht op bezwaar tegen direct marketing (hier moet altijd gehoor aan gegeven worden) en bezwaar op grond van bijzonder persoonlijke omstandigheden genoemd. In het laatste geval moeten die omstandigheden onderbouwd worden.
Ad Duidelijke informatie. De verwerker heeft de plicht duidelijke informatie te geven over wat waarom gedaan wordt met persoonsgegevens. Dit kan in een privacy-verklaring.

Beveiliging en datalekken

De AVG is primair bedoeld om te reguleren waar persoonsgegevens wel en niet voor gebruikt mogen worden. Het blijft onverkort noodzakelijk om gegevens veilig te gebruiken. Indien toch persoonsgegevens lekken (of daarvan een vermoeden bestaat), dient dit binnen 72 uur gemeld te worden bij de Autoriteit Persoonsgegevens.
Het in de AVG geformuleerde uitgangspunt Privacy by design zegt dat persoonsgegevens in IT-systemen altijd goed beschermd moeten zijn. Privacy by default zegt dat zo min mogelijk persoonsgegevens verwerkt moeten worden. Dit laatste sluit ook aan bij de noodzaak van het bestaan van een doelbinding.

Foto's

Als personen op basis van een foto eenduidige geïdentificeerd worden, is er sprake van een persoonsgegeven en valt het verwerken van die foto dus onder de AVG. In dat geval valt die foto onder bijzondere persoonsgegevens, aangezien in ieder geval ras afgeleid kan worden.



De vraag is wanneer sprake is van eenduidige identificatie. Dat een pasfoto bedoeld is voor identificatie moge duidelijk zijn. Een foto die gewoon op straat genomen is, is in principe geen persoonsgegeven, ook niet als daar toevallig mensen op staan. Maar wat te denken van foto's van de buurtbarbecue? Als je de buurt kent kun je op basis van de foto's ongetwijfeld een aantal individuen identificeren. Aan de andere kant worden die foto's niet genomen met het doel mensen te identificeren. Jurisprudentie zal moeten laten zien hoe de AVG voor foto's geïnterpreteerd gaat worden.
Portretrecht is in ieder geval van toepassing op foto's. Als foto's gebruikt worden voor publicatie en mensen daarop herkenbaar zouden kunnen zijn (zoals bij bedrijfsfeestjes of open dagen) is het goed toestemming te vragen voor publicatie.

Voorlichting

De AVG vraagt een flink pakket aan maatregelen die doorgevoerd moeten worden. De uiteindelijk succesvolle naleving staat of valt echter met de uitvoer in de dagelijkse praktijk. Niet alleen medewerkers die direct bezig zijn met werkzaamheden ten behoeve van naleving van de AVG zijn van belang, alle medewerkers moeten bekend zijn met de eisen van de AVG en daarmee rekening houden tijdens de dagelijkse werkzaamheden. Medewerkers moeten zich bewust zijn dat lijstjes en

andere registraties buiten de reguliere systemen om al snel strijdig kunnen zijn met de AVG. Interne communicatie, bewustwording en mogelijk ook opleiding zijn dan ook van groot belang om tot een goede uitvoer te komen.

Handhaving

De handhaving van de AVG wordt in de hele EU gedaan door nationale toezichthouders, in Nederland de Autoriteit Persoonsgegevens (AP). Voor al die toezichthouders geldt dat dit toezicht leidt tot een aanzienlijke uitbreiding van hun werkpakket. Hoe ze daaraan invulling gaan geven is nog onduidelijk, mede omdat lang niet al die toezichthouders van voldoende omvang zijn om die handhaving volledig uit te voeren. Een aantal elementen zal een rol spelen bij handhaving:

- **Reactief toezien**. In het algemeen wordt verwacht dat toezicht vooral zal gebeuren op het moment dat een melding van een overtreding gedaan wordt; zolang de AP geen aanwijzingen heeft dat een organisatie niet conform de AVG werkt, zal niet snel een controle gedaan worden. Hierbij speelt de beperkte omvang van de AP als organisatie een duidelijke rol.
  Overigens ligt het wel voor de hand dat de AP zal controleren of alle organisaties die een FG moeten hebben, ook daadwerkelijk een FG hebben die aan alle eisen voldoet.
- **Jurisprudentie afwachten**. De AVG is op lang niet alle punten helder. Op veel van die punten zal jurisprudentie duidelijkheid moeten brengen hoe de wet geïnterpreteerd wordt en waaraan organisaties zich moeten houden.
- **Praktijk**. De AVG is op een aantal punten strak geformuleerd. Het valt te verwachten dat hierdoor in de praktijk problemen gaan ontstaan. Dit zal waarschijnlijk deels zijn weg vinden in jurisprudentie. Maar er zal waarschijnlijk niet gehandhaafd gaan worden op de voetbalpoule van de afdeling of de barbecue van de sportvereniging.

Overigens zijn de landen van de EU verplicht de AVG te handhaven. Als ze dat niet doen kunnen ze daarvoor op de vingers getikt worden door de EU.

Overweging

In aanloop naar het ingaan van de wet heeft AP-directeur Aleid Wolfsen meermalen de pers gezocht, waardoor de contouren van de handhaving zichtbaar zijn geworden:

- De Autoriteit zal niet zelf op bezoek gaan bij organisaties, maar dat alleen doen als er sterke aanwijzingen zijn (zoals klachten) dat de AVG niet gevolgd wordt.
- Het aanstellen van een bevoegde FG door de organisaties waarvoor dat verplicht is, is van belang.
- Het primair doel van handhaven is dat organisaties zich aan de wet gaan houden. Hoewel de AP een behoorlijk mandaat heeft (onder andere het opleggen van hoogoplopende boetes en het stilleggen van verwerkende processen), zal toch vooral gezocht worden naar een manier om een organisatie die de wet overtreedt die alsnog te laten volgen. Hiervoor moet een organisatie wel laten zien serieus bezig te zijn met voldoen aan de wet.

Uit bovenstaande kan geconcludeerd worden dat er geen reden tot wanhoop is voor organisaties die nog niet klaar zijn met de implementatie van AVG. Tegelijkertijd is het wel

van groot belang die implementatie zo snel mogelijk op de rit te krijgen. De tijden van het verzamelen van persoonsgegevens die altijd wel handig kunnen zijn voor marketing-doeleinden en toestemming geven via de kleine lettertjes liggen duidelijk in het verleden.

Bronnen

De site van de Autoriteit Persoonsgegevens geeft een goed beeld van de plichten waaraan organisaties in het kader van de AVG moeten voldoen. Onderstaande links zijn bij uitstek waardevol:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/verantwoordingsplicht

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/rechten-van-betrokkenen

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg

https://www.cibit.nl/nl/blog/privacy-de-wettelijke-kaders-voor-de-verwerking-vervolg/

https://www.computable.nl/artikel/sponsored/security/6345753/5740344/de-verwerkersovereenkomst-wie-doet-wat-en-waar-moet-je-aan-denken.html?utm_source=nieuwsbrief&utm_medium=email&utm_campaign=Dagelijks_03_05_2018&utm_content=sponsored