De privacyverklaring onder de Algemene Verordening Gegevensbescherming; nog veel werk aan de winkel!

B. Oenema, M. van der Waal en B. Lashkari*

Trefwoorden: AVG, Privacyverklaring, transparantie

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dat betekent dat iedere organisatie binnen de Europese Unie (EU) aan dezelfde privacywetgeving moet voldoen. De AVG vervangt binnen Nederland de Wet bescherming persoonsgegevens (Wbp). De implementatie van de AVG heeft het thema databescherming bij veel organisaties hoog op de bedrijfsagenda gezet. Maar veel bedrijven en gemeenten zijn nog niet zover: 'Er is nog veel werk aan de winkel.'

Transparantie

Onder de Wbp waren organisaties in Nederland al verplicht om transparant te zijn over de verwerking van persoonsgegevens van onder andere hun websitebezoekers en -klanten. Deze transparantieverplichtingen schreven onder andere voor dat een organisatie haar klanten, bezoekers van haar website of haar medewerkers duidelijk moest informeren over welke persoonsgegevens werden verzameld en met welk doel. Veel organisaties voldeden aan deze transparantievereisten door middel van een zeer lange privacyverklaring op hun website. De transparantievereisten uit de Wbp zijn onder de AVG ook opgenomen en veel organisaties hebben de privacyverklaring gewoon op hun website laten staan. Onder de AVG hebben wel meer organisaties, stichtingen en verenigingen een uitgebreide privacyverklaring op de website opgenomen. Al dan niet met een korte animatie introductie over de overige AVG-verplichtingen die op de organisatie rusten. Dit omdat de AVG onder een breder publiek bekend is geworden door onder andere de media en doordat de boetes voor het niet vermelden significant hoger zijn. Ook onder de AVG is een privacyverklaring net als onder de Wbp slechts bedoeld om te voldoen aan de verplichting tot het geven van informatie aan betrokkenen en heeft deze geen juridische waarde. Waar de Wbp over transparantie *principal based* was, dat wil zeggen voor een gedeelte gebaseerd op regels en voor een groot deel gebaseerd op een set van gestelde doelen, schrijft de AVG met betrekking tot het begrip transparantie nauwkeuriger voor wat minimaal aan informatie moet worden verstrekt. De uitdrukking 'in de beperking toont zich de meester', is zeker van toepassing op een goede privacyverklaring. Er moet niet te weinig, maar zeker ook niet te veel in staan. Het moet voor mensen leesbaar en begrijpelijk zijn.

Waar de Wbp over transparantie *principal based* was, dat wil zeggen voor een gedeelte gebaseerd op regels en voor een groot deel gebaseerd op een set van gestelde doelen, schrijft de AVG met betrekking tot het begrip transparantie nauwkeuriger voor wat minimaal aan informatie moet worden verstrekt

Toestemming

In aanloop naar de AVG werden we overstelpt met mails van organisaties om in te stemmen met nieuw opgestelde privacyverklaringen. Ook verschenen pop-ups op websites om in te stemmen met de verklaring. In beide gevallen werd aangegeven dat wanneer je niet expliciet akkoord ging met de verklaring (vaak door het aankruisen van een vakje), je geen diensten of producten (meer) kon afnemen van de betreffende organisatie. Meestal was het niet duidelijk waar je nu eigenlijk akkoord mee moest gaan. Met het verwerken van jouw persoonsgegevens? Of met het verstrekken daarvan aan derde partijen?

* Mw. B. Oenema is werkzaam bij BKR als manager Risk en Compliance, binnen deze afdeling vallen de deelgebieden Risk, Compliance, Privacy, Security en Legal. Tevens is zij voorzitter kennistafel Privacy bij de VCO. Dhr. M. van der Waal is Compliance Officer bij Vesteda en lid kennistafel Privacy bij de VCO. Dhr. B. Lashkari is Compliance Officer en Privacy specialist ad interim, lid kennistafel Privacy bij de VCO.

De AVG bepaalt dat het verlenen van algemene toestemming niet is toegestaan. De toezichthouder Autoriteit Persoonsgegevens (AP) schrijft hierover: 'Toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel. Indien een organisatie bij de verwerking meerdere doeleinden heeft, dient deze de betrokkene hierover te informeren en betrokkene voor elk doel afzonderlijk toestemming te vragen'. Hoe komt het dan toch dat na ruim drie maanden na de invoering van de AVG nog door veel organisaties om algemene toestemming wordt gevraagd voor de privacyverklaring? Het betreft naar ons idee een vorm van schijnveiligheid. Een van de redenen waarom organisaties toestemming verlangen op de privacyverklaring is dat zij het idee hebben dat daarmee een *licence to operate* ontstaat voor het gebruik van persoonsgegevens. Dit is echter niet waar, integendeel zelfs! Met een privacyverklaring wordt alleen informatie verstrekt over de verwerking van persoonsgegevens. Het geeft een organisatie niet het recht om de op dat moment ontvangen persoonsgegevens naar eigen goeddunken te gebruiken. In die zin is een privacyverklaring een eenzijdige overeenkomst waarin je van de bezoeker of klant geen juridisch bindende toezeggingen kunt verlangen.

Met een privacyverklaring wordt alleen informatie verstrekt over de verwerking van persoonsgegevens. Het geeft een organisatie niet het recht om de op dat moment ontvangen persoonsgegevens naar eigen goeddunken te gebruiken

Indien een organisatie voor het verwerken van persoonsgegevens toestemming als grondslag nodig heeft, dan moet dat duidelijk en steeds afzonderlijk van de betrokkene worden gevraagd. Dat kan dus nooit via een privacyverklaring. Eenmaal verkregen toestemming voor een privacyverklaring, waarin diverse verwerkingsdoeleinden staan opgesomd, heeft juridisch geen rechtskracht. Wanneer voor een verwerking (van persoonsgegevens) toestemming nodig is, dient dit steeds uitdrukkelijk en apart gevraagd te worden. De conclusie van dit geheel: toestemming geven voor een privacyverklaring hoeft niet en heeft geen rechtskracht.

Privacyverklaring

Ook in de aanloop naar de AVG waren er veel radiocommercials waarin werd verkondigd dat het opstellen van een privacyverklaring *a piece of cake* is. Zo'n privacyverklaring zou volgens de commercial binnen een half uurtje door de adviseur zijn opgesteld. Voor degenen die hebben gewerkt aan een nieuwe privacyverklaring is het wel duidelijk dat het opstellen van een adequate privacyverklaring meer tijd kost dan een half uur. Dit zou nog wel kunnen gelden voor kleine verenigingen en organisaties die alleen een leden- en/of een klantenadministraties bijhouden. Maar zodra een organisatie meer (categorieën van) persoonsgegevens verwerkt of persoonsgegevens voor meerdere doeleinden verwerkt, dan red je het zeker niet met een half uur en een standaard privacyverklaring. Overweging 39 uit de AVG zegt het volgende: 'Dat beginsel (het transparantiebeginsel) **betreft** met name het informeren van de betrokkenen over de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking, alsook verdere informatie om te zorgen voor behoorlijke en transparante verwerking met betrekking tot de natuurlijke personen in kwestie en hun recht om bevestiging en mededeling te krijgen van hun persoonsgegevens die worden verwerkt.' Het transparantiebeginsel kent een relatieve component, doordat aan de tekst het woord 'betreft' is toegevoegd. Dus niet alleen hoe je communiceert is van belang, ook **wat** je communiceert is een onderdeel van transparantie.

Het hebben van alleen een (transparante) privacyverklaring is dus onvoldoende. Accountability houdt namelijk in dat iedere organisatie die persoonsgegevens verwerkt, ook moet kunnen laten zien *wat* er gebeurt met de persoonsgegevens

Accountability

In art. 5 lid 2 AVG wordt bepaald dat de verwerkingsverantwoordelijke niet alleen verantwoordelijk is voor de naleving van (onder andere) deze transparantie (informeren), maar deze ook moet kunnen aantonen. Dit laatste in het kader van de AVG-verantwoordingsplicht (*accountability*). Dat zou eenvoudig kunnen door te verwijzen naar het hebben van een privacyverklaring (het hoe). Maar omdat het transparantiebeginsel twee uitgangspunten kent: het hoe en wat, ben je er nog niet met alleen informeren. Het hebben van alleen een (transparante) privacyverklaring is dus onvoldoende. Accountability houdt namelijk in dat iedere organisatie die persoonsgegevens verwerkt, ook moet kunnen laten zien **wat** er gebeurt met de persoonsgegevens. Dit betekent dat wat de organisatie schrijft in de privacyverklaring ook aantoonbaar nagekomen moet worden (*accountable*). Een privacyverklaring is daarmee geen schijndocument of een verklaring voor de bühne. Wanneer een organisatie via de privacyverklaring bijvoorbeeld aangeeft dat het een actief beleid heeft op het gebied van bewaartermijnen en hiermee ook het opschonen van persoonsgegevens, dan moet de organisatie dit ook daadwerkelijk uitvoeren. De bewering 'na twee jaar opschonen' betekent dus dat de persoonsgegevens na twee jaar

ook echt opgeschoond moeten zijn (*accountability* = *auditability*). Wanneer de toezichthouder hierom vraagt, moet dit aantoonbaar kunnen worden gemaakt. Van *tell me* naar *show me*.

Dit alles vraagt dus om een zorgvuldige formulering van teksten en bepalingen in de privacyverklaring. Bij voorkeur zorgvuldig en daardoor misschien wat bescheiden in de formuleringen en in de uitgangspunten, dan klakkeloos een uitgebreide opsomming van zaken die in de praktijk niet waargemaakt kunnen worden. Met alleen een privacyverklaring op de website zonder gelijkwaardige inrichting van privacy binnen de organisatie, houdt de organisatie zowel de klant, zichzelf alsook de AP voor de gek. Let wel, de AP kan hoge boetes opleggen wanneer een organisatie niet kan aantonen dat het doet wat ze in de privacyverklaring aangeven te doen. Zeg 'wat' je doet en 'doe' wat je zegt.

Inhoud

In art. 13 en 14 AVG is beschreven voor 'wat' een organisatie moet communiceren. In art. 13 AVG staan de regels voor organisaties die de persoonsgegevens rechtstreeks bij natuurlijke personen verzamelen en art. 14 beschrijft de regels voor organisaties die de persoonsgegevens indirect, dus via een andere partij, ontvangen. Voor de indirecte ontvangst van persoonsgegevens geldt dat je aanvullend aan de regels van art. 13 moet vermelden via welke partij je de gegevens hebt ontvangen (bronvermelding). Persoonsgegevens zijn die gegevens waarmee je een natuurlijk persoon kunt identificeren of waarmee een natuurlijk persoon identificeerbaar is. Overweging 39 uit de AVG wettekst geeft iets meer duidelijkheid over wat binnen de context van de AVG wordt verstaan onder het 'wat'. Daarnaast heeft de Groep gegevensbescherming artikel 29 richtsnoeren opgesteld inzake transparantie overeenkomstig Verordening (EU) 2016/679.

Voor het 'wat' hebben we er niet voor gekozen om art. 13 en 14 AVG in dit artikel op te nemen, deze kun je ook lezen in de wet, de overweging en de richtsnoeren. We hebben wel acht aandachtspunten opgesteld, die iets meer verdieping geven over bepaalde regels in art. 13 AVG en van nut kunnen zijn bij het opstellen van een privacyverklaring voor jouw organisatie.

Daar waar een privacyverklaring gericht is op informatievoorziening naar klanten en/of bezoekers, maakt het privacybeleid onderdeel uit van de interne *governance* van de organisatie. In het privacybeleid staat beschreven hoe privacy compliance binnen de organisatie is ingericht, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits

1. Het opstellen van een privacyverklaring staat los van het hebben van privacybeleid. De AVG stelt zowel een privacyverklaring (art. 12), alsook het hebben van een privacybeleid (art. 24.2, 38.1 en 39.1b) verplicht. Tussen deze twee onderdelen is wel enige samenhang. De informatie die in de privacyverklaring staat, komt ook terug in het privacybeleid alleen dan meer organisatorisch uitgewerkt. Daar waar een privacyverklaring gericht is op informatievoorziening naar klanten en/of bezoekers, maakt het privacybeleid onderdeel uit van de interne *governance* van de organisatie. In het privacybeleid staat beschreven hoe *privacy compliance* binnen de organisatie is ingericht, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits. Een privacybeleid is gedetailleerder en kan vertrouwelijke interne processen bevatten, maar ook verplichte onderdelen zoals *privacy by design* (gegevensbescherming door ontwerp) en *privacy by default* (Privacy by default vereist dat de standaardinstellingen altijd zo privacy vriendelijk mogelijk zijn).
2. Heeft de organisatie een Functionaris voor de Gegevensbescherming (FG), dan moeten de contactgegevens van deze FG worden vermeld in de Privacyverklaring. Dit betekent niet dat het verplicht is om de naam van de FG bekend te maken. Wel moeten de contactgegevens die je in de Privacyverklaring opneemt informatie bevatten die de betrokkenen en de toezichthouders in staat stellen om de FG gemakkelijk te bereiken. Dit kan bijvoorbeeld door het opnemen van een postadres, een speciaal telefoonnummer of een speciaal e-mailadres, hotline of een contactformulier.
3. Geef naast de informatie over de doelen en grondslagen waarvoor je persoonsgegevens verzamelt ook een lijst met de persoonsgegevens die worden verwerkt. Persoonsgegevens zijn alle gegevens die informatie kunnen verschaffen over een geïdentificeerd of identificeerbare natuurlijke persoon. Niet ieder persoonsgegeven is op zichzelf een persoonsgegeven, maar, kan aan elkaar gerelateerd wel een persoonsgegeven worden, bijvoorbeeld een huisnummer en postcode alleen zeggen niet zo veel, maar gecombineerd is het een persoonsgegeven.
4. Verstrek je persoonsgegevens aan anderen, houd dan bij het opstellen van de informatie over deze partijen rekening met de definities 'ontvangers' en 'derden' in de AVG, art. 4 sub 9 en 10. In de praktijk worden doorgaans deze ontvangers bij naam genoemd zodat betrokkenen precies weten

wie hun persoonsgegevens heeft. Indien je ervoor kiest om de informatie in categorieën van ontvangers te verstrekken, dan moet je deze informatie zo specifiek mogelijk beschrijven door bijvoorbeeld een aanduiding van het type ontvangers en de industrie, de sector, de subsector en de locatie van de ontvangers.[1]

5. Wanneer gegevens worden verstrekt aan een derde land, houd er dan rekening mee dat dit de landen betreft buiten de EU, inclusief Noorwegen, IJsland en Liechtenstein. Deze landen hanteren namelijk hetzelfde niveau van persoonsgegevensbeveiliging als voor EU-burgers geldt. Gezamenlijk wordt dit de Europese Economische Ruimte genoemd.

Het in algemene zin verklaren dat persoonsgegevens alleen zo lang bewaard worden als nodig is voor de verwerking voor bepaalde doeleinden is onvoldoende. Dit moet je nader specificeren

6. Het beschrijven van de bewaartermijnen is voor de meeste organisaties lastig. De AVG stelt zelf geen bewaartermijnen, wel zegt de AVG iets over bewaren in art. 5. Het komt erop neer dat een organisatie persoonsgegevens niet langer mag bewaren dan strikt noodzakelijk is. Het in algemene zin verklaren dat persoonsgegevens alleen zo lang bewaard worden als nodig is voor de verwerking voor bepaalde doeleinden is onvoldoende. Dit moet je nader specificeren. In diverse wetten of sectorale regelgeving staat een aantal verplichte bewaartermijnen, deze zijn altijd leidend. In die gevallen waarin er geen bewaartermijn door de wet of sector is vastgesteld, moet de organisatie zelf de criteria vaststellen. Bij het opstellen van de criteria moet je rekening houden met het principe dat de persoonsgegevens niet te lang, maar ook niet te kort bewaard mogen worden en alleen die gegevens mogen worden bewaard die noodzakelijk zijn voor de verwerking. Bij het opstellen van de criteria mag alleen rekening gehouden worden met de bestaande verwerking, niet met eventuele toekomstige verwerkingen. Deze criteria moeten uitlegbaar en begrijpelijk zijn. De informatie over de verschillende bewaartermijnen moet per categorie van persoonsgegevens en/of verschillende verwerkingsdoeleinden specifiek worden vermeld en waar passend, inclusief de archiveringsperioden.
7. Het informeren over de rechten van de betrokkenen moet duidelijk, expliciet en begrijpelijk gebeuren. Dit betekent dat een betrokkene de informatie snel moet kunnen vinden. Het is niet verplicht om alle rechten afzonderlijk in artikelen te plaatsen, deze mogen ook in één artikel geplaatst worden. Daarnaast moet het voor de betrokkene volkomen duidelijk zijn welke verwerkingsverantwoordelijke hij of zij kan benaderen om een of meer van zijn of haar rechten uit te oefenen.
8. Belangrijk is dat duidelijke informatie wordt opgenomen over profilering[2], de werking van het geautomatiseerde besluitvormingsproces, de onderliggende logica, het belang van de verwerking en de verwachte gevolgen van die verwerking voor de betrokkene. De betrokkene heeft het recht informatie te verkrijgen over alle persoonsgegevens die voor profilering worden gebruikt, met inbegrip van de categorieën gegevens die zijn gebruikt om een profiel op te stellen. Naast deze informatie moet ook informatie worden verstrekt over de gegevens die gebruikt zijn als invoer voor het aanmaken van het profiel, de toegang tot de profielinformatie alsook de informatie in welk segment een betrokkene is ingedeeld conform het profiel.

Communicatievormen

De AVG zegt ook 'hoe' gecommuniceerd moet worden. Hoe eenvoudig de privacyverklaring te begrijpen en te lezen moet zijn, is afhankelijk van de doelgroep waarvoor het bestemd is. Op een website moet de verklaring snel vindbaar zijn. De privacyverklaring mag niet worden gekoppeld aan niet-privacy gerelateerde informatie zoals een aankoop, een contract of algemene gebruiksvoorwaarden. Voorkom informatiemoeheid waardoor een betrokkene niet meer de moeite neemt om de privacyverklaring te lezen. Uit art. 12 AVG kun je herleiden dat de geboden informatie beknopt, transparant, makkelijk toegankelijk, eenvoudig te lezen en begrijpelijk moet zijn. Houd er rekening mee dat wanneer een betrokkene daarom verzoekt, de informatie mondeling moet worden meegedeeld. Art. 12 lid 7 AVG geeft de mogelijkheid om informatie via gestandaardiseerde iconen aan te bieden. Voorbeelden hiervan zijn een duidelijke hyperlink of icoon op iedere pagina naar de privacyverklaring.

Het is belangrijk om te weten dat je je bij een privacyverklaring niet hoeft te beperken tot alleen een schriftelijke elektronische verklaring. Je kunt ook gebruik maken van een combinatie van methoden. Denk hierbij bijvoorbeeld aan contextuele 'just-in-time'-pop-upberichten, 3D Touch-berichten, *frequently asked questions*, mededelingen die verschijnen wanneer de muis eroverheen beweegt, privacydashboards en privacy chatboxen. Niet-schriftelijke elektronische middelen die je kunt inzetten zijn bijvoorbeeld filmpjes, cartoons, *infographics* of stroomschema's. Wanneer de privacyverklaring voor kinderen bestemd is, houd dan rekening met de doelgroep en pas de

[1] Groep gegevensbescherming artikel 29, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679. Goedgekeurd op 29 november 2017. Laatstelijk herzien en goedgekeurd op 11 april 2018.

[2] Zie art. 4.4 AVG definitie profilering.

manier van communiceren aan het kind aan. Denk hierbij aan stripverhalen/cartoons, pictogrammen, tekenfilms, enzovoorts. Je kunt ook denken aan een gelaagde privacyverklaring. Veel bedrijven hanteren deze vorm. Bij een gelaagde uitvoering van je privacyverklaring begin je met een korte samenvatting. Wanneer een betrokkene meer informatie wil lezen over het onderwerp, dan kan dit worden gevonden in een van de onderliggende tabbladen. Wanneer je gebruik maakt van een privacyverklaring in een gelaagde structuur of andere vormen van communicatie om je privacyverklaring onder de aandacht te brengen, dan moet je er rekening mee houden dat de privacyverklaring ook in haar geheel op één plaats beschikbaar moet zijn, bijvoorbeeld als pdf-bestand.

Conclusie

Veel organisaties onderschatten wat ze nog allemaal moeten doen om compliant te worden en te blijven. Het heeft geen zin om te verwijzen naar andere organisaties die de regels niet naleven, bijvoorbeeld omdat die de privacyverklaring ook nog niet hebben geüpdatet. Iedere organisatie heeft haar eigen verantwoordelijkheid om compliant te zijn. Het voornaamste is dat organisaties realiseren dat er nog veel werk aan de winkel is. Wanneer je denkt dat je eenmaal AVG-compliance bent, dan begint het vaak weer opnieuw doordat nieuwe rechterlijke uitspraken en *guidelines* van toezichthouders zijn. Of je start met nieuwe verwerkingen van persoonsgegevens of er komt een nieuwe verordening aan, zoals de e-Privacy verordening. Deze laatste kan enorme invloed hebben op de huidige marketingactiviteiten want vrijwel iedere organisatie verstuurt wel eens een nieuwsbrief en past cookies toe. Het proces van privacy regelnaleving vraagt om continue aandacht.

We wensen je daarom veel succes en wijsheid bij het opstellen van de Privacyverklaring en de naleving van de overige AVG-bepalingen. ■

Dit artikel komt voort uit de VCO Kennistafel Privacy. De VCO kent verschillende Kennistafels. In een Kennistafel werken leden aan concrete producten, zoals de Toolbox Gedrag & Cultuur, het Beroepscompetentieprofiel en een privacy-bibliotheek. In een open sfeer delen de leden hun kennis en expertise met vakgenoten. De producten blijken vaak een standaard te zetten voor compliance officers. Hiermee helpen we onze leden hun rol te vervullen. Onze omgeving hecht hier waarde aan en externe toezichthouders zoals DNB, AFM en andere toezichthouders staan hier positief tegenover.