De verantwoordingsplicht onder de AVG

De verantwoordingsplicht onder de AVG

19-06-2018

Organisaties moeten voor de verwerkingen waarvoor zij verwerkingsverantwoordelijke zijn in de zin van de privacyregelgeving kunnen aantonen dat zij de persoonsgegevens in overeenstemming met de basisbeginselen uit de privacyregelgeving verwerken. Deze nieuwe verplichting uit art. 5 lid 2 AVG heet ook wel de 'verantwoordingsplicht' of *accountability*. In dit artikel ga ik (*Liesbeth Woolschot, red.*) in op deze nieuwe verplichting aan de hand van informatie van een paar toezichthouders binnen de EU.

Wat houdt de verantwoordingsplicht in?

Om te kunnen aantonen dat wordt voldaan aan de privacyregelgeving zal de organisatie een aantal documenten moeten opstellen met betrekking tot de persoonsgegevens die door haar worden verwerkt. Art. 5 lid 1 AVG bevat de belangrijkste beginselen waar een verwerking aan dient te voldoen, zoals rechtmatigheid, transparantie, doelbinding en juistheid van de gegevens. Een aantal verplichtingen uit de AVG bieden concrete handvatten voor de invulling van deze verantwoordingsplicht. Hieronder bespreek ik daar een aantal van.

Register van verwerkingsactiviteiten

In art. 30 AVG staat de registerplicht. Alle verwerkingsactiviteiten zullen moeten worden vastgelegd in een register. Dit is de basis van de verantwoordingsplicht. Het register zal ook getoond moeten worden aan de toezichthouder als deze daar om verzoekt. In het register moet onder meer per verwerkingsactiviteit vastgelegd worden welke persoonsgegevens worden verwerkt, voor welke doeleinden en van welke categorieën betrokkenen. Daarnaast zal de toegang tot de gegevens, de bewaartermijn en de beveiliging moeten worden omschreven.

Beveiligingsbeleid

Art. 24 en 32 AVG verplichten zowel de verwerkingsverantwoordelijke als de verwerker tot het treffen van passende technische en organisatorische beveiligingsmaatregelen om te waarborgen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Deze maatregelen moeten worden vastgelegd in een gegevensbeschermingsbeleid 'wanneer dit in verhouding staat met de verwerkingsactiviteiten'.

Registratie van datalekken

Op grond van art. 33 lid 5 AVG zijn organisaties verplicht om datalekken te documenteren. Dat betekent dat een datalekprocedure nodig is en dat *alle* datalekken goed moeten worden geregistreerd.

Privacy by design, privacy by default en DPIA's

In de AVG zijn in art. 25 de principes van privacy by design en privacy by default opgenomen. Dit houdt kort gezegd in dat de instellingen in systemen die persoonsgegevens verwerken, zoals websites en apps, standaard moeten worden ingesteld op minimale gegevensverwerking. Voor verwerkingen die een hoog risico met zich brengen voor de rechten en vrijheden van betrokkenen zal de verwerkingsverantwoordelijke volgens art. 35 AVG een data protection impact assessment (DPIA) uit moeten voeren. Een risico-analyse van de verwerking met het bepalen van waarborgen om de privacy te beschermen.

Informatieplicht

De verwerkingsverantwoordelijke moet betrokkenen informeren conform art. 13 en 14 AVG. Dat kan in een online privacyverklaring waarin onder meer beschreven staat welke persoonsgegevens worden verwerkt voor welke doelen, wie de ontvangers van de gegevens zijn, hoe lang de gegevens worden bewaard en wat de grondslag is van de verwerking.

Functionaris voor de Gegevensbescherming (FG)

Voor overheidsinstanties en organisaties die op grote schaal bijzondere persoonsgegevens verwerken is het op grond van art. 37 AVG verplicht om een FG aan te stellen. De FG houdt onder meer intern toezicht op de naleving van de privacyregelgeving door de organisatie.

Uit art. 40-43 AVG volgt dat het aansluiten bij een gedragscode of certificering kan bijdragen aan een juiste toepassing van de AVG. Toezichthouders, lidstaten en het EDPB (European Data Protection Board) bevorderen deelname hieraan, onder meer door het accrediteren van de gedragscodes en certificeringen.

Aanknopingspunten privacytoezichthouders

De Autoriteit Persoonsgegevens (AP) ziet de verantwoordingsplicht als een instrument voor organisaties om een belangrijke bijdrage te kunnen leveren aan de bescherming van persoonsgegevens. Zij moedigt organisaties aan om bepaalde keuzes te documenteren, zoals de keuze om geen FG aan te stellen of geen DPIA uit te voeren als er twijfel bestaat of dat verplicht is. De AP geeft tevens aan dat de vraag of een gegevensbeschermingsbeleid moet worden opgesteld afhangt van de aard, de omvang, de context en het doel van de gegevensverwerking, maar dat dit wel raadzaam is om te doen.

De Information Commissioner's Office (ICO), toezichthouder in het Verenigd Koninkrijk, heeft een actieve en informerende rol met betrekking tot de AVG. De ICO geeft aan dat de verantwoordingsplicht een middel is om het vertrouwen van betrokkenen te vergroten en zo eventuele handhaving te beperken. ICO heeft een korte checklist opgesteld voor organisaties om te kunnen voldoen aan de verantwoordingsplicht. ICO wijst erop dat organisaties niet alleen maatregelen moeten treffen, maar deze ook moeten evalueren en beoordelen.

De Belgische privacyautoriteit, de Gegevensbeschermingsautoriteit, geeft aan dat de verantwoordingsplicht de rode draad vormt door de AVG. De Belgische autoriteit noemt als kern van de verantwoordingsplicht:

"De AVG verwacht dus van de verwerkingsverantwoordelijke een algemene, verhoogde behoedzaamheid en aandacht. Dit brengt met zich mee dat de verwerkingsverantwoordelijke er vanaf nu volledig moet voor instaan dat de regels daadwerkelijk worden nageleefd en hij is ten aanzien van de toezichthoudende autoriteiten aansprakelijk voor de maatregelen die hij daartoe heeft genomen."

De onafhankelijke Europese privacy autoriteit, de European Data Protection Supervisor (EDPS) legt bij haar uitleg over de verantwoordingsplicht de nadruk op passende technische en organisatorische beveiligingsmaatregelen. Organisaties moeten kunnen laten zien waarom ze voor die maatregelen hebben gekozen en dat zij effectief zijn. De EDPS noemt een aantal concrete maatregelen, waaronder in ieder geval het bijhouden van adequate documentatie en procedures. Het European Data Protection Board (EDPB), voormalig Werkgroep 29, belooft 'accountability tools' te publiceren, maar die zijn nog niet gepubliceerd.

Conclusie

De AVG bevat veel verplichtingen waarbij de verwerkingsverantwoordelijke zelf een afweging moet maken. Over de maatregelen die zij neemt hebben moet verantwoording worden afgelegd. Hoe de invulling van de verplichting er precies uit gaat zien en welke eisen er nader aan gesteld zullen worden is nog niet concreet. Verwerkingsverantwoordelijken zullen in ieder geval moeten voldoen aan de concrete maatregelen die de AVG noemt, zoals bijhouden van een verwerkingsregister of het opstellen van een privacyverklaring. Verder is het raadzaam om de keuze om bepaalde maatregelen niet te nemen te documenteren.

Dit artikel is geschreven door Liesbeth Woolschot van Hekkelman Advocaten te Nijmegen.

GEGEVENS

Wetgeving	
Jurisprudentie	
Officiële publicaties	
Europese regelgeving	
Soort nieuws	Beleid
Publicatiedatum	19-06-2018
Nummer	2018/17