OP **25 MEI 2018** TREEDT DE AVG (GDPR) IN WERKING

Nieuwe privacyregels

WAT MOET JE DOEN?

De media besteden al geruime tijd uitgebreid aandacht aan de nieuwe Europese privacyregels per 25 mei 2018. Desondanks onderschatten veel ondernemers wat ze in hun dagelijkse praktijk moeten gaan doen om deze nieuwe regels straks correct na te leven. Een korte rondleiding door deze regels.

CASPAR RUTTEN

De nieuwe privacyregels zijn opgenomen in de Algemene Verordening Gegevensbescherming, afgekort AVG (in het Engels GDPR: General Data Protection Regulation). De verordening werkt vanaf 25 mei aanstaande rechtstreeks in alle EER-landen (EU + 3). Daardoor worden de privacyregels in principe in de gehele EER gelijk getrokken, met dien verstande dat lidstaten hier op bepaalde gebieden toch nog van af zullen kunnen wijken, zodat er per land nog weer verschillen zijn.

Verwerking persoonsgegevens

De AVG gaat over de verwerking van persoonsgegevens, waarbij onderscheid wordt gemaakt tussen (verwerkings)verantwoordelijken en verwerkers. Het begrip 'verwerken' beperkt zich overigens niet tot het bewerken van persoonsgegevens, maar strekt zich ook uit tot het opslaan van deze gegevens in een bestand . De term 'persoonsgegeven' wordt heel ruim uitgelegd. Het gaat om de gegevens van een identificeerbare persoon. Welke gegevens dat zijn, hangt af van de omstandigheden. Het bekendste persoonsgegeven is de naam, maar denk bijvoorbeeld ook aan een persoonlijk e-mailadres, BSN-nummer, leeftijd of mogelijk een camerabeeld of IP-adres. Bedrijfsgegevens (zoals een vestigingsadres) vallen er meestal niet onder, maar bij een eenmanszaak kan dat anders zijn. Bepaalde soorten gegevens kunnen dus persoonsgegevens zijn, maar zijn dat ook weer niet altijd. Het is belangrijk om een goed overzicht te hebben van alle gegevens die (mogelijk) persoonsgegevens zijn. Voor bijzondere persoonsgegevens, zoals de gegevens over iemands gezondheid, gelden strengere regels. De lijst met mogelijke persoonsgegevens is overigens dermate lang, dat deze bewust niet is opgenomen bij dit artikel.

Doelomschrijving en algemene beginselen

De verwerking van de persoonsgegevens moet plaatsvinden op basis van een van de zes mogelijke grondslagen in de AVG. Daartoe behoren onder meer: toestemming, noodzaak voor de uitvoering van een overeenkomst of een gerechtvaardigd belang. Verder moet aan een aantal algemene beginselen worden voldaan, waaronder rechtmatigheid en transparantie. Dit betekent dat betrokkenen (personen van wie gegevens worden verwerkt) moeten worden geïnformeerd over de verwerking van hun gegevens. Ook geldt 'doelbinding'; gegevens mogen alleen worden gebruikt voor vooraf vastgestelde doelen. Alleen noodzakelijke gegevens mogen worden verwerkt – en niet langer dan nodig. De AVG stelt (uiteraard) ook eisen aan beveiliging en juistheid. Het is dus nodig om passende technische en organisatorische maatregelen te nemen om gegevens te beschermen. Onjuiste gegevens moeten worden gecorrigeerd of gewist.

Rechten betrokkenen

Betrokkenen hebben allerlei rechten. Zo hebben zij het recht om:

- hun gegevens in te zien;
- onjuiste gegevens te laten corrigeren;
- (in bepaalde gevallen) te verzoeken om gegevens te laten wissen;
- te vragen om een digitale kopie van de opgeslagen gegevens, zodat deze aan een andere partij kunnen worden overgedragen.

Datalekken

De AVG kent een verplichting om onder bepaalde omstandigheden datalekken te melden. Aan de Autoriteit Persoonsgegevens (AP) en aan de betrokkenen die het betreft.

Register, DPIA en functionaris (DPO)

Ondernemers moeten – tenzij de uitzondering van toepassing is, een register bijhouden van alle verwerkingsactiviteiten. Soms zijn zij verplicht een risicoanalyse (DPIA) uit te voeren en in bepaalde gevallen moet er een functionaris gegevensbescherming (in het Engels een DPO: Data Protection Officer) worden aangesteld. Een organisatie moet op verzoek van de Autoriteit Persoonsgegevens kunnen aantonen dat zij aan de wet voldoet.

Procedures

Procedures (zowel intern als extern gericht) moeten ervoor zorgen dat de AVG goed wordt uitgevoerd. Dit is van groot belang. Voor het doorgeven van persoonsgegevens aan derden (bijvoorbeeld om ze in de cloud op te slaan of voor de salarisverwerking) gelden ook strenge regels. Als de ontvanger buiten de EER gevestigd is, is een dergelijke doorgifte alleen toegestaan als aan allerlei eisen is voldaan. In alle gevallen moeten er contracten worden gesloten en moet er een privacypolicy/-statement zijn.

Boetes en aansprakelijkheid

Er kunnen hoge boetes worden opgelegd wanneer je als organisatie de AVG aan je laars lapt: in principe maximaal € 20 miljoen – en soms zelfs nog meer. Ook kan er hoofdelijke aansprakelijkheid bestaan. Daarnaast riskeer je als organisatie ook imagoschade. Idealiter zijn dit niet de voornaamste prikkels om de AVG goed na te willen leven, maar ben je als organisatie intrinsiek gemotiveerd om zorgvuldig om te gaan met de persoonsgegevens van je klanten, leveranciers en personeel.

Informatie en tools

Diverse branche- en ondernemersverenigingen hebben inmiddels allerlei brochures, (lijvige) handleidingen en tools gemaakt waarmee je je goed op de komst van de AVG kunt voorbereiden. Ook BOVAG heeft dat gedaan. (Zie ook het 'Het AVG-10 stappenplan' op www.autoriteitpersoonsgegevens.nl.) Praktische hulpmiddelen zijn uiteraard handig. Want handleidingen mogen dan wel veel informatie bieden, u moet er uiteindelijk gewoon in de praktijk mee aan de slag! Wie dit goed wil doen, zal er voldoende tijd voor vrij moeten maken. Nuttige informatie en begeleiding zijn daarbij onmisbaar, want de materie is vooralsnog complex.

Mr. C.A.I.J. Rutten CIPP/E, Advocatenkantoor Rutten.

Voor het doorgeven van persoonsgegevens aan derden **gelden strenge regels**