Artikel Privacy & informatiebeveiliging
Tekst Drs. Laszlo Nagy EMIA RO
Beeld Koen Olsthoorn

AVG: techniek of **gedrag**?

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Organisaties die persoonsgegevens verwerken krijgen dan meer verplichtingen. Meer dan onder de huidige Wet bescherming persoonsgegevens (Wbp) ligt de verantwoordelijkheid bij de organisaties zelf om aan te tonen dat zij voldoen aan de eisen van de wet. Wat zijn de belangrijkste elementen van de AVG en waar ligt de nadruk: op techniek of gedrag?

Al vele jaren moeten organisaties die – al dan niet bijzondere – persoonsgegevens verwerken voldoen aan privacyregels. De huidige Wbp is inmiddels goed bekend in Nederland. Onder deze wet moeten organisaties die persoonsgegevens verwerken (of: 'bewerken') zich houden aan een aantal regels, zoals het vastleggen van het doel van de verwerking, het op een adequate wijze beveiligen van persoonsgegevens en het melden van datalekken. De Autoriteit Persoonsgegevens (AP) is verantwoordelijk voor het handhaven van de regels. Waar nodig, kan de AP onderzoek uitvoeren bij organisaties of zelfs een bestuurlijke boete tot 820.000 euro opleggen. Hoewel de Wbp goed bekend is in Nederland, is het maar de vraag in hoeverre organisaties de huidige wet écht serieus nemen.
Met de nieuwe AVG, in Europa bekend als General Data Protection Regulation (GDPR), verandert het een en ander drastisch. Niet alleen wordt het aantal rechten van 'natuurlijke personen' flink uitgebreid, ook worden de rechten inhoudelijk versterkt. Hierdoor neemt de impact op organisaties die persoonsgegevens verwerken fors toe. Tot slot gaat het er niet alleen om dát je als organisatie voldoet aan die nieuwe regels, maar dat je dat ook aantoonbaar doet. Dus niet meer impliciet, maar expliciet compliant zijn. En als kers op de taart: als organisaties ernstig en/of verwijtbaar de nieuwe regels aan hun laars lappen, kan de bestuurlijke boete oplopen tot zelfs 20 miljoen euro of 4% van de wereldwijde jaaromzet!

Stappenplan
Inmiddels zijn zowel door de AP als door andere organisaties handreikingen en stappenplannen geïntroduceerd teneinde te helpen aan de AVG te voldoen. De AP heeft eind 2017 het *In 10 stappen voorbereid op de AVG* gepubliceerd, die de belangrijkste stappen beschrijft.

Stap 1 – Bewustwording
Relevante stakeholders, zoals directie en beleidsmakers, moeten bekend zijn met de AVG. Zij moeten bepalen wat de impact ervan is op de organisatie, processen en

Hoe beter de beveiliging hoe sneller mensen geneigd zijn het olifantenpaadje te willen vinden

werkwijzen en welke aanpassingen nodig en wenselijk zijn. Aanpassingen aan organisatie, processen en werkwijzen als gevolg van de AVG kunnen behoorlijke impact hebben, zelfs op het verdienmodel.

Stap 2 – Rechten van betrokkenen
Met de AVG krijgen betrokkenen (natuurlijke personen) niet alleen sterkere, maar ook meer rechten. Versterkte rechten zijn er bijvoorbeeld ten aanzien van inzage, correctie en verwijdering. Een nieuw recht is er ten aanzien van data-portabiliteit, waarbij betrokkenen hun gegevens eenvoudig moeten kunnen opvragen ten behoeve van bijvoorbeeld een overstap naar een andere leverancier.

Stap 3 – Overzicht verwerkingen
Organisaties moeten in een 'verwerkingenregister' in kaart brengen welke persoonsgegevens worden verwerkt, met welk doel, waar de gegevens vandaan komen en met wie ze worden gedeeld. Onder de AVG is er een verantwoordingsplicht, dat wil zeggen dat aangetoond moet kunnen worden dat conform de wetgeving wordt gewerkt. Het verwerkingenregister is onderdeel van de verantwoordingsplicht, maar is ook nodig om de privacyprocessen goed uit te kunnen voeren. Bijvoorbeeld bij het opvragen, corrigeren of verwijderen van persoonsgegevens.

Stap 4 – Data protection impact assessment
Als een beoogde gegevensverwerking een hoog privacyrisico met zich meebrengt, is het verplicht om een data protection impact assessment (DPIA) uit te voeren. Daarmee worden vooraf de privacyrisico's van een gegevensverwerking in kaart gebracht en kunnen vervolgens de juiste maatregelen worden bepaald om de risico's te beperken. Indien er onvoldoende (sterke) beperkende maatregelen zijn, is er de verplichting om vooraf de AP te raadplegen.

Stap 5 – Privacy by design & privacy by default
Belangrijke uitgangspunten van de AVG zijn privacy by design en privacy by default.
Privacy by design houdt in dat al bij het ontwerpen van producten en diensten de vereisten van de AVG worden toegepast. Bijvoorbeeld een adequate bescherming, het niet meer gegevens verzamelen dan strikt benodigd voor het beoogde doel en niet langer dan benodigd (of wettelijk vereist) bewaren. Niet meer 'nice to have' maar 'need to have'.
Privacy by default houdt in dat technische en organisatorische maatregelen worden genomen om te zorgen dat, als standaard, alléén persoonsgegevens worden geregistreerd en verwerkt die noodzakelijk zijn voor het specifieke doel

van de verwerking. Het bekende standaard ingevulde vinkje bij 'akkoord met algemene voorwaarden' mag dan niet meer, gebruikers moeten zelf ondubbelzinnig akkoord geven.

Stap 6 – Functionaris gegevensbescherming
Bepaalde organisaties zijn verplicht om een formele Functionaris Gegevensbecherming (FG) aan te stellen. Dit geldt in de basis voor overheids- en publieke organisaties, voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen en voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken en waarvoor dit een kernactiviteit is.

Stap 7 – Meldplicht datalekken
Net als onder de Wbp geldt onder de AVG een meldplicht voor datalekken. De AVG stelt wel strengere eisen aan de registratie en documentatie van de datalekken, op basis waarvan de AP moet kunnen controleren of aan de meldplicht is voldaan.

Stap 8 – Bewerkersovereenkomsten / Verwerkersovereenkomsten
Indien (een deel van) de verwerking van persoonsgegevens is uitbesteed aan een derde partij (bewerker, 'verwerker' volgens de AVG), moet beoordeeld worden of deze partij ook op de juiste manier voldoet aan de eisen van de AVG ten aanzien van persoonsgegevens die zijn 'uitbesteed'. Een en ander dient vastgelegd te zijn in een verwerkersovereenkomst. Uitbesteden betekent dus niet het uitbesteden van de verantwoordelijkheid.

Stap 9 – Leidende toezichthouder
Wanneer een organisatie vestigingen in meerdere EU-lidstaten heeft dan wel de gegevensverwerkingen impact hebben in meerdere lidstaten, bijvoorbeeld een webwinkel die in meerdere landen actief is, hoeft er onder de AVG nog maar met één privacytoezichthouder te worden gewerkt: de leidende toezichthouder. Bepaald moet worden onder welke toezichthouder de organisatie valt.

Stap 10 – Toestemming
Het verzamelen en verwerken van persoonsgegevens mag niet zomaar plaatsvinden. Er moet sprake zijn van een algemeen belang, een gerechtvaardigd belang, een vitaal belang, een overeenkomst, een wettelijke verplichting of toestemming van de betrokkene. De AVG stelt strengere eisen aan toestemming. Aangetoond moet kunnen worden dat geldige toestemming is verkregen om van een betrokkene persoonsgegevens te verwerken. Voorts moet het intrekken

van de toestemming net zo makkelijk zijn als het geven van toestemming.

Techniek of gedrag?
Zoals in het 10-stappenplan zichtbaar is, betekent het aantoonbaar voldoen aan de AVG het naleven van een flinke set van formele regels. De vraag is of de primaire oplossingsrichting hiervoor ligt in de techniek. In bijvoorbeeld goede beveiliging of het vragen van expliciete toestemming. Of ligt de primaire oplossingsrichting meer aan kant van de business, de bewustwording en het gedrag van de organisatie? Het antwoord is: het laatste! Het gaat dan met name om zaken als verzamelwoede, schijnveiligheid en werkbaarheid.
Allereerst de ontembare verzamelwoede, we lijken soms wel strandjutters. Alles wat aanspoelt, is van ons en bewaren we. Geen idee of de eigenaar het goed vindt, maar laten we het maar gewoon bewaren en waar nodig gebruiken. 'Doe mij ook een kopietje' of 'doe dat er maar voor de zekerheid bij' zijn hiervan typische voorbeelden. Hiermee verzamelen en bewaren we – soms écht onbewust – enorme hoeveelheden (persoons)gegevens. Van cv's van sollicitanten die we jarenlang bewaren tot kopietjes van een paspoort 'voor het geval dat'. Op dit vlak hebben we allemaal opvoeding nodig: afvragen waarom we die informatie willen of écht nodig hebben. Maar ook of we die gegevens wel mogen hebben.
Daarnaast is er de schijn van veiligheid door de veelvuldige focus op informatiebeveiliging. Doordat er zoveel aandacht voor is, denken we (te) snel dat ons niets meer kan gebeuren. 'Het zal best goed beveiligd zijn' denken we dan. Maar aan de achterkant van het schijnbaar veilige fort zit het gezellige achtertuintje waar de medewerkers vertoeven. Medewerkers die zich veilig wanen, 'we hebben immers een virusscanner en een firewall', maar ook medewerkers die graag gemak willen hebben en de onbegrijpelijke of onwerkbare regels graag omzeilen. Hoe beter de beveiliging – en daarmee des te meer sloten op de deur – hoe sneller mensen geneigd zijn toch het olifantenpaadje, ook wel de 'work around', te willen vinden. Je kent het wel, het versleten stukje graspad dat naast de mooie en dure slagboom loopt. Of de nooddeur aan de achterkant van het zwaarbeveiligde gebouw die de hele dag open is om makkelijk van en naar het rookhok te kunnen lopen. Dit zijn niet alleen figuurlijk, maar ook letterlijk de achterdeuren waar kwaadwillenden naarstig naar op zoek zijn.

Wat te doen?
Veiligheid en compliance zijn zaken waar we ons allereerst goed bewust van moeten zijn. We moeten het 'waarom' begrijpen. We moeten ons ervan bewust zijn waarom we iets verzamelen en wat we ermee doen. En waarom we het op een bepaalde manier beveiligen. Maar ook waarom de personen in kwestie bepaalde rechten hebben. Bewustwording is ook jezelf afvragen wat je ervan zou vinden als dat jouw – al dan niet bijzondere – persoonsgegevens zouden zijn. De spiegel voorhouden dus.
Tot slot moet het werkbaar zijn. Anders maak je – bewust of onbewust van de regels – 'voor het werkgemak' toch die lokale kopie van de klantgegevens op je privétablet. En ben je onbewust onderweg naar non-compliance. Of naar erger: een datalek.
Soms kunnen we gewoon wat minder opvragen en bewaren om nog steeds prima ons werk te kunnen doen. Waarom heeft een internetwinkel je volledige geboortedatum nodig? Is een geboortejaar niet genoeg? En waarom moet je je fysieke adres opgeven voor een elektronische nieuwsbrief? Allemaal nice to have!
We moeten dus toe naar een situatie dat we minder gaan opvragen en bewaren. En laat dát nu grote voordelen hebben. Niet alleen kom je met minder verzamelen per definitie dichter bij naleving van de AVG. Maar als je minder bewaart, hoef je ook minder (en soms minder streng) te beveiligen. En je houdt zelfs (opslag)ruimte over! Als je geen smartphone naar het strand meeneemt, kan die ook niet gestolen of nat worden. Easy, toch?
Of toch niet zo easy? De smartphone – overigens ook zo'n prachtige bron van interessante informatie voor kwaadwillenden – vinden we écht onmisbaar. Net als data. Maar is dat zo? Moeten we niet gewoon afkicken van onze verzamelverslaving? We kunnen dat misschien maar beter gelijkmatig doen, anders ondergaan we voordat we het doorhebben de 'cold turkey' van de toezichthouder.
Begin dus met een goede inventarisatie van wat je opslaat en waarom. Ga vervolgens aan de slag met dataminimalisatie, opruimen en keuzen maken dus. Maak tegelijk de organisatie bewust van de eisen van de wet en wat van medewerkers zelf wordt gevraagd. Start dus met weinig techniek en veel gedrag! <<

We moeten ons ervan bewust zijn waarom we iets verzamelen en wat we ermee doen

Laszlo Nagy is hoofdredacteur van *Audit Magazine* en director Business Risk Services bij Improven.
Linkedin: https://www.linkedin.com/in/laszlo-nagy-44735a4/