# **PRIVACY:** IEDEREEN HEEFT WAT TE VERBERGEN!

Ieder mens vertelt zijn of haar mening en vindt het belangrijk dat die gezegd kan en mag worden. Hetzelfde zou dan ook voor het recht op privacy moeten gelden. Het is begrijpelijk dat mensen denken 'het zijn alleen maar mijn NAW-gegevens' of 'het is alleen maar een kopie-ID'. Maar als deze gegevens in verkeerde handen komen, kan dit verregaande gevolgen hebben voor deze persoon. Zo kan bijvoorbeeld identiteitsfraude plaatsvinden.

Ondernemingen die persoonsgegevens verwerken hebben te maken met de Algemene verordening gegevensbescherming (AVG). Vaak hebben ondernemingen niet in de gaten wanneer er sprake is van verwerking van persoonsgegevens. Verwerking is: bewerken, opslaan, ordenen, vastleggen, vernietigen, wijzigen, raadplegen of gebruiken van deze persoonsgegevens. Het is dan ook belangrijk dat een onderneming inzichtelijk heeft welke gegevens er gebruikt worden binnen de dienstverlening en met welk doel. Er moet namelijk sprake zijn van een geldige grondslag voor verwerking, zoals:

- Er is toestemming van de betrokkene;
- Het is noodzakelijk voor de uitvoering van een overeenkomst;
- Het is noodzakelijk op grond van de wet;
- Of de bescherming van vitale belangen vereist dat:
- Of het is nodig voor het algemeen belang of voor gerechtvaardigde belangenbehartiging.

Wanneer de verwerking niet gerechtvaardigd is, hebben betrokkenen de mogelijkheid om een aantal rechten te gebruiken. Zij hebben verschillende rechten, namelijk: recht op inzage, het recht op vergetelheid, recht op rectificatie, recht op dataportabiliteit (overdracht van gegevens), recht met betrekking tot geautomatiseerde besluitvorming, recht op bezwaar en het recht op duidelijke informatie. Bijvoorbeeld bij het recht met betrekking tot geautomatiseerde besluitvorming heeft een betrokkene het recht op een 'menselijke tussenkomst'.

De AVG vereist dat gegevens passend worden beveiligd aan de hand van de huidige stand van de techniek. Naast het feit dat deze gegevens beveiligd moeten zijn, is het ook van belang dat een onderneming de vereiste documenten opstelt en deze ook hanteert. Hierbij moet je denken aan een verwerkersovereenkomst, waarin je de doeleinden en beveiliging over de verwerking van gegevens vastlegt.

**Verwerking is bewerken, opslaan, ordenen, vastleggen, vernietigen, wijzigen, raadplegen of gebruiken van persoonsgegevens**

**Verwerking buiten de Europese Economische Ruimte (EER)**

Binnen de financiële dienstverlening worden veel gegevens opgeslagen 'in de cloud'. Dit kan een back-up zijn, maar ook toegang tot een onlineserver. Vaak wordt er gebruikgemaakt van externe partijen, die services aanbieden. Deze externe partijen kunnen zich in Europa bevinden, maar ook in de Verenigde Staten.

Heeft jouw onderneming inzichtelijk wat er met (persoons)gegevens gebeurt? Blijven deze binnen de Europese Economische Ruimte (EER)? Of gaan deze mogelijk naar een derde land zoals China, Verenigde Staten of Rusland? Heb je dan met de partij die de gegevens verwerkt een modelcontract (Standard Contractual Clauses) gesloten? En heeft die partij ook passende waarborgen getroffen?

Er is op het moment veel verwarring over het delen van persoonsgegevens naar de Verenigde Staten. Door de ongeldigverklaring van het Privacy Shield (adequaatheidsbesluit VS, dat is goedgekeurd door de Europese Unie) was het ineens lastiger om op een compliant manier gegevens vanuit de Europese Unie met de Verenigde Staten te delen. In 2022 heeft de Europese Commissie nieuwe stappen gezet door opnieuw in overleg te treden met de Verenigde Staten. Tot op de dag van vandaag is er nog geen nieuw besluit tot stand gekomen.

Hoe kan je als organisatie toch persoonsgegevens delen met een land zoals de Verenigde Staten? Afgezien van de 'normale' eisen waaraan partijen in de EU moeten voldoen, is het noodzakelijk om een modelcontract te sluiten met de partij die zich in het derdeland bevindt. Dit modelcontract is een contract waarin je afspraken maakt over de verwerking van gegevens, maar ook over de beveiliging hiervan. Het is bijvoorbeeld belangrijk om afspraken te maken over het bewaren van gegevens en dat deze voorzien worden van encryptie. Encryptie zorgt ervoor dat gegevens versleuteld worden en dat deze alleen met een sleutel kunnen worden geopend. In bijvoorbeeld de Verenigde Staten is het mogelijk dat inlichtingendiensten toegang kunnen krijgen tot een database waar ook gegevens van Europese burgers instaan. Om deze gegevens te beschermen en te


voldoen aan de eisen van de AVG is het verstandig om ervoor te zorgen dat gegevens (in de cloud) voorzien zijn van encryptie.

**Documenten**

Veel bedrijven hebben een website waarop zij hun diensten of producten aanbieden. Vaak is daar wel iets opgenomen over privacy, maar dit is niet altijd goed zichtbaar op de website geplaatst. Het is belangrijk dat er een privacystatement (ook wel privacyverklaring genoemd) op de website staat. In zo'n privacystatement moet een bedrijf namelijk vermelden of het persoonsgegevens verwerkt en wat men ermee doet. In het privacystatement moet onder andere zijn opgenomen wat de doeleinden zijn voor de verwerking, de bewaartermijn van de gegevens, maar ook de rechten van betrokkenen, zoals het recht op inzage of bezwaar.

Wanneer partijen (verwerkingsverantwoordelijke en verwerker) persoonsgegevens verwerken, moeten zij onderling afspraken maken over de aard, omvang en doel van de verwerking. Zij leggen deze afspraken vast in een verwerkersovereenkomst. In deze verwerkersovereenkomst moet duidelijk worden aangegeven wie de verwerkingsverantwoordelijke en wie de verwerker is. Zo kunnen partijen onderling afspraken maken over de mogelijkheid van het inschakelen van derden, maar ook wat er moet gebeuren in het geval van een datalek of als een betrokkene haar recht van inzage inroept.

**Kun je als organisatie persoonsgegevens delen met een land als de Verenigde Staten?**

In de financiële dienstverlening staan partijen onder toezicht van of de Autoriteit Financiële Markten (AFM) of De Nederlandsche Bank (DNB). Financieel dienstverleners zijn dan ook gehouden aan afspraken tot het meewerken aan audits van toezichthouders. Om hier gehoor aan te kunnen geven, moet er ook in een verwerkersovereenkomst worden opgenomen dat de (derde) verwerker moet meewerken als er een audit plaatsvindt.

**Verwerkingsregister**

Ook bestaat er nog steeds onduidelijkheid over het wel of niet moeten opstellen van een verwerkingsregister. Zo krijg ik regelmatig de opmerking van ondernemers dat zij dit register niet hoeven op te stellen omdat zij minder dan 250 medewerkers in dienst hebben. Het klopt dat er partijen zijn die op grond daarvan geen verwerkingsregister hoeven op te stellen. Alleen geldt dit niet in de financiële dienstverlening. De AVG en de Autoriteit Persoonsgegevens (AP) geven namelijk aan dat er een verwerkingsregister opgesteld moet worden als er sprake is van verwerking van persoonsgegevens wanneer dit vaker gebeurt dan zo af en toe (incidenteel). In de financiële dienstverlening is het noodzakelijk om persoonsgegevens te verwerken, dit gebeurt aan de lopende band. Een verwerkingsregister is dus verplicht. In zo'n verwerkingsregister neem je onder andere de contactgegevens van de onderneming op, maar ook de doeleinden voor de verwerking, om welke persoonsgegevens het gaat, hoelang deze worden bewaard en of er sprake is van verwerking buiten de EER.

**Cookies zijn meer dan tussendoortje**

Mogelijk dat jouw onderneming gebruik maakt van cookies op de website. Het gebruik van cookies is niet verboden, maar je moet bijvoorbeeld wel een cookieverklaring publiceren op je website. De meeste websites gebruiken functionele cookies. Deze zorgen voor een goed werkende website of applicatie. Het kan ook zijn dat de website gebruikmaakt van analytische cookies. Deze verzamelen informatie over het gebruik van de website of applicatie. Als we naar cookies kijken vanuit een AVG-perspectief, zijn de tracking cookies het meest spannend. Tracking cookies kunnen namelijk het surfgedrag van een bezoeker volgen. De interesses van een bezoeker worden vastgesteld en hiermee wordt een profiel opgebouwd (profilering). Deze informatie wordt gebruikt om gerichte advertenties te laten zien aan de bezoeker. Tegenwoordig zijn er partijen, zoals Microsoft, die een patent hebben om mensen emotiegerichte advertenties te tonen. Door middel van een webcam, of het aantal berichten dat iemand op social media plaatst, is af te leiden of iemand gelukkig of mogelijk depressief is. Aan de hand daarvan worden er andere adver- »

tenties getoond.
Als jouw website gebruikmaakt van cookies, dan ben jij verplicht om goed zichtbaar een cookieverklaring op de website te plaatsen. In zo'n cookieverklaring moet onder andere zijn opgenomen welke soort cookies er zijn ingesteld, hoelang deze blijven bestaan op de browser en welke gegevens zij bijhouden en hoe je cookies kunt weigeren. Een cookieverklaring is een document dat de onderneming op de website plaatst. Daarnaast krijg je vaak ook een pop-up te zien met een cookiemelding, waarin je toestemming voor het gebruik van cookies wordt gevraagd.


**Invloed van privacywetgeving in de financiële dienstverlening**
Het is duidelijk merkbaar dat toezichthouders, verzekeraars en de overheid steeds strengere eisen gaan stellen op het gebied van IT, privacy en informatiebeveiliging. Bijvoorbeeld op het uitvoeren van een audit om te beoordelen hoe het is gesteld met de bedrijfsvoering, maar ook of de organisatie voldoet aan wet- en regelgeving, waaronder de privacywetgeving. Met de komst van steeds weer nieuwe wet- en regelgeving is het voor de financieel dienstverlener lastig om alleen nog focus te hebben op de core business.

De AFM heeft in 2019 de *Principes voor informatiebeveiliging* gepubliceerd. In deze principes is aangegeven wat wordt verwacht op het gebied van informatiebeveiliging van ondernemingen die onder toezicht staan van de AFM. De *Principes voor informatiebeveiliging* zijn gebaseerd op verschillende certificeringsmethodieken, zoals Cobit en ISO 27001. Bedrijven die bijvoorbeeld een ISO 27001-certificering hebben behaald, kunnen mogelijk al voldoen aan de eisen van de Principes.

**DORA**
In het eerste kwartaal van 2023 treedt er een nieuwe Europese verordening in werking, ook wel bekend als DORA. DORA staat voor Digital Operational Resilience Act. DORA helpt ondernemingen om hun financiële weerbaarheid te analyseren. Maar zorgt er ook voor dat zij inzichtelijk hebben of zij voldoende weerbaar zijn in geval van ernstige operationele verstoringen.

DORA gaat gelden voor onderneming die meer dan 250 fte in dienst hebben en een omzet van meer dan 50 miljoen euro en/of een balanstotaal groter dan 43 miljoen euro hebben. Dit betekent niet dat DORA voor kleine ondernemingen niet van waarde kan zijn. Zo kan de nieuwe verordening invulling bieden aan een beheerste en integere bedrijfsvoering, met name op het gebied van interne controle en IT-aspecten. De AFM benoemt dit dan ook in het rapport *Marktindrukken 2022*.

**In een verwerkersovereenkomst moet duidelijk zijn aangegeven wie de verwerkingsverantwoordelijke en wie de verwerker is**

**Meer ontwikkelingen**
Naast de nieuwe verordening DORA zien we nog meer ontwikkelingen in de markt op het gebied van privacy. Het UBO-register is niet meer zomaar openbaar toegankelijk en de Uitvoeringswet AVG wordt kritisch onder de loep genomen door het kabinet. We zien ook steeds meer uitingen van de AP. Zo heeft de AP zich uitgelaten over dat de nieuwe witwaswet onrechtmatig is. In deze nieuwe witwaswet wil het kabinet dat banken alle transacties van bedrijven kan monitoren en dat van burgers alle bankbetalingen boven de 100 euro in de gaten gehouden mogen worden. De AP heeft zich ook uitgelaten over de mogelijke nieuwe centrale database met paspoortgegevens. Volgens de toezichthouder is alle gegevens opslaan op één plek een ideale goudmijn voor hackers.

Zo zien we maar dat zelfs na de komst van de AVG privacy en bescherming van persoonsgegevens een hot item is en iedereen hiermee te maken heeft. We zijn gezamenlijk verantwoordelijk voor onze eigen privacy en die van anderen. ●

J.J. (Joyce) Koops
De auteur is compliance- en privacy officer bij SVC Groep B.V. te Amersfoort.

**Bij twijfel over privacy- en informatiebeveiliging**
Mocht een organisatie twijfelen of men alles goed geregeld heeft rondom privacy- en informatiebeveiliging, dan is het verstandig om een privacy- en informatiebeveiligingsaudit uit te laten voeren. Zo weet je wat al op orde is en waar eventueel nog knelpunten zitten. Zo voorkom je in de toekomst boetes en sancties van toezichthouders. En ook weet je dan zeker dat de gegevens binnen de organisatie goed verwerkt worden en veilig zijn.