GENERAL DATA PROTECTION REGULATION: GEVOLGEN VOOR FINANCIËLE INSTELLINGEN

Door Berry van de Bunt

Per 25 mei 2018 treedt de General Data Protection Regulation (GDPR) in werking. De GDPR volgt op de eerste privacywetgeving in de Europese Unie (Directive 95/46/EC). De GDPR is binnen de EU opgezet om de gevolgen van data-ontwikkelingen voor de bescherming van persoonsgegevens te ondervangen. Dit artikel geeft een beknopt overzicht van de bredere regelgeving ten aanzien van data en de eisen die de GDPR stelt aan financiële instellingen.

DATA-ONTWIKKELINGEN EN REGULERING

In de jaren na de eerste privacyregelgeving zorgden IT-ontwikkelingen voor een groeiende economische waarde van de persoons-gegevens in de systemen bij organisaties. Daarnaast waren er technologische ontwikkelingen rondom social media en binnen het applicatielandschap. Systemen gingen in organisaties van lokale installaties van software naar 'software as a service' in de cloud (ook wel 'hosted solutions' genoemd).

Figuur 1 geeft een aantal ontwikkelingen weer en de reactie hierop van de regelgever.


Foto: Archief Berry van de Bunt

Berry van de Bunt

Zoals zichtbaar in Figuur 1 is er regelgeving gekomen om de transparantie van de processen van financiële instellingen te verbeteren. Met als doel om meer inzicht te krijgen in de risico's in de markten (Trade reporting vanuit Dodd Frank Act en EMIR) en inzicht te krijgen in de manier waarop financiële instellingen de belangen van de klant behartigen (pre- en post trade transparency in MiFID II).

Deze regelgeving ziet alleen niet toe op de bescherming van directe persoonlijke gegevens van klanten, maar richt zich primair op transactiedata. De GDPR vult de bestaande regelgeving aan voor de bescherming van persoonsgegevens met inachtneming van de bovengenoemde ontwikkelingen. Hieronder worden beknopt de veranderingen toegelicht die de GDPR met zich meebrengt voor financiële instellingen.

GENERAL DATA PROTECTION REGULATION: VERANDERINGEN

De GDPR kent een aantal belangrijke veranderingen ten aanzien van de eerste privacywetgeving. Deze betreffen onder andere het verruimde toepassingsgebied, de verruimde rechten van het 'data subject' (natuurlijke persoon wiens persoonlijke gegevens worden verwerkt door een controller of verwerker), de beveiliging van data en de sancties die mogelijk zijn wanneer een organisatie niet voldoet aan de regels van de GDPR.

TOEPASSINGSGEBIED

De regelgeving is van toepassing op de verwerking van persoonsgegevens door controllers (organisatie die het doel, de voorwaarden en de manieren van het verwerken van de data bepaalt) en verwerkers (organisatie die data verwerkt namens de controller) in de Europese Unie, ongeacht of de daadwerkelijke verwerking van die data in de EU plaatsvindt. Ook is de regelgeving van toepassing indien diensten of goederen worden aangeboden aan inwoners van de Europese Unie, ongeacht of het land van vestiging in de EU ligt.

RECHTEN VOOR HET DATA SUBJECT

De GDPR heeft voor data subjects de rechten verruimd betreffende het recht om informatie te krijgen over de verwerking van data van het subject, het recht van rectificatie en het recht om gegevens te laten wissen ('right to be forgotten').

Organisaties dienen plannen te hebben waaruit blijkt dat een omgeving wordt gecreëerd waarbinnen data subjects bovenstaande rechten kunnen uitoefenen.

VERPLICHTING TOT BEVEILIGINGSMAATREGELEN

De GDPR verplicht tot het nemen van beveiligingsmaatregelen om de veiligheid van de verzamelde persoonsgegevens te waarborgen.

De GDPR schrijft geen specifieke verplichte maatregelen voor, maar verplicht organisaties om deze zelf te bepalen, afhankelijk van de aanwezige data, de gevoeligheid hiervan en de relevante processen en schrijft voor: 'Het waarborgen van een passend beveiligingsniveau, waarbij rekening dient te worden gehouden met de stand van de techniek en met de kosten van de uitvoering van de maatregelen.'

Een belangrijke gerelateerde verplichting is om binnen 72 uur melding te maken van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en daarna zonder onnodige vertraging aan de betrokkene.

AANSTELLEN VAN EEN DATA PROTECTION OFFICER (DPO)

Afhankelijk van de hoeveelheid en typen data die worden verwerkt, dient een functionaris voor gegevensverwerking te worden aangewezen binnen de organisatie. Deze DPO dient kennis te hebben van databeveiliging en de betreffende wetgeving. Contactgegevens van de DPO dienen bekend te zijn bij de toezichthouder.

SANCTIES

De nieuwe regelgeving kent significante boetes: maximaal 4% van de jaarlijkse omzet of 20 miljoen euro (hoogste bedrag). De sancties kennen staffels afhankelijk van de ernst van de inbreuk op de regulering. De sancties zijn daarbij van toepassing op zowel controllers als verwerkers, waarmee data binnen hosted/cloud applicaties ook binnen het toepassingsgebied vallen.

Ook kunnen data subjects schadeclaims indienen inzake tekortkomingen in de bescherming van hun gegevens.

AANBEVELING

Met de nieuwe GDPR maakt de regelgever een inhaalslag op het gebied van de bescherming van persoonsgegevens. Financiële instellingen hebben bij het inrichten van dit proces baat bij de IT- beveiligingsmaatregelen die zij reeds vanuit procesgerichte regelgeving hebben moeten nemen.

Toch zorgen de relatief grote veranderingen ervoor dat er veel geregeld moet worden door organisaties, waaronder de financiële instellingen. Zeker omdat niet alleen technische aanpassingen, maar ook het opstellen van documentatie en communicatie inzake de verwerking van de persoonsgegevens richting het data subject en de toezichthouder noodzakelijk zijn om te voldoen aan de regels van de GDPR.

De significante sancties maken het zeer wenselijk om tijdig alle benodigde stappen te nemen om te voldoen aan de GDPR op 25 mei 2018. «

Figuur 1: Technologische ontwikkelingen en bijbehorende reacties van de regelgever

TYPE DATA	ONTWIKKELINGEN	REGULERING
- Transactiedata	STP Outsourcing/SAAS/Cloud Robotics	- Dodd Frank Act/EMIR - MiFID/MiFIR - Cloud Risk Assessment - CRA (DNB) - CSP (SWIFT)
- Persoonsgegevens	E-commerce Big Data	- Privacy Directive - 1995 - GDPR - 2018

Dit artikel is geschreven door Berry van de Bunt, Associate bij Lijn3 Management-consulting en eigenaar van BEBUNT Consultancy.

Definities en hoofdbeginselen

De nieuwe GDPR Regulation start in artikel 4 met definities over wat moet worden verstaan onder persoonsgegevens, onder een controller en onder een verwerker.

De invloed van nieuwe technologische ontwikkelingen is zichtbaar in het feit dat social media posts, cookies en een IP-adres ook worden benoemd als persoonsgegevens.
De definitie is verder zo breed dat zelfs gegevens onder de noemer 'persoonsgegevens' vallen die niet persoonlijk lijken. Zoals een foto zonder personen, waarbij deze gelinkt is door een unieke code of nummer aan een identificeerbaar persoon. Zelfs geanonimiseerde data die gelinkt kunnen worden aan een identificeerbaar natuurlijk persoon vallen eronder.

Vervolgens worden in artikel 5 van de GDPR de zes hoofdbeginselen benoemd inzake de verwerking van persoonsgegevens. De hoofdbeginselen hebben betrekking op hoe data dienen te worden verwerkt en voor welke doeleinden. De data en de verwerking ervan dienen in verhouding te staan tot het doel.

De GDPR benoemt nog een aantal andere verantwoordelijkheden voor organisaties, zoals:
- Het bewaren van documentatie inzake alle verwerkingssystemen en procedures onder verantwoordelijkheid van de verantwoordelijke en van de verwerker.
- Voldoen aan de eisen van databeveiliging.

Daarnaast worden eisen aan de IT gesteld:
- Privacy by design: bepaalt dat privacybescherming onderdeel moet zijn van het ontwerp van het systeemdesign, de producten en de services.
- Privacy by default: implementeren van maatregelen die verzekeren dat by default niet meer data worden verwerkt dan noodzakelijk is.