Position paper

Nieuwe privacywet doet belang data governance toenemen

Matthias Geerse

Jeroen Kriele

maart 2017

solid professionals

Advisory | Interim | Recruitment

Nieuwe privacywet doet belang data governance toenemen

Door de recente invoering van de nieuwe EU wet Algemene Verordening Gegevensbescherming (AVG) moeten organisaties aan strengere regels gaan voldoen op het gebied van privacy. Het spanningsveld tussen het al dan niet noodzakelijk verzamelen van allerlei gegevens over de klant versus het vergemakkelijken van de dienstverlening neemt hierdoor toe. Hoe krijg je voldoende grip op je klant bij verdere digitalisering van het klantcontact en zorg je er tevens voor dat privacy geen struikelblok wordt?

Hieronder maken we eerst een korte uitstap naar het huidige wettelijke kader, de nieuwe wet en de verwachte impact, waarna het gebruik van (persoons)gegevens binnen de financiële sector in context wordt geplaatst. Het artikel eindigt met een uitdaging voor banken en verzekeraars.

Wet Bescherming Persoonsgegevens

De Wet bescherming persoonsgegevens (in het kort: Wbp) is de Nederlandse uitwerking van de Europese Privacyrichtlijn uit 1995[1]. Uitgangspunt van die wet is het minimale gebruik van persoonlijke gegevens waardoor de kans op inbreuk op privacyregels vooraf zo klein mogelijk wordt gemaakt. Door de opkomst van internet en verdere digitalisering van producten en diensten was deze richtlijn dringend aan vernieuwing toe. Verder heeft het gebruik van big data voor (interne) marketingdoeleinden en –instrumenten, zoals profiling, recent een enorme vlucht genomen.[2] In welke mate er op basis van deze gegevens wordt voorspeld, ingedeeld (bucketing) en geïnterpreteerd, bepaalt mede de uitdagingen op het vlak van privacy en het geoorloofd gebruik van persoonsgegevens. Parallel hieraan speelt het spanningsveld tussen enerzijds customer convenience (snelheid en gemak) en anderzijds compliance (ofwel juistheid, volledigheid en tijdigheid van verstrekte gegevens).

Nieuw wettelijk kader: Wat gaat er veranderen?

In mei 2016 is de AVG in werking getreden. Handhaving zal plaats gaan vinden per 25 mei 2018. Op die datum zal ook de hiervoor

1 *Richtlijn 95/46/EG*

2 *Transparantie op het gebied van profiling vormt een key thema in het toezicht uitgevoerd door de Autoriteit Persoonsgegevens voor 2017.*

aangehaalde Wbp vervallen. De AVG is zonder doorvertaling naar landelijke wetgeving direct van toepassing in de hele Europese Unie. Maar ook daarbuiten. De werkingssfeer reikt tot alle organisaties die persoonlijke gegevens van EU ingezetenen verwerken, ongeacht de locatie van de onderneming of instelling. Hiermee is zowel de uitwerking als de impact van deze wet concreter en veelomvattender dan die van de richtlijn.
Deze nieuwe EU wet schrijft voor onder welke strikte voorwaarden persoonlijke informatie mag worden verzameld, verwerkt en bewaard. Het overgrote deel van de AVG heeft overigens betrekking op bepalingen die in meer of mindere mate reeds werden geraakt door de Wbp. Zo blijft het opstellen en bijhouden van een register met persoonsgegevens verwerkende activiteiten gehandhaafd. Daarentegen wordt het aanstellen van een privacy officer in bepaalde gevallen wel verplicht gesteld, worden de principes privacy by design/ & default geïntroduceerd en worden privacy impact assessments (PIA) in bepaalde gevallen als norm gesteld. Het maximale boetebedrag wordt tot maximaal 20 miljoen Euro verhoogd (of 4% van de wereldwijde jaaromzet). Al met al zal de impact dus groot zijn, en dan met name omdat organisaties aantoonbaar in control moeten zijn én blijven.

Het gebruik van persoonsgegevens

Een persoonsgegeven is elk gegeven dat in relatie kan worden gebracht met een geïdentificeerde of identificeerbare natuurlijke persoon. Dit wil zeggen dat aan de hand van persoonsgegevens zonder veel inspanning een natuurlijk persoon kan worden geïdentificeerd. Gegevens van een overleden persoon vallen niet onder persoonsgegevens. Voorbeelden: naam, adres en woonplaats, maar denk ook aan emailadressen, pasfoto's en iemands IQ. Naast persoonsgegevens wordt onderscheid gemaakt naar bijzondere persoonsgegevens. Dit zijn gegevens die iemands privacy ernstig kan aantasten. Deze gegevens mogen dan ook alleen onder zeer strenge voorwaarden worden verwerkt. Voorbeelden van deze bijzondere persoonsgegevens zijn gezondheid, geloofsovertuiging, politieke voorkeur, ras en Burgerservicenummer.
Banken en verzekeraars verwerken op grote schaal (bijzondere) persoonsgegevens en overige privacygevoelige gegevens (denk hierbij aan betaalgegevens). Om tot een gedegen risicobeeld van een klant te komen, worden er (bijzondere) persoonsgegevens gebruikt.
In het kader van Know Your Customer (KYC) moet iedere klant zich kunnen identificeren. Banken en verzekeraars zijn daarnaast wettelijk verplicht het Burgerservicenummer (BSN) van hun klanten te gebruiken om gegevens met de Belastingdienst uit te wisselen.
Gezondheidsgegevens spelen een rol bij het aanvragen van arbeidsongeschiktheids- en levensverzekeringen.
De verkregen persoonsgegevens moeten zoveel mogelijk transparant en het liefst geautomatiseerd worden verwerkt. Dit is echter niet altijd het geval.

Data lineage wordt nog belangrijker

Waar ontstaat data en wie kan deze gegevens, op welke grond en op welke momenten aanpassen voordat informatie ontstaat en besluitvorming plaatsvindt? Is er een duidelijke golden source en waar worden de gegevens en afgeleide informatie opgeslagen? Banken worstelen nog steeds met data lineage en data kwaliteit. Data lineage, ook wel data life cycle genoemd, beschrijft wat er met data gebeurt van ontstaan tot gebruik. Toezichthouders verlangen intussen een gedegen beheersing ervan in de keten en een gezonde verhouding tussen geautomatiseerde en handmatige verwerking van gegevens. Naast AQR, AnaCredit en de noodzaak tot verdere alignment tussen Finance en Risk terminologie (e.g. IFRS 9) vormt nu ook AVG een trigger om oorsprong, verwerking, rapportage en opslag van gegevens strak neer te zetten.
De AVG geeft klanten straks ook het recht om vergeten te worden of gegevens aan te laten passen. Voorheen lag vooral de focus op zoekmachines – met de inwerkingtreding van de AVG kunnen we verwachten dat bedrijven die persoonsgegevens verwerken er hier een extra last bij krijgen.
Om de gevraagde klantgegevens uit alle databases te verwijderen moet een organisatie zorgen dat ze goede grip hebben op hun data lineage: van de bron tot aan de gebruiker.

Uitdaging van formaat

Op het moment dat wetgeving en beheersing van (persoons)gegevens belangrijker wordt, is het valide om stil te staan bij nut en noodzaak van deze gegevens, zeker gezien de te verwachten kosten van de interne beheersing ervan. Dit past ook in het "privacy by design" principe van de AVG. Waar wordt gebruik gemaakt van gevoelige klantgegevens en waarom hebben we ze nodig? In welke mate voedt dit marketing, compliance en acceptatie-afdelingen en worden er vervolgens beslissingen genomen op basis van privacygevoelige gegevens? Deze processen dienen helder te zijn om vervolgens tot eventuele aanpassingen te komen voordat maatregelen worden gedefinieerd om AVG compliant te worden.
Voor veel organisaties betekent dit een uitdaging van formaat. Nog niet alle banken zijn optimaal "in control". Het AVG zal als een vergrootglas werken en zal een volledige "in control" verlangen van privacygevoelige data. Dit betekent dus dat organisaties naast AVG compliance op hoofdlijnen ook een stapje verder moeten met data governance en data lineage.

Matthias Geerse *is bedrijfskundige en Managing Consultant bij Solid Professionals | Advisory. Hij heeft ruim 12 jaar consultancy ervaring binnen de financiële sector. Governance, Risk en Compliance hebben zijn aandacht. Hij heeft ervaring met het begeleiden van verandering op het gebied van risk management, analyse van internationale rapportagestromen en het implementeren van risico control raamwerken.*

Jeroen Kriele *is bedrijfseconoom en werkzaam als Principal Consultant bij Solid Professionals | Advisory. Hij is een ervaren project manager op het gebied van datakwaliteit/data lineage, risk management en business intelligence. Hij was betrokken bij verschillende projecten bij zowel banken als verzekeraars.*