Data is het nieuwe goud voor bedrijven geworden

Er liggen zo vaak persoonsgegevens op straat, dat je je af kunt vragen of het beschermen van je privacy een achterhoedegevecht is. Er zijn wel regels voor, maar er is ook zowel verouderde als voortschrijdende technologie, die allebei op hun eigen manier het handhaven lastig kunnen maken. Vanaf 25 mei 2018 dienen bedrijven en overheids-instanties persoonsgegevens te verwerken conform de beginselen en bepalingen van de Algemene Verordening Gegevensbescherming (AVG). Dit is een Europese wet met als doel de bescherming van privacyrechten van mensen van wie persoonsgegevens worden gebruikt. De wet geldt voor alle landen in Europa. Esther Bliek en Judith van de Vorle vertellen ons meer over de ideeën achter de verordening en de gevolgen voor de werkzaamheden van de Business Analist.

door Reinoud de Leve en Hans Siebering

Bescherming

De AVG beschermt ons tegen oneigenlijk gebruik van persoonsgegevens. Het is een stap geweest in een lange geschiedenis van wetgeving, die in 1948 begonnen is met de Universele Verklaring van de Rechten van de Mens. Na de Tweede Wereldoorlog realiseerde men zich dat bijvoorbeeld de registratie van het feit dat iemand jood is heel desastreuze gevolgen heeft gehad. Daar wilde men in de toekomst voorzichtiger mee zijn. In de decennia daarna maakte de opkomst van de informatietechnologie het mogelijk grote hoeveelheden gegevens met elkaar te combineren en zo bijvoorbeeld gericht producten aan te bieden: data is het nieuwe goud voor bedrijven geworden.

Daarom is het van belang is dat je als burger

Esther Bliek en Judith van de Vorle over de AVG

zeggenschap hebt over je eigen persoonsgegevens. Je moet zelf invloed kunnen uitoefenen op welke gegevens men van je heeft en op wat men ermee doet. Dat heeft eerst geleid tot een Europese richtlijn, met ruimte voor elk land om op zijn eigen manier hieraan invulling te geven. Dit leidde vanaf 1995 tot verschillen in de nationale privacywetgeving in de Europese landen en hiermee tot onduidelijkheid. Daarom is er een harmonisatietraject opgestart dat ertoe heeft geleid dat in 2016 de AVG is aangenomen. Met een periode van twee jaar om deze te implementeren. Vanaf 25 mei 2018 wordt deze verordening gehandhaafd.

De verordening geldt ook voor bedrijven van buiten de EU, die producten en diensten aanbieden aan EU-burgers. Daardoor heeft de AVG in de praktijk een *global scope*.

Global scope

Met de AVG is wetgeving binnen de verschillende Europese lidstaten geharmoniseerd, waardoor zakendoen binnen de EU eenvoudiger is gemaakt. De verordening geldt ook voor bedrijven van buiten de EU, die producten en diensten aanbieden aan EU-burgers. Daardoor heeft de AVG in de praktijk een ***global scope***. Het is knap werk dat dat gelukt is, maar het is ook wel nodig, omdat bedrijven als Facebook, Google Amazon en Uber anders altijd mogelijkheden zullen vinden om zich eraan te onttrekken.

Judith van de Vorle CIPPE

Judith is een ervaren business analist met veel ervaring binnen de overheid (uitvoeringsorganisaties, Rijksoverheid, Provincie). Sinds 2017 heeft zij zich verdiept in het onderwerp privacy. De combinatie van analytische vaardigheden en de kennis van de AVG maakt dat zij gemakkelijk de verbinding kunnen leggen tussen legal, business en IT. Resultaat staat bij haar voorop, ook wanneer de omgeving uitdagend is. Op dit moment adviseert zij enkele vrijwilligersorganisaties omtrent privacy aangelegenheden (waaronder het Dream event) en probeert zij 'privacy by design' op het netvlies te krijgen van de scrumteams bij haar huidige opdrachtgever.

Mr. Esther Bliek CIPPE CIPM CIPT FIP

Esther is een ervaren Privacy Expert met een bewezen trackrecord in de consulting branche. Zij is een professional met stevige change management ervaring opgedaan binnen zowel de overheid als het bedrijfsleven, gecertificeerd op het gebied van Privacy Compliance: legal content (CIPPE), Privacy Program Management (CIPM) en Privacy IT (CIPT). Als lid van de International Assocation of Privacy Professionals beschikt zij altijd over de meest actuele kennis en ontwikkelingen op het gebied van Privacy Compliance. Esther geeft geregeld certificeringstrainingen via opleidingscentrum TSTC en is verbonden als docent aan USG Legal voor de, door haar ontwikkelde, leergang The Privacy Compliance Experience en The Privacy Compliance Experience on the move (intervisiesessies). Zij is Associate Cybersecurity & Privacy bij VKA. Esther is spreker op DREAM19.

Impact van de AVG

De grootste verandering met de komst van de AVG is dat bedrijven die persoonsgegevens gebruiken aantoonbaar gedocumenteerd moeten kunnen duiden wat ze met persoonsgegevens doen, voor welk doel, met wie deze worden gedeeld, waarom en hoe lang ze deze bewaren, hoe deze worden beschermd, waar de persoonsgegevens zich bevinden, welke privacyrisico's aan de verwerking verbonden zijn en hoe deze zullen worden gemitigeerd. Voor elke stap in de *Data Life Cycle* van verzamelen, gebruik, verspreiden, opslaan en vernietigen, dienen organisaties na te denken over de bescherming van de privacyrechten van degene die het betreft. Elk initiatief dat een organisatie wil opstarten waarbij sprake is van verwerking van persoonsgegevens dient bekeken te worden op privacyrisico's en hoe deze te mitigeren, dit noemt men ook wel *Privacy by Design*.

Information security versus privacy

Security en privacy worden nog wel eens onder één noemer geplaatst, maar het zijn verschillende vakgebieden. Information security kijkt naar de beveiliging van het systeem, ongeacht de gegevens die erin worden verwerkt. Privacy kijkt juist naar de verwerking van persoonsgegevens in het systeem.

Benodigde vaardigheden

Als business analist heb je uiteenlopende competenties nodig. Vaak word je gezien als 'het schaap met de 5 poten'. Daar komt nu het aspect van *Privacy by Design*

bij. Hoewel deze kennis niet primair bij de business analist zal liggen, maar veelal bij *Legal*, *Audit* en *Compliance* afdelingen, is het nuttig als je basiskennis hebt van de wettelijke bepalingen en beginselen van de AVG. Het spreekt voor zich dat in grote organisaties veelal een specifieke afdeling zich met privacy (en meestal ook security) bezighoudt. Echter, als business analist ben je vaak betrokken bij de ontwikkeling van nieuwe functionaliteiten en wijzigingen in applicaties en dan is het nuttig als je weet wat een *PIA*, *Verwerkingsregister* en *Privacy by Design* is en hier een bijdrage aan kan leveren.

De AVG is meer dan alleen juridisch van aard. Het raakt de hele organisatie. Niet voor niets zijn er drie opleidingen om kennis op te doen: uitleg van de wet (CIPP/E(uropa), de techniek (CIPT) en programma management (CIPM).

De rol van de business analist

Sinds de invoering van de AVG is *Privacy by Design* (zie kader) verplicht. Bij de realisatie hiervan kan een business analist zeker een rol vervullen. Bijvoorbeeld om ervoor te zorgen dat de gegevens zodanig georganiseerd worden dat het geen dagenlang werk kost om aan een inzageverzoek te voldoen. In de softwaredesign cycle is de inzet van een business analist waardevol. Denk hierbij aan de fase van requirements engineering waarin de legal AVG requirements verzameld moeten worden. Ook bij de vertaling van de requirements naar de design fase is de inzet van business analisten van toegevoegde waarde.

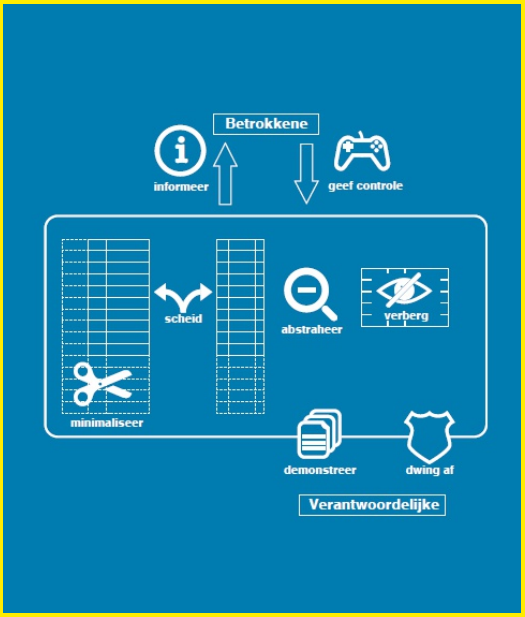
In het kader worden acht ontwerpstrategieën genoemd om tot een goede bescherming van persoonsgegevens te komen. Het is belangrijk je niet te beperken tot één van die strategieën. Ze zijn geschikt om naast elkaar te gebruiken. Bovendien mag het toepassen van de strategieën mag zich niet beperken tot alleen de fase systeemontwikkeling. Ze komen kijken in alle fasen vanaf de conceptie tot en met de ontmanteling.

Wanneer de verwerking van persoonsgegevens een hoog risico op kan leveren voor degenen van wie de gegevens verwerkt worden, is het verplicht om een *Privacy Impact Assessment (PIA)*, ook wel Gegevensbeschermingseffectbeoordeling genoemd, uit te voeren. Dit is een instrument, waarmee je privacyrisico's in kaart kunt brengen. Een business analist zou een rol kunnen spelen bij het opstellen van de privacyrisico's en de te treffen mitigerende maatregelen. Daarnaast kan een business analist ook helpen bij het opstellen van het Verwerkingsregister. Dat is een verplicht op te leveren verantwoordingsinstrument, waarin alle verwerkte gegevens (een kopie maken van een ID valt daar onder) zijn opgenomen. Om dit inzichtelijk te maken dient een organisatie de werkprocessen, systemen, verwerkers en stakeholders te inventariseren. Het is nog niet uitgekristalliseerd welke rollen bij welke activiteiten betrokken zullen worden, maar er zijn zeker kansen voor analisten.

Privacy by Design is sinds de invoering van de AVG wettelijk verplicht. *Privacy by Design* is er op twee niveaus: data en proces. Jaap-Henk Hoepman heeft hierover een handzaam boekje (https://www.deprivacycoach.nl) geschreven, waarin hij acht *privacyontwerpstrategieën* beschrijft.

Vier daarvan zijn ***data*** georiënteerd en dus technisch van aard:

- **Minimaliseer**: Beperk zo veel mogelijk de verwerking van persoonsgegevens.
- **Scheid**: Scheid de verwerking van persoonsgegevens zo veel mogelijk van elkaar.
- **Abstraheer**: Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.
- **Verberg**: Bescherm persoonsgegevens, of maak ze onherleidbaar of onobserveerbaar. Voorkom dat persoonsgegevens openbaar worden.



De andere vier zijn ***proces*** georiënteerd en dus organisatorisch en procedureel van aard:

- **Informeer**: Informeer gebruikers over de verwerking van hun persoonsgegevens.
- **Geef controle**: Geef gebruikers controle over de verwerking van hun persoonsgegevens.
- **Demonstreer**: Toon aan dat je op een privacy vriendelijke wijze persoonsgegevens verwerkt.
- **Dwing af**: Committeer je aan een privacy vriendelijke verwerking van persoonsgegevens, en dwing deze af.

Privacy by Default is een term die in dit verband ook vaak gebruikt wordt en maakt onderdeel uit van *Privacy by Design*. Deze houdt in dat systemen *'privacyvriendelijk'* ingericht zijn. Het betekent dat je bij voorkeur géén persoonsgegevens registreert en als je toch iets móét registreren, het zo snel mogelijk weer verwijdert of alleen nog maar op geaggregeerd niveau bewaart. De herleidbaarheid tot personen moet tot het noodzakelijke beperkt worden.