Inleiding

Het was medio 2013 dat de Europese Commissie een draft publiceerde van de General Data Protection Regulation (GDPR). Deze verordening moet zorgen voor een geharmoniseerde wetgeving rond persoonsgegevens en het beschermen van data. In de huidige situatie heeft iedere EU lidstaat zijn eigen regels en is de EU richtlijn uit 1995 verouderd en weinig dwingend. De reden voor deze nieuwe wet werd veroorzaakt door vele, ernstige incidenten waarbij grote hoeveelheden privacygevoelige data op straat kwam te liggen.

Een medewerker van een grote telecomprovider in Nederlands is een onversleutelde laptop kwijtgeraakt met persoonlijke gegevens van ruim 40 duizend klanten die contact hadden gehad met de helpdesk. Op de gestolen laptop stonden klantnummers, namen, mailadressen, postcodes, geslacht en de laatste vier cijfers van het bankrekeningnummer. Ook het onderwerp van het helpdesk gesprek stond vermeld.

Deze General Data Protection Regulation vereist dat een bedrijf of organisatie aantoonbaar moet voldoen aan de wet- en regelgeving rondom privacy. “Dat betekent dat het niet alleen juridisch moet zijn geregeld, maar ook dat de IT omgeving er naar ingericht is én hiernaar moet werken. Om dat te realiseren is het noodzakelijk dat men maatregelen op bedrijfsniveau maar ook op IT niveau moet nemen.

De invoering van deze wet moet bij de burger leiden tot een herstel van het vertrouwen dat hun data op een veilige en voor overheden controleerbare manier wordt beheerd en verwerkt. Op 12 maart 2014 hield het Europees Parlement een plenaire stemming rond de GDPR. Deze GDPR was op commissie niveau al goedgekeurd, maar nu, met grote meerderheid, door het voltallige parlement. Er zijn nu enkele amendementen die moeten worden doorgevoerd maar algemeen wordt aangenomen dat uiterlijk in 2015 de nieuwe verordening officieel bekrachtigd worden zal worden en dat deze rond 1-1-2016 in werking treedt.

Privacy by Design

Invoering van de GDPR heeft voor veel bedrijven ingrijpende gevolgen. Het is daarom niet verassend dat Forbes heel recent heeft duidelijk gemaakt dat het "Privacy by design principe" het heetste hangijzer voor veel bedrijven zal worden. Hieronder de belangrijkste punten en verschillen met de huidige EU richtlijn van 1995:

- De GDPR is een **verordening** en geen richtlijn zoals die van 1995, oftewel een Europese wet i.p.v. een doelstelling die in alle 27 lidstaten als wetgeving geldt wanneer de GDPR op Europees niveau wordt geratificeerd.
- Data Protecion Officers (DPO's) verplicht voor bedrijven met meer dan 250 medewerkers (In de laatste wijziging van de GDPR is de grootte van het bedrijf niet meer relevant maar de hoeveelheid verwerkingen).
- Boetes tot **5%** van de wereldwijde omzet bij overtredingen met een maximum van 100 miljoen euro.
- Uniformiteit van aangiftes: één Data Protection Authority (In Nederland het CBP) uit het land van aangifte is de leidende instantie voor een Europese aangifte.
- Europese aansturing van DPA's vanuit de European Data Protection Board

Door een beveiligingslek in het computerprogramma Humannet van IT-bedrijf VCD zijn medische en persoonlijke gegevens van meer dan 300.000 werknemers maandenlang toegankelijk geweest voor onbevoegden. In Humannet staan onder meer medische dossiers van bedrijfsartsen. Het zou gaan om het grootste lek van persoonlijke en medische data in de Nederlandse geschiedenis. De gegevens van werknemers van honderden bedrijven en arbodiensten staan in het systeem. Onder de bedrijven zijn FC Twente, de gemeente Deventer, Praxis, Bijenkorf en V&D

Bekijkt men de GDPR vanuit het beheer van deze gegevens dan zijn dit de belangrijkste punten:

- Right to erasure : Bedrijven en dienstverleners zijn verplicht op verzoek van een data subject (Lees natuurlijk persoon) al zijn of haar persoonlijke data te verwijderen. Dit is ook van toepassing op persoonsgegevens die via de oorspronkelijke verwerker bij derden terecht zijn gekomen
- Toestemming is specifiek gericht op het doel van verwerking van persoonsgegevens, wijzigt het doel dan vervalt de toestemming
- De toestemming dient bewezen te kunnen worden door de verwerker en moet eenvoudig ingetrokken kunnen worden
- De vastlegging van het Privacy by Design (Privacy by Design gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over het goede gebruik van persoonsgegevens binnen een organisatie, de noodzaak van het gebruik van deze gegevens en de bescherming ervan). principe en de verplichte uitvoering van Privacy Impact Assessments (PIA).
- Data portability: een data subject moet in staat zijn om zijn persoonlijke data op te vragen en te kopiëren op een manier die bruikbare data oplevert is voor het data subject
- Pseudonieme data zijn nu opgenomen als een aparte definitie, maar zijn en blijven persoonsgegevens in tegenstelling tot richtlijn van 1995.

Het is dus van belang om al bij het ontwerpen van nieuwe producten, informatiesystemen , databanken na te denken over het waarborgen van privacy gevoelige gegevens en deze afdoende te beschermen tegen reële bedreigingen en risico's (Privacy by Design). Het is vanuit de GDPR vereist dat dit men dit ook het principe van Privacy by Design hanteert.

Indien men een nieuw informatiesysteem ontwikkelt is het eenvoudig om tijdens het design rekening te houden met bestaande regelgevingen. Veel lastiger is om bestaande informatie systemen of producten dusdanig aan te passen dat deze voldoen aan de GDPR.

Opslag is niet het probleem. Met een prijs van minder dan 10 eurocent per gigabyte is uitbreiding van de opslagcapaciteit goedkoop. De grootste uitdaging zit hem echter in de ongestructureerde data. Ongestructureerde data is alles wat we opslaan in files: documenten, spreadsheets, video, voice en images / foto's. Vaak is deze data verspreid over verschillende fileservers, NAS (Network Attached Storage) devices, werkplekken, smartphones, tablets, the cloud etc. Uit diverse onderzoeken blijkt dat slechts 15 tot 20% van bedrijfsdata gestructureerd is. De overige is dus semi-gestructureerd (bijv. e-mail) of volledig ongestructureerd.

Met de wetenschap dat de hoeveelheid data iedere 2 jaar verdubbelt (Gartner & IDC) is dit dus een extra grote uitdaging. Echter welke informatie deze ongestructureerde data bevat is in de meeste gevallen slechts bekend bij een data-owner of men weet het gewoonweg niet meer. In tegenstelling tot gestructureerde data, welke over het algemeen goed geordend en beveiligd is levert ongestructureerde data dus veel meer risico's.

Welke informatie bevat deze data? Aan welke regelgeving dient deze data te voldoen? Bevat deze data privacygevoelige gegevens? Het is dus vanuit bedrijfsoptiek belangrijk om duidelijkheid te krijgen waar privacygevoelige gegevens zijn opgeslagen.
De GDPR vereist zelfs dat men dit inzicht heeft.

Big Data

Big Data is een ander gevaar. Steeds meer bedrijven willen correlaties ontdekken die tot nu toe onbekend zijn. Ze willen op ontdekkingstocht, in plaats van zoektocht. Ze willen ongestructureerde data gebruiken om nieuwe patronen, verbanden en concepten te ontdekken.

Een vraag die men dan als bedrijf moet stellen: Wat mogen wij wel met deze data en wat niet? M.a.w. aan welke regelgeving zijn wij gebonden? Welke risico's zijn er aan gebonden met dergelijke data?

Duidelijk inzicht welke risico's er zijn kunnen van bedrijfsbelang zijn. Immers, als men goed inzicht heeft welke risico's er zijn dan kan men als verantwoord bepalen welk risico men wilt nemen.

Het is dus belangrijk dat je als bedrijf je goed verdiept in privacy compliance. Niet alleen ter voorkoming van boetes, maar vooral ook voor het behoud van klantvertrouwen, het voorkomen van een negatief bedrijfsimago en in geval van overheidsinstanties maar ook ander publieke organisaties verlies van het maatschappelijke vertrouwen. Als bedrijf of organisatie moet men de vraag stellen: Heeft men als bedrijf of organisatie duidelijk inzicht waar welke data staat dan wordt ook duidelijk waar mogelijke risico's liggen.

Als de risico's inzake privacy goed in kaart zijn gebracht, liefst visueel, is het voor iedereen binnen het bedrijf helder welke risico's er zijn. Een voorbeeld is het recht van inzage op eigen persoonsgegevens, dat ieder mens heeft. Het is een sterk recht waar over het algemeen nog weinig gebruik van wordt gemaakt in ons land. "Als een bedrijf of organisatie een verzoek tot inzage van de eigen persoonsgegevens is dat meestal geen probleem. Zijn het er tientallen per week, dan loopt een bedrijf daar een operationeel risico mee. Het kost capaciteit en geld om snel en doeltreffend aan zoveel verzoeken te voldoen. Het is van bedrijfsbelang dat systemen en processen moeten daarop ingericht worden.

Door een gericht onderzoek van IO4U kan een organisatie erachter komen of ze hun IT-omgeving beter zouden moeten inrichten. Zijn we als bedrijf goed beschermd tegen cybercriminaliteit? Zijn er risico's inzake data leakage?

Recent onderzoek door Iron Mountain heeft bijvoorbeeld aangetoond dat maar liefst 51% van de werknemers aan de haal gaat met informatie van de werkgever bij vertrek. Het gaat dan om presentaties, vakinformatie maar ook vertrouwelijke informatie zoals offertes, klantenbestanden en proposals.

Waar heeft een bedrijf zijn gegevens opgeslagen. Zijn er gegevens opgeslagen bij third-party? En zijn daar privacy gevoelige gegevens bij betrokken? Hoe veilig is als we dergelijke data in de cloud opslaan?

Inzake de cloud zijn de laatste tijd de voordelen breed genoeg uitgemeten, variërend van meer efficiëntie, wereldwijde toegang tot uw data en verminderde kosten. Zeer terecht, maar het grootste risico is: de data is niet meer in eigen handen. Ook cloud services worden gehacked en kunnen leiden tot data breaches.

Al in 2008 waarschuwde Gartner hiervoor! De door hen in kaart gebrachte risico's blijven actueel. Als dat zo is, welke risico´s heeft men dan als bedrijf of organisatie? Hoe kan een bedrijf of organisatie aantoonbaar voldoen aan de General Data Protection Regulation? Een bedrijf of organisatie kan besluiten om risico's te nemen, maar het moeten wel bewuste keuze risico's zijn.

Ook moet er duidelijke procedures hoe om te gaan met dergelijke data. IO4U kan op meerdere vlakken ondersteuning bieden door middel van Consultancy en bijpassende oplossingen. Wij zijn ook expert op het gebied van de Bowtie[1] Methode om visueel te maken welke bedrijfsrisico's er zijn inzake deze nieuwe verordening.

[1] Meer informatie over de Bowtie methode vind u op: http://www.io4u.nl/partners/bowtiexp/

DATAMANAGEMENT

BEVEILIGING

BEREIKBAARHEID

BEHEERSBAARHEID

BESCHIKBAARHEID

Door vele jaren ervaring in het ontwerpen en implementeren van complexe datawarehouse, back-up en security oplossingen, kunnen wij wel stellen dat datamanagement onze specialisme is geworden. Door onze kennis zijn wij in staat om in te spelen op iedere situatie en behoefte van onze klanten.

Voor ons is het vanzelfsprekend dat we met de klant meedenken: eerst goed de 'business' van de klant begrijpen en daarna pas adviseren over een oplossing. Het is onze missie is om niet enkel een product te verkopen, maar door onze uitgebreide kennis zo onderscheidend te zijn dat elke klant uiterst tevreden is over onze high-end oplossingen.

Wij willen hoogstaande kwaliteit leveren. Deze eis stellen we niet alleen aan onze medewerkers, maar ook aan onze partners. We initiëren projecten en bedenken oplossingen om maximale resultaten te behalen. Onze oplossingen komen voort uit visie, inhoudelijke kennis, de juiste producten en een flinke dosis enthousiasme.

Our knowledge is your solution

Eekholt 42

1112 XH Diemen

020 4950 228 tel

020 4950 223 fax

www.io4u.nl.nl