Notities HSD Café: Security & GDPR
8 mei 2018

Notities van de break-out sessies

- Na de plenaire presentaties zijn de deelnemers uiteengegaan in vier interactieve break-out sessies. De notities zijn gebaseerd op de input en discussie van de aanwezigen binnen deze groepen.-

Key points

- Veiligheid en kostenbesparing. Doordat bedrijven verplicht data beter moeten beschermen, verlaagt dit het risico op datalekken. Door efficiënt te werken en overzicht te hebben, kan ook goedkoper gewerkt worden.
- Innovatie. Nieuwe inzichten worden verkregen, bedrijven worden creatiever.
- Marktpositie. De mate van data beveiliging kan als USP gebruikt worden.
- Bewustzijn. De GDPR is een stap in de goede richting, omdat alle organisaties nu gedwongen worden om na te denken over welke data zij verzamelen. De bewustwording dat dit belangrijk is, onder andere met de cyberaanvallen die voorkomen.
- Handhaving. De beboeting moet naar redelijkheid zijn volgens bezoekers van het HSD Café. In verband met onduidelijkheid die heerst over de grenzen van de wet, wachten partijen jurisprudentie af.
- Doorvoering en bijhouden. De uitdagingen die bij grote bedrijven/organisaties spelen, houden verband met het feit dat data zo verspreid is, en er veel verschillende afdelingen moeten samenwerken. Bij MKB-bedrijven liggen de uitdagingen vooral op het gebied van capaciteit.
- Human error. Al zijn ICT-systemen nog zo up-to-date en ontwikkeld volgens privacy by design, mensen blijven mensen en maken soms fouten. Wanneer een medewerker een fout maakt, heeft dit gevolgen. Draag dus niet alleen zorg voor de digitale systemen, maar licht je personeel ook goed voor op dit gebied.

Notitie break-out sessie 1 – Boardroom

Stelling: We moeten de huidige Security Maatregelen beperken om de privacy te waarborgen

Reacties:

- Security en privacy kunnen elkaar ook versterken, hoeven elkaar niet uit te sluiten
- Beiden zijn nodig vanuit de wet, het is niet of -of
    - Verantwoording voor de inzet van (security) middelen is wel nodig (kan ook achteraf)
- Veel organisaties zijn nog niet erg volwassen bij het inregelen van privacy (tussen niveau 1 en 2), maar de maatregelen zijn er wel de Functionaris Gegevensbescherming (FG) moet dan in verschillende systemen kunnen kijken
    - De middelen moeten er dan wel zijn
    - De huidige tools zijn niet altijd voldoende om privacy mee in te kunnen richten (bijvoorbeeld inperken van rechten security office t.b.v. privacy)
    - De oplossingen moeten vooral aan de menskant komen en in de organisatie niet in de systemen
    - Het moet wel mogelijk zijn om op details te kunnen inzoomen, indien dit nodig is
- De FG-rol is de schakel om te benaderen in een organisatie als uit een PIA (als tool) blijkt dat er risico's zijn
    - Maar het doel bepalen en het borgen moet door functionarissen in de organisatie gebeuren en meten bevoegdheden hebben om met gegevens te kunnen werken (bijvoorbeeld CIO)

AVG heeft veel uitzonderingen en verwijst naar andere (wettelijke) bepalingen en regels die een hoger belang kunnen hebben

- Bijvoorbeeld voor bewaartermijnen, dit moet doel specifiek zijn (bijvoorbeeld in de bouw waar 7 jaar geld, of academische ziekenhuizen waar 150 jaar geld?)
- Het beperken van het verzamelen van gegevens is aan de orde omdat vaak niet duidelijk is wie een doel heeft om hiermee te werken
    - Privacy kan dan soms ook door Security worden afgedwongen

Een grotere vraag voor de discussie is niet: *Hoe moeten Nederlandse organisaties met GDPR omgaan?* maar *Hoe beschermen we ons tegen mogelijke lekken bij de zeer grote spelers in de telecom/Apps (Google, Facebook, Samsung etc.)?* Dit is niet alleen voor de werkgevers om zijn personeel te beschermen maar ook voor de burger (rollen burger en werknemer vervagen).

Nu er een wet is met een boete gaan bedrijven wellicht wel handelen, maar vanuit de wetgever is het niet bedoeling om de boetes te gaan innen maar om bewustzijn en anders handelen te stimuleren. Uiteindelijk hoeft niet alleen de wetgever/toezichthouder te controleren maar ook de burger kan maatregelen nemen om GDPR af te dwingen, bijvoorbeeld door gebruik te maken van de rechten om te worden vergeten of om de informatie op te vragen.

Nationale wetgeving kan nog strenger zijn, bijvoorbeeld Duitsland. GDPT is dan ook opgezet vanwege de economische groei en protectionisme in de EU. Binnen twee jaar komt er een review naar de invoering van de GDPR per land. Dit creëert ook de druk vanuit de maatschappij in het ook daadwerkelijk in te voeren. Zoals:

- De burger/klant kan opvragen welke gegevens heb je van mij (dit stelt eisen en efficiency aan organisaties om hier mee om te kunnen gaan)
- Niet voldoen geeft ook reputatie schade niet alleen een boete

Deze tandem van de AP en de burger is dus nodig, het moet pijn doen bij een organisatie om niet te voldoen… Maar de AVG-maatregelen moeten naar redelijkheid worden getroffen en moeten een doelbinding hebben. Een (kleine/MKB) organisatie kan dus goed afwegen en onderbouwen wat wel en niet in te voeren.

Notitie break-out sessie 2 – Innovation Room

Is de GDPR-wetgeving evolutie of revolutie?

- Evolutie, maar het zou we een revolutie mogen zijn.
- Alle functionaliteiten die dus al bestaan maken het lastig om terug te gaan in het ontwerp van alle functionaliteiten van software om het beter te beveiligen.

Privacy by design en risicofactoren

- Bij A.I.-producten zou je ook een norm moeten hebben. RDW voor alle IOT-apparaten.
- Kijk daarnaast eens naar de info mailbox van jouw organisatie. Deze zit vol met interessante cv's en andere mails die niet altijd doorgezet en gewist worden. Bij een hack van deze mailbox, zit je met een enorm data lek.
- De opslag van data op back-ups is ook een risico, weet je welke data je wel en niet bewaard?
- Er wordt veel gevraagd van een DPO, de persoon binnen organisatie die de privacy op zicht neemt. Het vergt juridische kennis, ICT-kennis, bestuurlijke kennis, etc.

Awareness

- Het begint bij het feit dat het bekend is wat er mag en niet mag en wat mensen van je weten en niet weten. Daarom zijn discussies als deze relevant.
- Wat versta je onder persoonsgegevens; alles waaruit je als (één) persoon herleid kan worden.
- De wet lijkt duidelijk, maar is dit blijkbaar niet, bedrijven vragen om software die de eigen van de wet al verwerkt hebben. Mooie rol voor security sector.
- Impact moet duidelijk zijn voor kleinere bedrijven, wat is het gevaar van een gestolen identiteit? Media speelt hierbij een grote rol.
- De verantwoordelijkheid is ook niet altijd duidelijk.

Transparantie

- Commerciële bedrijven willen zo veel mogelijk data, maar dit hoeft niet tegen transparantie in te gaan.
- De overheid had gehoopt dat marktwerking het werk zou doen. Dat consumenten zouden kiezen voor goed beveiligde producten/diensten(GDPR) die dus verder niet je data 'claimen'. Echter is het zo dat bedrijven geld verdienen door die data. Doordat bedrijven ook weer nieuwe producten/diensten kunnen ontwikkelen die aansluiten bij de vraag die blijkt uit die data. Daarom blijven bedrijven die veel data verzamelen succesvol en zal de overheid beter moeten reguleren en handhaven.

Handhaving

- Er zal na 25 mei een eerste melding komen. Wat voor impact heeft dat? Dit geeft meer duidelijkheid over de grenzen van de wet.
- De APG geeft aan dat je ook zelf voorzichtig moet zijn om persoonlijke gegevens te laten slingeren. Echter is het probleem van een zzp'er. BSN-nummer kun je een persoon herleiden. Maar bij de belastingdienst/kvk is je BSN-nummer je bedrijfsnummer.
- Europese wetgeving wordt landelijk ingevoerd. Elke land verschilt dus nog iets. Nu geeft dat ook weer verschuivingen van hoofdkantoren van bedrijven die in een ander land gaan zitten, waar andere normen gelden dan elders.

Notitie break-out sessie 3 – Education Room

Vragen gesteld in de sessie:

- Certificering voor AVG, als een KemaKeur?
- Hoe om te gaan met Privacy bij Internet of Things (IoT)?
- Wat doet de overheid zelf?

Knelpunten

- AVG is complex omdat er meerdere ingewikkelde wetten zijn die samenhangen en soms tegenstrijdig zijn, zoals de Archiefwet en de Opschoningstermijn in de AVG/GDPR.
- Mensen binnen gemeenteraden maken zich zorgen omdat bestuurders (wethouders bijvoorbeeld) hoofdelijk aansprakelijk zijn maar vaker niet dan wel kennis hebben over privacy en security.
- E-marketing mag niet zomaar meer, dat heeft een impact op de businessmodellen van partijen. Dit kan echt pijn doen en verandering noodzakelijk maken.
- Onduidelijkheid over de interpretatie van de wetgeving, wat is bijvoorbeeld een 'redelijke termijn'? Dit blijkt afhankelijk van de context, niet een vaste periode.
- Er zijn veel producten en diensten die van verschillende componenten van anderen gebruik maken. Als system integrator is het bijna onmogelijk op de GDPR-compliance te bewaken van geïntegreerde producten en diensten. Mogelijk certificering van de losse componenten?

Kansen

- In positieve zin blijkt de AVG een effectief instrument voor verandering van met name het securitybeleid en staat het op de bestuursagenda.
- Tevens positief bij het in kaart brengen van welke data men bezit is dat er nieuwe waarde wordt gevonden (partijen blijken inzichten te kunnen halen uit rechtmatig verzamelde data door het overzicht voor het eerst te krijgen).
- Er is een kans voor publieke en private partijen om zich te onderscheiden door 'GDPR/AVG-compliant' te zijn, benut het als USP.
- Er is een potentie in kostenbesparing door het opschonen van data: dat scheelt onderhoud, serveropslagruimte, archief.

Oplossingen

- Het is goed te beginnen met de papieren exercitie en vervolgens de jurisprudentie af te wachten en daarnaar te handelen.
- Door weloverwogen informatie te verzamelen en actie te nemen, alsook de besluiten goed vast te leggen, beperk je de risico's al enorm. De AVG betekend niet dat je geen persoonsgegevens meer mag verzamelen. Wees duidelijk over dát je verzameld, wát je verzameld en wáárom je verzameld.
- Er zijn al goede startpunten voor het interpreteren van de wetgeving met praktische handvatten, zoals het Normenkader Informatiebeveiliging van CIP dat gratis beschikbaar is.
- Het is mogelijk om verwerkersovereenkomsten af te spreken met leveranciers, maar dat vraagt wel vasthoudendheid, kennis en organiseren inkoopmacht. Voorbeeld is er van ROC's die dat gezamenlijk met leverancier printers/scanners hebben gedaan.

Notitie break-out sessie 4 – HSD Plaza

Belangrijkste opmerkingen, vragen deelnemers:

- Papieren compliance is goed, maar hoe vertaalt zich dit in de praktijk?
- Grootste verschil naleving gaat zitten in de grote bedrijven versus de MKB-organisaties.
- MKB is en blijft zorgenkind m.b.t. GDPR; dit komt door een gebrek aan middelen en capaciteit.
- Gedragsverandering werknemers realiseren door enerzijds awareness en anderzijds goede systemen beschikbaar te stellen. Een solide datamanagement plan moet hieraan ten grondslag liggen.
- Technologische ontwikkelingen/apparaten bieden enorm veel kansen maar vormen tegelijkertijd een risico's voor individuele vrijheden.
- Individuen zouden altijd inzage moeten kunnen hebben in hun gegevens. Dit legt grote druk op bedrijven als straks de verzoeken hiervoor binnenkomen. Bij wie ligt het eigenaarschap?
- Allen eens dat GDPR een stap in de goede richting is.

- Kansen GDPR; zitten vooral in het tegengaan van de gegevens verzamelwoede. Minder administratieve lasten.
- Cybersecurity; mens is en blijft zwakste schakel door cyberonhandigheid. Digitale geletterdheid van groots belang. Ook hier combinatie van awareness en juiste systemen noodzakelijk.

Ervaringen/ adviezen deelnemers:

- Allen eens dat correcte naleving van GDPR zeer veel tijd en middelen kost.
- Waar correcte informatie op te halen niet altijd even duidelijk. ICT Nederland en MKB-Nederland wel relevante informatieverstrekkers op het gebied van GDPR.
- Er wordt binnen sommige organisaties zeer goed met data classificatie (binnen/buiten organisatie) omgegaan, terwijl dat bij andere organisaties nauwelijks onder de werknemers leeft. Medewerkers kunnen verantwoordelijk gehouden worden voor misstappen.
- Er is nog veel te veel onbewustheid (bv. in de zorgsector, fysiotherapeuten e.d.) over wat mag en wat niet. Er wordt te gemakkelijk omgegaan met informatie. Voorbeeld uit andere sector; te snel wordt overgestapt op bijvoorbeeld privé emailadressen uit gemakzucht.
- Hoe groter/complexer de organisatie in elkaar zit, hoe moeilijker het is om alle gaten te dichten en risico's af te dekken.
- Hoe serieus er wordt omgegaan met veiligheidsrisico's (en de naleving van beleidsupdates hieromtrent) afhankelijk van soort organisatie. Als veiligheid 'in het DNA' zit evidenter dan bijvoorbeeld in de zorgsector. Terwijl hier juist wel veel gevoelige informatie aanwezig is.
- Maak nog zichtbaarder voor alle werknemers hoe risico's te beperken zijn. DPO's en IT-afdelingen moeten hier de lijn uitstippelen.

Risico's:

- Technologische oplossingen zoals biometrie voor identificatie lijken haaks op de GDPR te staan.
- Door het analyseren data van IoT apparaten in huis, gemakkelijk te achterhalen wie op welk moment in welke ruimte aanwezig was (door bv. CO2 level te meten en te koppelen aan personen).
- Per onderdeel is losse informatie ongevaarlijk. Echter door koppeling verschillende databronnen, kan een nogal volledig beeld gemaakt worden. Dit is onwenselijk.
- Onbekend wat op lange termijn de trend is, dit brengt onzekerheden met zich mee.
- Ethische vraagstukken: gebrek aan diversiteit codeschrijvers zorgt voor knelpunten in algoritmes. Advies om een zo divers mogelijk team van programmeurs in te zetten.