PRIVACY EN INFORMATIEBEVEILIGING WORDEN SAMEN VOLWASSEN

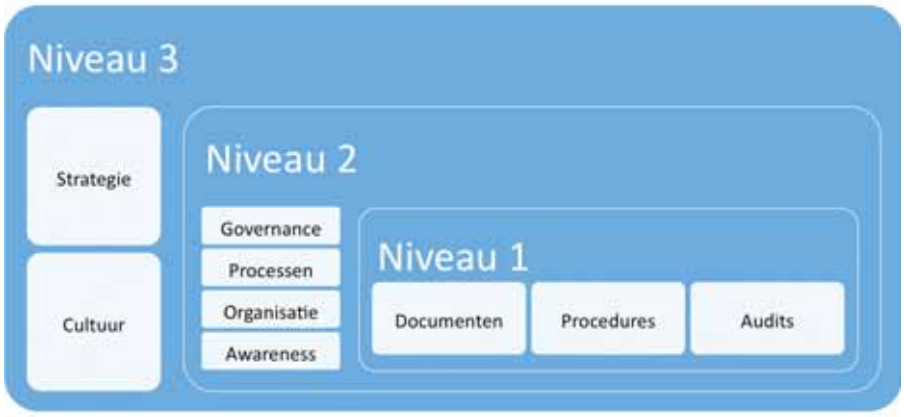
Veel lezers van dit blad zijn inmiddels drukdoende met de voorbereiding op 25 mei 2018, de datum waarop de Algemene Verordening Gegevensbescherming (AVG) van toepassing wordt. De hoogte van de mogelijke boetes, en de aansprakelijkheid voor bestuurders, is voor veel organisaties de voornaamste reden om het onderwerp privacy nu echt serieus op te pakken. De achterliggende reden van de AVG biedt organisaties echter ook een kans: een uniforme wetgeving voor heel Europa waarmee de open markt verder gestimuleerd zal worden.

De AVG benadrukt het belang van een goede beveiliging van persoonsgegevens, maar vooral: stelt het belang van de betrokkene centraal. De AVG legt ook nadruk op accountability en op het aantoonbaar in control zijn. Verantwoording kunnen afleggen over dit onderwerp is uiteraard nodig. Aantoonbaar in control zijn, stimuleert organisaties om de beheersing van de levensloop van data en de kwaliteit van data te verhogen. Een te sterke nadruk op in control zijn, kan helaas wel leiden tot de creatie van een papieren tijger. Een organisatie legt dan het zwaartepunt op allerlei controles om zeker te zijn dat er geen missers worden gemaakt. Deze nadruk op in control zijn en compliance kan leiden tot het invoeren van allerlei extra processen en overhead die de normale bedrijfsvoering kan gaan hinderen. Dit kan zeker ontstaan als voor privacy losstaande processen en functies worden ingericht. De aandacht voor privacy, waarbij informatiebeveiliging voor persoonsgegevens uitdrukkelijk onderwerp is, kan ertoe leiden dat door het gebrek aan middelen, tijd, geld enzovoorts de informatiebeveiliging van andere type gegevens minder aandacht kan krijgen.

Een organisatie kan immers maar een beperkt deel van haar middelen inzetten voor activiteiten die niet direct bijdragen tot de primaire activiteiten van de organisatie. De oplossing voor dit probleem is de additionele processen ten behoeve van de AVG zodanig in te richten dat optimaal gebruikgemaakt kan worden van reeds bestaande processen voor informatiebeveiliging en deze zoveel mogelijk in te bedden in de bestaande bedrijfsprocessen. In het verleden (WBP-tijdperk) werden informatiebeveiliging en privacy vaak als twee verschillende 'losstaande' disciplines gezien. Zowel privacy als informatiebeveiliging kunnen echter beschouwd worden als disciplines die zich richten op de beheersing van risico's geassocieerd met de kwaliteit van de informatievoorziening van een organisatie. Managementsystemen voor risicomanagement vormen daarmee een aanknopingspunt voor het samenvoegen van de activiteiten (integratie) voor deze disciplines. De integratie ondersteunt de volwassenheidsgroei van beide disciplines. Gebaseerd op dit uitgangspunt gaan we eerst in op de wijze waarop verschillende risicomanagementdisciplines kunnen worden geïntegreerd. We beschrijven vervolgens voor- en nadelen van integratie van privacy en informatiebeveiliging. Tenslotte gaan we in op een aantal praktische voorbeelden van integratie.

Modellen voor integratie

Privacy en Informatiebeveiliging zijn niet de enige risicomanagementdisciplines waar een organisatie aandacht aan moet besteden. Een organisatie van enige omvang zal aandacht besteden aan een waaier van risicomanagementdisciplines, zoals kwaliteitsmanagement, arbeidsomstandigheden, milieuzorg en informatiebeveiliging. Het is daarom niet verwonderlijk dat er nogal wat onderzoek gedaan is naar het integreren van managementsystemen voor het beheersen van risico's. Op



Figuur 1 – Niveaus van integratie.

basis van dergelijk onderzoek (1) zijn er vier niveaus van integratie te onderscheiden:

- Niveau 0: Geen integratie, losstaande managementsystemen.
- Niveau 1: Integratie op basis van structuurovereenkomsten veelal tot uitdrukking komend in de integratie van documenten, procedures en audits.
- Niveau 2: Integratie op basis van procesovereenkomsten veelal gebaseerd op de onderliggende PDCA-cyclus van de managementsystemen.
- Niveau 3: Integratie op basis van organisatie waarbij de onderliggende waarden en normen van de managementsystemen ingebed zijn in de strategie en de cultuur van de organisatie.

De niveaus 1 tot en met 3 zijn weergegeven in figuur 1.

De bovenstaande niveaus geven aan welke aspecten van managementsystemen kunnen worden geïntegreerd. Voor het uitvoeren van deze integratie zijn er in principe twee verschillende, voor de hand liggende, wegen:

- Eerst een afzonderlijk systeem opstellen voor een van de onderwerpen en deze vervolgens integreren met systemen voor de andere onderwerpen.
- Een enkel geïntegreerd systeem ontwikkelen en dit vervolgens implementeren.

De eerste vorm van integratie is veelal gebruikt door organisaties die vanwege commerciële of wettelijke redenen beginnen met een enkel onderwerp. Veel organisaties zijn bijvoorbeeld eerst begonnen met managementsystemen voor kwaliteit en hebben daar later milieuzorg en arbeidsomstandigheden aan toegevoegd.

De daadwerkelijke integratie van privacy en informatiebeveiliging kan uitgevoerd worden op basis van de achterliggende managementsystemen. Voor informatiebeveiliging ligt het gebruik van het managementsysteem beschreven in ISO 27001 (2) voor de hand. Voor privacy is er zover bekend nog geen breed gedragen standaard voor het te hanteren management-systeem. De managementsystemen opgesteld binnen ISO bevatten allen vergelijkbare elementen. De elementen uit ISO 27001 kunnen daarom gebruikt worden voor het identificeren van elementen die in een management-systeem aanwezig moeten zijn. De managementsystemen zijn daarnaast ook gebaseerd op een PDCA-cyclus. Die cyclus kan daarmee ook gebruikt worden voor integratie.

Joseph Mager, MISM, is Information Security Officer bij de Nederlandse Spoorwegen en vervult daarnaast een brugfunctie als Privacy Officer om synergie tussen privacy en informatiebeveiliging te creëren. Dit artikel is geschreven op persoonlijke titel en borduurt voort op zijn Master Thesis (5). Hij is bereikbaar via joseph.mager@ns.nl.

Renato Kuiper is security architect bij Verdonck, Klooster en Associates en vervult verschillende rollen op het snijvlak van architectuur, security en privacy. Hij is bereikbaar via renato.kuiper@vka.nl.

Figuur 2 - Managementsysteem en PDCA-cyclus.

Figuur 2 combineert die twee invalshoeken en geeft een aantal elementen van een managementsysteem weer in de PDCA-cyclus.

Het samenvoegen van de managementsystemen gebaseerd op de PDCA-cyclus leidt tot een integratie van niveau 2: de integratie op basis van procesovereenkomsten. De stap naar niveau 3, integratie op basis van organisatie, lijkt voor de meeste organisaties nog een brug te ver. Overigens kan door gebruik te maken van achterliggende waarden en normen het uiteindelijk eenvoudiger zijn om meerdere disciplines gezamenlijk naar niveau 3 te tillen. Veel risicomanagementdisciplines zijn gebaat bij het creëren van een open cultuur waarbij fouten in alle vrijheid kunnen worden besproken en een lerende organisatie die deze fouten gebruikt om haar processen te verbeteren. Hierbij wordt de PDCA-cyclus op het onderwerp ook daadwerkelijk doorlopen. Qua aanpak ligt het voor een organisatie die al ISO 27001 hanteert voor de hand om daar het managementsysteem voor privacy aan toe te voegen. Dit zal vooral in de IT-industrie, waar ISO 27001 veel wordt gebruikt, een geschikte aanpak zijn. Als ISO 27001 nog niet wordt gehanteerd, ligt het opzetten van een geïntegreerd systeem meer voor de hand. In beide gevallen dient de integratie projectmatig te worden opgepakt. Voor het opzetten van een dergelijk project kan het ISO-handboek voor de projectmatige integratie van managementsystemen (3) gebruikt worden.

Voor- en nadelen van integratie

Een organisatie kan ervoor kiezen om losstaande managementsystemen voor informatiebeveiliging en privacy in te voeren. De integratie bevindt zich in dit geval op niveau 0, geen integratie. Het voordeel van deze aanpak is dat er geen inspanning nodig is voor integratie en daarmee kunnen initieel de managementsystemen sneller worden opgezet. Deze aanpak kent echter ook nadelen. Er zullen daarna twee afzonderlijke systemen en bijbehorende processen in stand moeten worden gehouden. De informatie en rapportages over de bedrijfsprocessen en informatiesystemen benodigd voor beide disciplines zal twee keer worden opgesteld. De cultuurverschillen tussen beide disciplines worden niet aangepakt waarmee concurrentie om aandacht en middelen kan ontstaan. De genoemde aspecten leiden tot overhead in communicatie, tragere uitwisseling van informatie en verspilling van menselijk kapitaal. Het belangrijkste nadeel is dat medewerkers in de primaire processen van de organisatie opgezadeld worden met vergelijkbare activiteiten ten behoeve van het beheersen van de risico's voor beide disciplines.

Integratie op niveau 1 vereist dat bij het opstellen van documentatie en procedures structurele overeenkomsten voor beide disciplines worden gecreëerd. Denk hierbij bijvoorbeeld aan het creëren van documenten met eenzelfde opzet en indeling. Dit minimaliseert de inspanning die nodig is voor het opstellen van geïntegreerde documentatie en het bijhouden van administratie. Deze aanpak leidt tot een reductie van bureaucratie, waarmee additionele personeelskosten worden beperkt. De geïntegreerde documentatie vereenvoudigt daarnaast de uitvoering van interne en externe audits.

Een succesvolle integratie op niveau 2 vergt de betrokkenheid van het (top) management, gelijkvormige processen en het gebruik van gemeenschappelijke middelen, zoals informatiesystemen en mensen. Bij dit niveau van integratie is er aandacht voor en focus op de relatie tussen de beiden gebieden en de relatie van de gebieden met de bedrijfsvoering. Het belang van beide onderwerpen kan daarmee beter worden aangetoond. Daarnaast is het mogelijk prioriteiten te bepalen over beide gebieden heen en kunnen maatregelen worden geoptimaliseerd. De organisatie en verantwoordelijkheden kunnen op een enkele plek worden gedefinieerd. Een mogelijk obstakel voor integratie is dat de benodigde onafhankelijkheid van de functionaris gegevens-bescherming (FG) wellicht niet kan worden gerealiseerd. De privacy-rol ingevuld door een FG is een onafhankelijke rol.

De FG moet zich vrijelijk kunnen bewegen in de organisatie, geniet ontslagbescherming en rapporteert aan het hoogste managementniveau of zelfs aan de AP (Autoriteit Persoonsgegevens). Daarnaast vergt dit niveau van integratie een team waarin beide disciplines afdoende vertegenwoordigd zijn en teamleden voldoende affiniteit hebben met de andere discipline. Integratie van de CISO-rol en FG biedt grote voordelen voor informatiebeveiliging, immers een van de belangrijkste privacy principes gaat over de bescherming van de persoonsgegevens. Op dat vlak, lees principe, is maximale integratie te realiseren. Voor alle andere privacyzaken (lees basisprincipes), heeft een CISO ook baat bij bijvoorbeeld de transparantie over de gegevensverwerking.

Integratie in de praktijk

Het model voor integratie zoals weergegeven in figuur 1 en de onderdelen van het ISMS zoals weergeven in figuur 2 bieden aanknopingspunten voor integratie. Een aantal aspecten komen we daarvan al in de praktijk tegen en beschrijven we hieronder. Andere aspecten kunnen gebruikt worden om aanvullende kansen voor integratie te identificeren en te realiseren.

Governance en strategie

Met het model van een managementsysteem als uitgangspunt begint integratie van privacy en informatiebeveiliging aan de top. De besturing van beide disciplines is op het hoogste niveau van de organisatie belegd. Gezien het toenemend belang van informatiebeveiliging en privacy vormt dit aspect tegenwoordig geen al te grote uitdaging meer. Hierbij geldt wel dat de bestuurders moeten inzien dat informatiebeveiliging geen IT-feestje is. Het onderwerp risicomanagement moet in de volle breedte (lees Enterprise Risk Management) als portefeuille belegd worden in de Raad van Bestuur (RvB). De RvB bekrachtigt principiële uitspraken over het nut en de noodzaak van beide onderwerpen, zoals ze dit ook doet voor de uitgangspunten voor maatschappelijk ondernemen van de organisatie. Een zorgvuldige omgang met persoonsgegevens en een goede beveiliging is immers een maatschappelijke verplichting van elke organisatie, zoals ook naar voren komt in het rapport over zorgplicht opgesteld door Cyber Security Raad (4). Deze situatie kan dan ook alleen werken vanuit de inherente behoefte om zorgvuldig om te gaan met persoonsgegevens met een risico gebaseerde aanpak als uitgangspunt en geen compliance gedreven aanpak, het moetje…

Organisatie

De organisaties voor informatiebeveiliging en privacy kunnen geïntegreerd worden. Het is daarbij nodig om het betreffende team zo samen te stellen dat recht gedaan wordt aan de kennis en vaardigheden die nodig zijn voor beide disciplines. De medewerkers gericht op privacy zullen veelal een juridische achtergrond hebben. Enig begrip en kennis van IT is daarbij zeer zinvol, en in feite onontbeerlijk. De medewerkers gericht op informatiebeveiliging zullen veelal een IT-achtergrond of management-achtergrond hebben. Hierbij is uiteraard aanvullende kennis op juridisch gebied onontbeerlijk. Idealiter bevat het team ook een of meerdere personen die thuis zijn in beide disciplines, misschien vraagt dat om een SPA (Security en Privacy Architect). Zij zijn in staat om bruggen te bouwen tussen de disciplines en met de business en bestuurders en spelen een cruciale rol in opzetten van een enkel geïntegreerd managementsysteem.

Processen

Privacy en informatiebeveiliging kunnen beide beschouwd worden als risicomanagementdisciplines. Het ligt daarom voor de hand om de risicomanagementprocessen van beide disciplines te integreren. Een van de randvoorwaarden hiervoor is dat er ook nagedacht is over de risicobereidheid op beide gebieden. Informatie-beveiliging maakt vaak gebruik van een Business Impact Assessment (BIA) om de waarde van de informatie voor de organisatie te bepalen. Hierbij wordt nagegaan wat de gevolgen voor de bedrijfsvoering zijn als de informatie niet beschikbaar, juist, actueel of volledig (integer) is of de vertrouwelijkheid wordt geschonden. In de AVG staat het uitvoeren van een Privacy Impact Assessment (PIA) voor risicovolle verwerkingen centraal. Een dergelijke PIA is vaak ook benodigd als de verwerking plaatsvindt op basis van de grondslag van gerechtvaardigd belang. In die situatie moeten de belangen van de organisatie afgewogen worden tegen de belangen van de betrokkenen, de personen van wie de gegevens worden verwerkt. Het belang van de informatie voor de bedrijfsvoering wordt al bepaald in de BIA. Ten behoeve van de PIA moet dan nog aanvullend de belangen van de betrokkenen worden bepaald.

Nadat de BIA en PIA opgesteld zijn, kan door middel van een risicoanalyse bepaald worden welke maatregelen genomen dienen te worden om de risico's afdoende te beheersen. De AVG noemt expliciet beveiliging van de persoonsgegevens als uit te voeren maatregelen. Logischerwijs dragen de maatregelen genomen op basis van de risicoanalyse voor informatiebeveiliging daarmee bij aan de maatregelen voor privacy. Aanvullend kunnen

maatregelen vanuit de AVG ertoe leiden dat er minder zware maatregelen voor het beveiligen van persoonsgegevens nodig zijn. Indien bijvoorbeeld dataminimalisatie wordt toegepast, wordt de impact van het uitlekken van persoonsgegevens verlaagd. Deze verlaging van impact geldt daarbij ook nog eens voor de gevolgen voor de betrokkenen en voor de gevolgen voor het bedrijf.

Integratie van de BIA en PIA is mogelijk. Een organisatie is vrij om te kiezen op welke wijze zij het proces voor het bepalen van informatiebeveiligingsrisico's en risico's met betrekking tot verwerking van persoonsgegevens uitvoert. In de AVG worden wel minimale eisen gesteld, bijvoorbeeld dat er onder andere een risicoafweging gedaan moet worden. Beide processen zijn simpel te integreren, maar moeten wel met brede kennis ter ondersteuning integraal met de business worden gedaan. De business wordt nu voor een nieuw informatiesysteem slechts eenmaal bevraagd op zowel de BIA- als de PIA-vragen.

Het risicomanagement van beide disciplines moet daarnaast ook ingebed worden in de bedrijfsprocessen. Omdat beide disciplines risico's in de informatievoorziening van de organisatie behandelen, is het zinvol om aan te sluiten bij de ontwikkelprocessen van deze informatie-voorziening. Als er een standaard voortbrengingsproces is met bijvoorbeeld Quality Gates, kan zowel het bepalen van de maatregelen als de controle op implementatie daarvan in dit proces worden ingebed. Bij een organisatie waar informatiemanagement goed is ingevoerd, wordt daarnaast op dit niveau aangesloten op de informatie-planning. Het is zoals altijd zinvol om zo vroeg mogelijk aangesloten te zijn op nieuwe ontwikkelingen. Op deze wijze kan het beste invulling worden gegeven aan het principe van privacy by design.

Een andere mogelijkheid voor integratie van processen betreft het afhandelen van incidenten. Het proces voor informatiebeveiligingsincidenten is vrij eenvoudig uit te breiden met een proces voor het melden van datalekken. De uitbreidingen richten zich op het bepalen van de impact van een datalek voor betrokkenen, het op tijd melden bij de AP, de juistheid van de melding en de afweging of er gemeld moet worden bij de betrokkenen. De integratie betreft overigens niet enkel het melden en afhandelen van incidenten. Deze strekt zich uit tot de evaluatie, de check- en act fase, van een managementsysteem van incidenten en op basis daarvan het bijstellen van maatregelen. Op deze wijze wordt pas echt een meerwaarde gecreëerd voor de bedrijfsvoering.

Awareness en communicatie

De belangrijkste aspecten waarop de disciplines kunnen integreren zijn bewustwording, opleiding en communicatie. Deze aspecten dragen bij aan de stap naar integratie op niveau 3. Door het belang van beide aspecten te benadrukken, kan het zorgvuldig omgaan met de persoonsgegevens onderdeel gaan uitmaken van de cultuur van de organisatie. Het is daarbij van belang dat de activiteiten op deze aspecten zorgvuldig op elkaar afgestemd zijn en uiteraard toegesneden op de verschillende doelgroepen in de organisatie.

Conclusie

Invoering van de AVG biedt kansen om privacy en informatiebeveiliging verder te integreren. In de praktijk gebeurt dit al binnen veel organisaties. Door gebruik te maken van de achterliggende managementsystemen kunnen ook andere mogelijkheden voor integratie worden geïdentificeerd en gerealiseerd. Een organisatie die gebruikmaakt van alle mogelijkheden, zal in staat zijn om de risico's op beide gebieden efficiënter te beheersen. De benodigde inspanning zal uiteindelijk lager zijn dan wanneer beide gebieden afzonderlijk worden ingericht. Daarnaast zal de bedrijfsvoering minder belast worden. Afhankelijk van de rol en ophanging van zowel de CISO als de FG is dit eenvoudig of lastiger in te voeren.
Informatiebeveiligingsmaatregelen die getroffen worden op basis van de AVG worden gezien de compliancedruk van mei 2018 nu sneller geïmplementeerd. De CISO kan zich in een later stadium daarom gaan focussen op de beveiliging van andere typen informatie: financieel, intellectueel eigendom en operationele IT.

Als privacy gezien wordt als een zorgplicht om goed om te gaan met gegevens van betrokkenen en niet als een moetje, en er wordt er een risico gebaseerde aanpak voor privacy als basis gebruikt, dan is deze goed te integreren met de PDCA-cyclus van informatiebeveiliging. Zo kunnen beide disciplines gezamenlijk in volwassenheid groeien.

Referenties

(1) How integrated are environmental, quality and other standardized management systems. An emperical studgy. Merce Bernardo et al. 2008, Journal of Cleaner Production.
(2) ISO. ISO 27001:information security management system, www.iso.ch, 2013.
(3) The integrated use of system management standards. sl : Internatial Organisation for Standardization, 2008.
(4) CSR. Ieder bedrijf heeft digitale zorgplichten. sl : Cyber Security Raad, 2017.
(5) Mager, Joseph. Het succes van risicomanagement. 2010.