Naar een volwassen privacy-implementatie

Een nieuw Privacy Control Framework als onderdeel van de informatiehuishouding

8 september 2017

In de IT-Auditor wordt regelmatig over het onderwerp privacy gepubliceerd. In het artikel Privacy, meer dan compliance en informatiebeveiliging van Ed Ridderbeekx en Suzanne Scheuller[1] wordt gepleit voor een bredere visie op dit onderwerp. Privacy is meer dan een optelsom van juridische en beveiligingstechnische maatregelen.

Waar Ed Ridderbeekx en Suzanne Scheuller de focus leggen op het fundamentele privacybegrip, richt dit artikel zich vooral op de praktische implementatievragen die dit met zich meebrengt. Onze eigen ervaringen met de implementatie van privacybeveiliging, aangevuld met literatuurstudie, hebben ons tot de conclusie gebracht dat voor een volwassen privacy-implementatie twee voorwaarden gelden. Ten eerste moet privacybescherming als onderdeel van het informatiemanagement een geschikte plaats binnen de organisatie krijgen. Ten tweede moet de organisatie de privacybescherming systematisch organiseren door uit te gaan van een omvattend raamwerk dat de essentiële maatregelen beschrijft.

In dit artikel ontwikkelen we aan de hand van verschillende internationale privacy-normstelsels een nieuw privacy control framework. Vervolgens geven we aan hoe de set maatregelen van dit framework het beste kan worden geïmplementeerd als onderdeel van een organisatiebrede informatiehuishouding.

Een reeks van incidenten, de recent ingevoerde Meldplicht Datalekken en de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG) hebben het privacyvraagstuk weer volop in de belangstelling geplaatst. Daarbij wordt nogal eens de indruk gewekt dat dit alleen maar extra bureaucratische maatregelen met zich meebrengt, zonder duidelijk doel of voordeel. Niets is minder waar. Privacy is een fundamenteel menselijk en maatschappelijk belang dat adequaat beschermd moet worden. Een boodschap die in de nieuwe Europese wetgeving ook duidelijk is verwoord en die aan bedrijven en burgers een nieuw speelveld biedt om hun privacybelangen te wegen en te beheersen.

In dit artikel staan we niet alleen stil bij het belang van een goede privacybescherming voor organisaties die omgaan met privacygegevens, maar ook bij de noodzaak om tot een adequaat beheersingssysteem te komen. We gaan daarbij niet uit van een

specifieke juridische of IT-technische visie, maar vanuit een brede informationele visie. Vervolgens vergelijken we de belangrijkste privacy frameworks met elkaar en plaatsen we de daaruit geselecteerde maatregelen in een privacy control framework. Dit privacy control framework geeft een volledig en samenhangend beeld van de meest relevante beheersmaatregelen en is binnen een groot aantal organisaties toepasbaar.

Noodzaak van privacy

Lange tijd is het privacyvraagstuk beschouwd als een merkwaardige hobby van een kleine groep juristen. Toch hadden deze pioniers een vooruitziende blik. Een maatschappij waarin niet een zekere mate van privacybescherming bestaat, is volstrekt onleefbaar. Niet voor niets kennen we van oudsher het briefgeheim, het medische beroepsgeheim, de bescherming van het huisrecht, het verschoningsrecht voor echtgenoten en nog vele andere vormen van privacybescherming.

Volledige transparantie maakt mensen kwetsbaar, met name voor partijen die een grote informatievoorsprong weten op te bouwen. Zo zijn overheden in een steeds hoger tempo bezig om enorme verzamelingen van privacygevoelige gegevens aan te leggen. Vooralsnog met legitieme bedoelingen, maar het is slechts een kleine stap naar manipulatie en misbruik. Zo is het digitaal volgen van terroristen misschien nog acceptabel, maar dergelijke instrumenten kunnen even gemakkelijk tegen andere 'onwelgevallige' groepen en 'lastige' individuen worden gebruikt.

De beste waarborg tegen dergelijke privacyschendingen zou zijn dat persoonsgegevens helemaal niet verzameld mogen worden, maar dat punt zijn we inmiddels al ruim gepasseerd. Wat ons nu nog rest is een stevige wettelijke regulering in combinatie met onafhankelijk toezicht, precies datgene waar juristen zich al jarenlang druk om maken. Terecht, gezien een reeks van opzienbarende incidenten zoals het Echelon afluisterschandaal, de documenten van Edward Manning op WikiLeaks en de grootschalige afluisterpraktijken van de NSA die Edward Snowden openbaar maakte.

Niet alleen regeringen, maar ook grote commerciële partijen begrijpen maar al te goed de waarde van informatie – informatie die voor een belangrijk deel uit persoonsgegevens bestaat. Waar bedrijven steeds meer aandacht besteden aan het beschermen van deze waarde met als direct gevolg dat de informatiebeveiliging steeds belangrijker wordt, blijft dit besef bij de individuele burger nog wat achter. De laatste jaren lijkt er echter, met name vanuit burgergroeperingen in de VS, een steeds sterkere tegenbeweging te ontstaan. Dit misschien ook wel, omdat er in de VS voor is gekozen om juist geen wettelijke privacybeschermende maatregelen te nemen en dit aan de vrije markt over te laten.

Beheersen van privacyrisico's

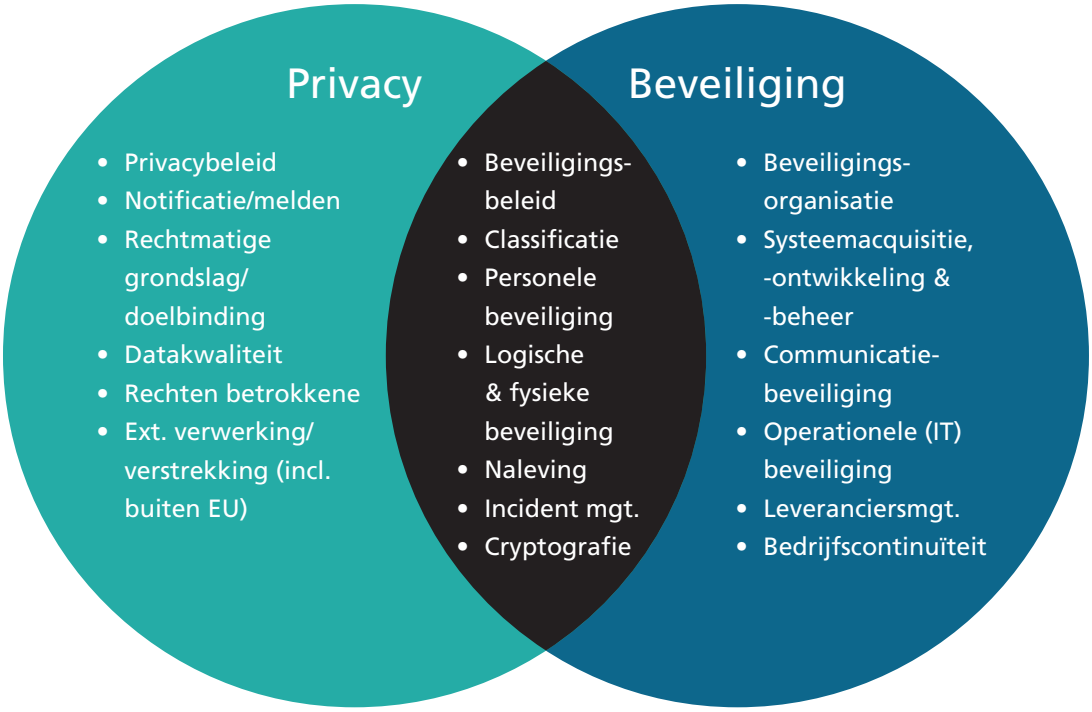
In Europa is onder aanvoering van Duitsland en daarin actief gesteund door Nederland, in eerste aanleg gekozen voor een versterking van de privacybescherming door wetgeving. De inmiddels in werking getreden AVG kan voor organisaties tot hoge boetes leiden in geval van datalekken en privacy non-compliance. Privacy wordt daarmee voor Europese bedrijven een juridisch en financieel risico, maar met de toename van het algemene privacybewustzijn onder de burgers, ook een steeds belangrijker imagorisico. Dit is een van de redenen waarom het senior management van bedrijven en de overheid steeds meer aandacht heeft voor het beheersen van privacyrisico's. Daarnaast wordt binnen de overheid bij het vaststellen van nieuw beleid of bij de implementatie van nieuwe projecten, nu al het uitvoeren van een Privacy Impact Analyse (PIA) verplicht gesteld. De Autoriteit Persoonsgegevens heeft samen met NOREA daarvoor een handleiding opgesteld, waarin ook een flinke vragenlijst is opgenomen. De meest recente versie 1.2 van de handleiding uit 2015 is inmiddels aangepast aan de nieuwe eisen van de Meldplicht Datalekken. Overigens zal met de invoering van de AVG ook het bedrijfsleven verplicht worden om PIA's te gaan uitvoeren als de verwerking een hoog privacyrisico heeft.

Belangrijkste doel van de PIA is het creëren van bewustwording en inzicht in de privacy- en compliance-risico's die niet alleen de organisatie zelf, maar ook anderen kunnen lopen. De risicoanalyse is slechts een eerste stap, die gevolgd zal moeten worden door het treffen van daadwerkelijke beheersmaatregelen die de gesignaleerde privacyrisico's mitigeren. Een dergelijk samenhangend geheel van beheersmaatregelen wordt ook wel een Privacy Control Framework genoemd.

Nadeel van de PIA-vragenlijst is dat deze puur uitgaat van de wettelijke vereisten van de Wet bescherming persoonsgegevens (Wbp). Een control framework dat op de PIA is gebaseerd zal dan ook in het beste geval de wettelijke privacy en compliance-risico's afdekken, maar ook niet meer dan dat.

Informatiemanagement als startpunt

De visie op privacy zou breder moeten zijn dan enkel het juridische, compliance- of het IT-securityperspectief. Het hoeft geen betoog dat informatiemanagement – en meer specifiek de informatiebeveiliging – in het gehele privacybeschermingsvraagstuk een belangrijke rol speelt. Zo hebben informatiebeveiliging en privacybescherming een duidelijk gemeenschappelijk doel, namelijk de bescherming van waardevolle en gevoelige bedrijfsinformatie. Daarbinnen biedt informatiebeveiliging de noodzakelijke en concrete maatregelen die nodig zijn om privacybescherming te kunnen realiseren (zie figuur 1).



FIGUUR 1: PRIVACYBESCHERMING EN INFORMATIEBEVEILIGING

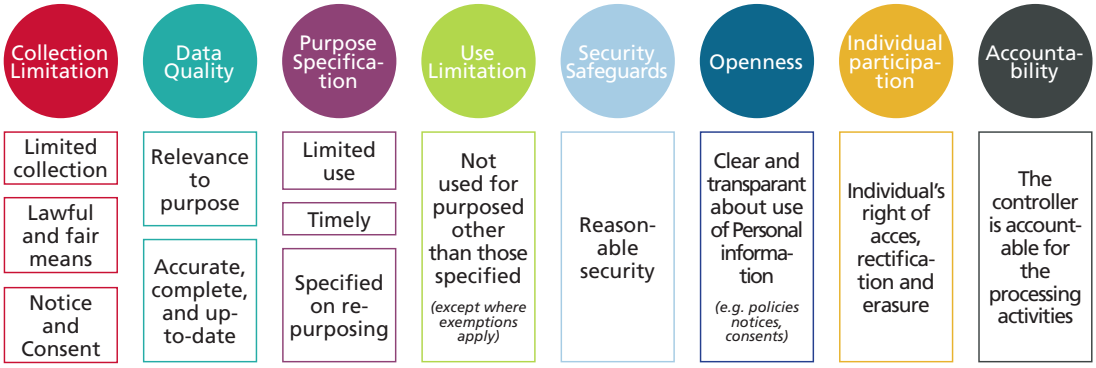
De wens van organisaties om het informatiebeveiligingsbeleid zo snel mogelijk op orde te krijgen, leidt er in de praktijk nog weleens toe dat de nadruk eenzijdig op de praktische implementatie van concrete securitymaatregelen komt te liggen. Door deze focus op techniek ontstaat het gevaar dat andere, minstens zo belangrijke aspecten worden ondergewaardeerd. Het zou dan ook de voorkeur hebben om het vraagstuk van privacybescherming niet alleen vanuit een juridisch of een security kader te benaderen, maar vanuit een veel breder informationeel kader.

Informatiemanagement vormt een intermediair tussen de bedrijfsvoering en de IT. Vanuit dit perspectief staat niet zozeer de bedrijfsvoeringskant (juridische aspecten) of de IT-kant (security aspecten) centraal, maar juist de informatie (follow the data). Voor informatiemanagement vormt de cyclus van creatie tot en met het vernietigen van data de basis. Zowel fysieke als digitale informatie, maar ook de verschillende typen data waaronder HR-data, klantdata, financiële data en medische data. Persoonsgegevens zijn een bijzondere vorm van informatie en daarmee een integraal onderdeel van de informatiehuishoudingsvraag.

Internationale principes

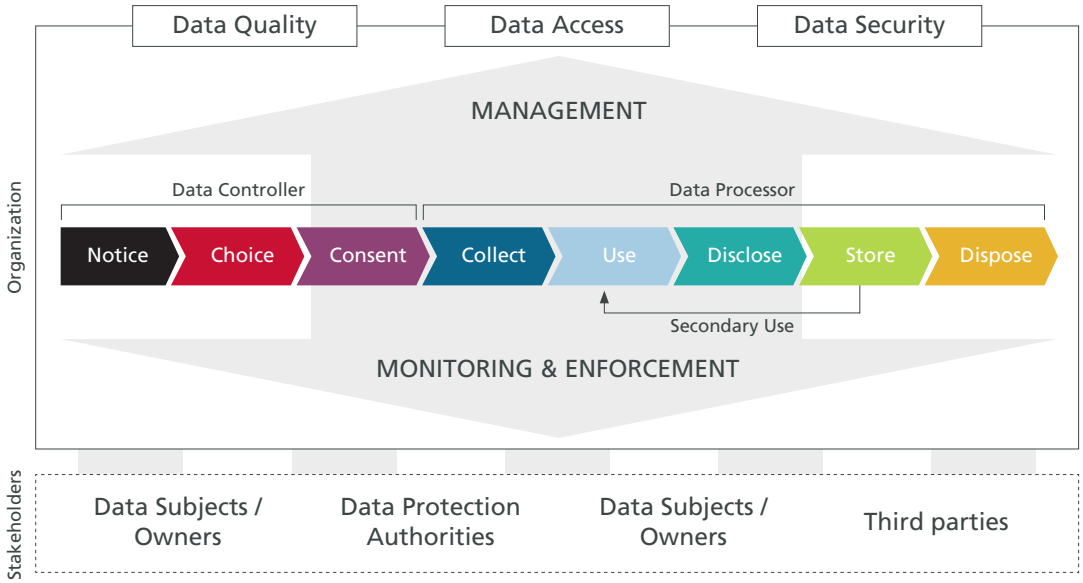
Inmiddels is er een aantal internationale privacy-frameworks ontwikkeld waarin de belangrijkste privacy principles zijn opgenomen. De privacy principles vormen de basis van nationale wetgeving in Europa, sectorale wetgeving in Amerika en nationale wetgeving in de Aziatisch-Pacifische regio. De Organisation for Economic Co-operation and

Development (OECD) heeft in 1980 privacyrichtlijnen opgesteld die via de EU-richtlijn en haar opvolger, de AVG, ook van toepassing zijn op de Nederlandse wetgeving. Figuur 2 bevat een schematische weergave van de acht genoemde principes uit de OECD-richtlijnen.



FIGUUR 2: PRINCIPES IN DE OECD-RICHTLIJN

In Amerika wordt veelal gerefereerd aan de Generally Accepted Privacy Principles. Deze GAPP-principes zijn in grote lijnen gelijk aan de OECD-richtlijnen, maar leggen meer nadruk op management en monitoring van privacy. Een vergelijking van de internationale privacy principles maakt duidelijk dat de informatielevenscyclus verweven zit in al deze raamwerken. In de Wbp echter komt dit principe minder duidelijk naar voren, terwijl informatiebeveiliging hier juist weer meer aandacht krijgt. Dit is het vertrekpunt geweest voor het ontwikkelen van een informatielevenscyclusmodel voor privacy, waarmee organisaties privacyrisico's kunnen identificeren. Het conceptueel model geeft de informatielevenscyclus weer binnen een organisatie en is opgebouwd uit een combinatie van onderdelen van de GAPP-principes en de OECD-richtlijnen.



FIGUUR 3: INFORMATIELEVENSCYCLUSMODEL VOOR PRIVACY

De verschillende fasen in het model, maar ook het management, de datamanagementaspecten (datakwaliteit, toegang tot data en databeveiliging) en de stakeholders zijn componenten die in beschouwing genomen moeten worden bij identificatie van privacyrisico's. Het model dient als kapstok voor identificatie van privacyrisico's door organisaties en vormt daarmee de basis voor de selectie van relevante privacy-beheersmaatregelen.

Internationale frameworks en good practices

Naast de bekende GAPP-principes is gekeken naar nog een tiental nationale en internationale privacy frameworks en good practices. Vervolgens is per onderwerp zoveel mogelijk een vergelijking gemaakt en is al deze informatie in een matrix vastgelegd. De beheersmaatregelen zijn geanalyseerd en er heeft een beoordeling plaatsgevonden in hoeverre deze relevant zijn voor het privacydomein. Dit heeft geresulteerd in een 'short list' van vier specifieke raamwerken, te weten:

- GAPP (AICPA/CICA).
- SP800-R53 Privacy Control Catalog (NIST).
- Raamwerk Privacy Audit (NOREA, gebruikt bij de 3600n standaard).
- European Privacy Seal (EuroPriSe) raamwerk.

Vanuit de vier geselecteerde raamwerken heeft een horizontale toetsing plaatsgevonden op de geïdentificeerde beheersmaatregelen en zijn deze verder met elkaar vergeleken en op elkaar afgestemd. Bij de uiteindelijke selectie van de beheersmaatregelen was het criterium dat elke maatregel in minstens drie raamwerken diende voor te komen. Dit heeft geleid tot één nieuw privacyraamwerk, dat voor iedere fase en iedere component in het informatielevenscyclusmodel en voor de bijbehorende privacyrisico's, de daaraan gerelateerde (mogelijke) mitigerende beheersmaatregelen weergeeft. Tabel 1 bevat de selectie van de eenendertig belangrijkste beheersmaatregelen, waarbij steeds een link is gelegd met de componenten uit het informatielevenscyclusmodel. Deze eenendertig maatregelen zijn de meest genoemde privacy-beheersmaatregelen en ze worden waarschijnlijk ook wereldwijd het meest toegepast.

Control ID	Control naam	Control domein	Link met informatie-levenscyclusmodel
1.1	Privacy Policies	Privacy Policies	Management
1.2	Privacy Roles & Responsibilities	Privacy Officer ('FG')	Management
1.3	Personal Data Identification and Classification	Data Infrastructure	Management
1.4	Risk Assessment	Risk and Control Framework	Management
1.5	Privacy Impact Assessment for New Products & Services, Processes and Systems	Privacy Processes	Management
1.6	Privacy Incident and Breach Management	Privacy Incident and Breach Management	Management
1.7	Qualifications of Internal Personnel	Training and Awareness	Management
1.8	Privacy Awareness and Training	Training and Awareness	Management
1.9	Legal Review of Changes in Regulatory and Business Requirements	Legal Processes	Management
2.1	Privacy Notice / Statement	Privacy Policies	Notice
2.2	Registration with the Data Protection Authorities	Privacy Processes	Notice
3.1	Consent Framework (opt-ins / opt-outs)	Information Lifecycle Management	Choice and Consent
4.1	Data Minimisation (collection)	Information Lifecycle Management	Collect
5.1	Use Limitation of Personal Data	Information Lifecycle Management	Use, Store and Dispose
5.2	Privacy Architecture (Privacy by Design)	Privacy Architecture / Requirements	Use, Store and Dispose
5.3	Data Retention	Information Lifecycle Management	Use, Store and Dispose
5.4	Disposal, Destruction and Anonymization	Information Lifecycle Management	Use, Store and Dispose
6.1	Data Access Requests	Privacy Processes	Data Access
6.2	Data Correction Requests	Privacy Processes	Data Access & Data Quality
6.3	Data Deletion Requests	Privacy Processes	Data Access
7.1	Third Party Disclosure and Registration	Third Party Management	Disclose
7.2	Third Party Agreements	Third Party Management	Disclose
7.3	Mechanisms for Data Transfers to non-EU and non-EEA countries	Privacy Processes	Disclose
8.1	Information Security Policy	Information Security Management	Data Security
8.2	Identity & Access Management	Information Security Management	Data Security
8.3	Secure Transmission of Personal Data	Information Security Management	Data Security
8.4	Encryption of Personal Data on Portable Media	Information Security Management	Data Security
8.5	Logging of Access to (Sensitive) Personal Data	Information Security Management	Data Security
9.1	Measures on Accuracy and Completeness of Personal Data	Privacy Processes	Data Quality
10.1	Review on Privacy Compliancy	Accountability & Auditing	Monitoring and Enforcement
10.2	Periodic Monitoring on Privacy Controls	Accountability & Auditing	Monitoring and Enforcement

TABEL 1: SELECTIE VAN BEHEERSMAATREGELEN UIT VERSCHILLENDE RAAMWERKEN

Informatiemanagementmodel

Nu we de belangrijkste privacy-beheersmaatregelen kennen zoals die in het nieuwe Privacy Control Framework zijn vastgelegd, is de volgende vraag waar deze binnen organisaties dienen te worden belegd. In de praktijk is er vaak een tweedeling. De maatregelen met een compliance-aspect krijgen bijvoorbeeld een plaats binnen de afdeling juridische zaken of een stafafdeling binnen het domein Governance, Risk en Compliance (GRC). De meer praktische en technisch gerichte maatregelen vinden hun weg naar het IT- en securitydomein. Een dergelijke tweedeling is een ongewenste verzwakking van het

privacybeleid, wat nog eens wordt verergerd doordat deze bedrijfsonderdelen zich aan weerszijden van de zogenaamde alignmentkloof bevinden. Dit alignmentbegrip is in de jaren '90 van de vorige eeuw ontstaan als verzamelbegrip voor de moeizame relatie en communicatie tussen business en IT.

Na vele jaren van stagnatie was het Rik Maes die met zijn Informatiemanagementmodel – ook wel bekend als het Negenvlaksmodel – de impasse van de alignmentkloof doorbrak. Door een intermediaire organisatie in te richten tussen business en IT kan de relatie tussen deze twee onderdelen hersteld worden. Daarnaast kunnen de voor beide onderdelen wezensvreemde taken in de intermediaire organisatie worden samengebracht.

Het gebruik van het negenvlaksmodel voor het inrichten van een privacyraamwerk heeft een tweeledig voordeel. Allereerst heeft het geen last van de fragmentatie van de getroffen privacymaatregelen door het ontbreken van de alignmentkloof. Daarnaast is het negenvlaksmodel specifiek bedoeld voor de inrichting en beheersing van de informatiehuishouding. In feite zijn de gegevens waarop de privacybescherming zich richt, persoonsgegevens, niets anders dan een bijzondere informatiestroom en integraal onderdeel van de informatiehuishouding.

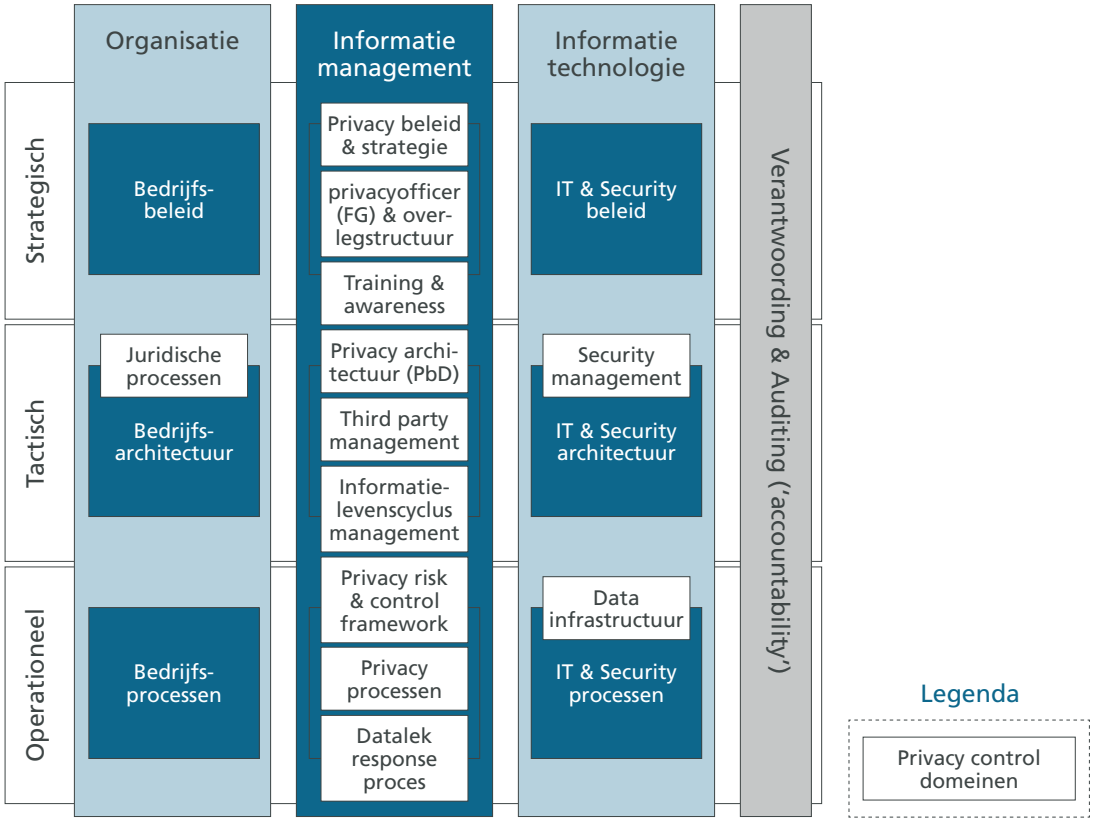
In het overzicht van de eenendertig belangrijkste privacy-beheersmaatregelen is ook aangegeven binnen welk controldomein deze geïmplementeerd dienen te worden. In totaal zijn het er dertien die een plaats in het informatiemanagement model van Maes zouden moeten krijgen. Deze dertien privacy controldomeinen zijn:

- *Privacybeleid & strategie:* het organisatiebeleid, ingebed in de organisatiestrategie, dat beschrijft hoe werknemers in de gehele organisatie dienen om te gaan met het verzamelen, gebruiken, bewaren, verstrekken en verwijderen van persoonsgegevens, inclusief het externe beleid dat informatie verschaft aan externe belanghebbenden.
- *Privacy Officer & Overlegstructuur:* de organisatiestructuur, rollen en verantwoordelijkheden voor het beheersen van de verzameling, het gebruik, het bewaren, het verstrekken en het verwijderen van persoonsgegevens, en voor de operationele afstemming daarover.
- *Training & Awareness:* generieke en specifieke training toegepast op de verzameling, het gebruik, het bewaren, het verstrekken en het verwijderen van persoonsgegevens door de organisatie, en awareness-activiteiten om de privacykennis te onderhouden.
- *Privacy Architectuur (Privacy-by-Design):* het proces om te borgen dat principes als gegevensminimalisatie en doelbinding, privacy-by-default, en gegevens ontdoen van persoonsinformatie (de-identificatie) vanaf het begin worden toegepast.
- *Third Party Management:* processen die de privacyrisico's bij externe partijen beheersen.
- *Informatie Levenscyclus Management:* processen en beheersmaatregelen voor de hele informatielevenscyclus van persoonsgegevens, gericht op het verzamelen tot en met het verwijderen van persoonsgegevens.
- *Privacy Risk & Control Framework:* alle concrete maatregelen zoals genoemd in het Privacy Control Framework om de privacyrisico's in kaart te brengen en de beheersmaatregelen te selecteren om deze risico's te managen en mitigeren.
- *Privacy Processen:* privacyspecifieke processen die borgen dat de organisatie persoonsgegevens verwerkt conform zijn verplichtingen, zoals recht op inzage.

- *Datalek Response Proces:* procedure voor het identificeren en beoordelen van incidenten met persoonsgegevens en voor de respons daarop.
- *Juridische Processen:* processen die de huidige en toekomstige eisen in privacywetgeving inzichtelijk maken en monitoren om zo de juiste processen en beheersmaatregelen in te richten.
- *Security Management:* de interactie tussen privacy en security binnen een organisatie om te borgen dat privacy-eisen voor logische en fysieke toegangsbeveiliging op een voldoende niveau zijn ingericht.
- *Data Infrastructuur:* een overzicht van de datastromen en persoonsgegevens die binnen de organisatie worden verwerkt inclusief de verschillende doeleinden en de classificatie van persoonsgegevens.
- *Verantwoording & Auditing (Accountability):* het continue proces waarin de organisatie zijn beheersmaatregelen toetst op effectiviteit, via rapportages, zelfevaluaties en audits.

Privacy Control Framework

De dertien privacy-controldomeinen zijn geplot op het negenvlaks-informatiemanagementmodel van Maes. Hierin worden de verschillende functies op de horizontale as weergegeven: de bedrijfsvoering, het informatiemanagement en de IT-organisatie. Op de verticale as zijn de verschillende niveaus geplaatst – strategisch, tactisch of operationeel – waarmee uiteindelijk de relatie tussen de (aard van de) control aandachtsgebieden en de verschillende niveaus en functies binnen een organisatie wordt gelegd. Op basis hiervan kunnen privacy-beheersmaatregelen worden ingericht en geborgd door de verschillende functies binnen een organisatie. Een belangrijke rol is hierbij weggelegd voor informatiemanagement en securitymanagement. Dit heeft geresulteerd in het onderstaande privacy-controlraamwerk.



FIGUUR 4: PRIVACY-CONTROLDOMEINEN GEPLOT OP HET INFORMATIEMANAGEMENT MODEL VAN MAES (2010)

Conclusie

Privacy krijgt net als informatie een steeds belangrijkere positie als waardecomponent binnen de bedrijfsvoering. Het ligt dus voor de hand om deze ontwikkelingen op een gelijksoortige manier te benaderen door de privacybeheersing een plaats te geven binnen de intermediaire informatiemanagement-organisatie. Voor het beleggen van deze verantwoordelijkheid hoeft dan ook geen keuze gemaakt te worden of het privacyvraagstuk nu primair een compliance- of een securitykarakter heeft. Daarmee wordt ook voorkomen dat privacyfuncties aan weerzijden van de alignmentkloof terechtkomen.

De meerwaarde van het gepresenteerde Privacy Control Framework is dat het een gewogen en actuele selectie bevat van de concrete beheersmaatregelen afkomstig van internationaal geaccepteerde standaarden. Daarmee ontstaat een effectief instrument om de juiste beheersmaatregelen te selecteren.

Door privacy te beschouwen als een bijzonder aspect van informatiemanagement en het te verankeren in een aparte intermediaire organisatie, ontstaat ruimte voor een verdere ontwikkeling van het steeds belangrijker wordende privacyvraagstuk.

Mr. W. (Winfried) R. Nanninga RE CISA MMC, Ir. A. (Ali) Ougajou MSC RE en H.M (Maurice) Koetsier MSc CIPM CIPP/E

Winfried Nanninga is een zelfstandig gevestigd IT-auditor met ruime audit- en advieservaring. Daarnaast is hij als docent verbonden aan AVANS Hogeschool, waar hij de IT-auditopleiding verzorgt. Bij NOREA is hij bestuurslid en actief in verschillende werkgroepen. Ali Ougajou is manager bij KPMG IT Advisory en houdt zich bezig met vraagstukken op het snijvlak van organisatie en informatietechnologie, voornamelijk gericht op IT-assurance, informatiebeveiliging en dataprivacy. Maurice Koetsier is manager bij KPMG IT Advisory en richt zich op vraagstukken op het gebied van data privacy, informatiebeveiliging en data management. Bij NOREA is hij actief in de werkgroep Privacy.