MANAGEN VAN PRIVACYCOMPLIANCE

*Jeroen Terstegge**

In het voorstel voor de Algemene Verordening Bescherming Persoonsgegevens (2012/0011 COD) worden een aantal beheersmaatregelen *(accountability controls)* voorgeschreven, zoals een documentatieplicht, het uitvoeren van Data Protection Impact Assessments en het aanstellen van een functionaris voor de gegevensbescherming (DPO). Dit artikel geeft een overzicht van mogelijke beheersmaatregelen die organisaties kunnen nemen om privacycompliance te organiseren.

In het voorstel van de Commissie moeten de meeste maatregelen worden geïmplementeerd ongeacht of de betreffende verwerkingen in de organisatie risico's voor de betrokkene inhouden of niet. Voor zover er al uitzonderingen gelden voor deze verplichtingen, worden deze opgehangen aan het aantal werknemers in de onderneming (< 250 werknemers) of op basis van een arbitrair lijstje van hoge risico-verwerkingen. Deze benadering wordt door velen – terecht – bekritiseerd. Het verplicht opleggen van dergelijke beheersmaatregelen mag immers alleen worden gerechtvaardigd door de aanwezigheid van significante risico's voor de door de Verordening beschermende belangen van de betrokkene. Het verplicht opleggen van beheersmaatregelen zou dan al snel leiden tot onevenredige compliance-lasten voor de organisatie. Ook creëren dergelijke verstekkende verplichtingen een onredelijke verwachting dat een organisatie in al haar haarvaten compliant is met de wet. Voor zover dat überhaupt al mogelijk is (veel kleinere gegevensverwerkingen, zoals de opslag van documenten op draagbare media, bijlagen bij e-mail of de inhoud van Sharepoints, vallen buiten het toezicht door het management), is 100% compliance met Europees dataprotectierecht ook een buitengewoon kostbare operatie. Ook is de omvang van een onderneming nauwelijks een factor van belang voor de omvang van de risico's. Sterker, door bepaalde verplichtingen wel aan grote, maar niet aan kleine ondernemingen op te leggen, worden grotere ondernemingen gehouden aan een hogere beschermingsstandaard dan het midden- en kleinbedrijf. Dat verhoudt zich slecht tot het grondwettelijke karakter van het gegevensbeschermingsrecht alsook met het gelijkheidsbeginsel.

Compliance moet je organiseren

Volgens de Europese Commissie bespaart het Europese bedrijfsleven zo'n 2,4 miljard euro per jaar door vermindering van administratieve lasten.[1] Echter, dit laat zien dat de wetgever weinig oog heeft voor de zogeheten 'nalevingskosten' van een wet. Traditioneel worden deze nalevingskosten namelijk niet meegerekend in de administratieve-lastenberekening bij een wetsvoorstel. De wetgever vindt nalevingskosten vanzelfsprekend. Er wordt in het voorstel voor de Verordening daarom nauwelijks aandacht besteed aan de kosten die gemoeid zijn met de naleving van de wet. Er zijn wel

* mr.drs. **Jeroen Terstegge** CIPP is directeur van adviesbureau PrivaSense en hoofdredacteur van dit tijdschrift. Daarnaast is hij trainer in de *Certified Information Privacy Professional (CIPP)* en het *Certified Information Privacy Manager (CIPM)* programma's van de International Association of Privacy Professionals (IAPP). In het verleden was hij onder meer als Corporate Privacy Officer bij Philips verantwoordelijk voor compliance met de (internationale) privacywetgeving. Hij is bereikbaar via www.privasense.nl, terstegge@privasense.nl of @PrivaSense.

1 Communication of the European Commission of 25 January 2012 (COM 2012 9), *Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century*, pag. 8.

schattingen. Zo denkt de Europese Commissie dat de nalevingskosten ongeveer een half miljard euro voor het hele Europese bedrijfsleven zijn.[2] Peter Fleischer (Google) denkt echter dat de kosten voor het bedrijfsleven onder de Verordening 10x (!) de kosten onder de huidige Richtlijn zijn.[3] En dat zonder de kosten voor boetes en sancties. Deze kosten worden vooral veroorzaakt door het feit dat op het niet-adequaat documenteren van verwerkingen een forse boete staat. Een ruwe schatting van VNO-NCW en MKB Nederland laat zien dat de nalevingskosten van de Verordening voor het Nederlandse bedrijfsleven per jaar ongeveer even hoog zijn als de totale besparingen aan administratieve lasten voor het hele Europese bedrijfsleven als begroot door de Europese Commissie. Volgens Minister Opstelten (Veiligheid en Justitie) is het Nederlandse bedrijfsleven 1,1 miljard euro ***per jaar*** kwijt aan de naleving van de Verordening als het voorstel van de Commissie ongewijzigd zou worden overgenomen.[4] Organisaties, publiek én privaat, doen er dus goed aan om alvast na te gaan denken over de vraag hoeveel compliance met de Verordening hen gaat kosten.

Compliance met de wet gebeurt niet zomaar. De enkele letter van de wet is vaak onvoldoende om mensen en organisaties tot compliance te bewegen. Dat heeft de Europese wetgever ook begrepen. Verplichtingen die hoge administratieve lasten met zich meebrengen, zoals de meldingsplicht (zie art. 27 WBP) worden dan ook moeiteloos ingeruild voor verplichte beheersmaatregelen (***actieve compliance***). Anders dan bij het strafrecht waar de dreiging met vrijheidsbeneming de meeste mensen op het rechte pad houdt (***passieve compliance***), moeten organisaties, publiek en privaat, groot en klein, compliance met het dataprotectierecht vanwege de vele positieve verplichtingen, ***organiseren.*** Van de enkele dreiging met sancties, zoals boetes of stillegging, gaat onvoldoende preventieve werking uit, simpelweg omdat een sanctie de medewerker die de wet feitelijk overtreedt meestal niet of slechts indirect raakt. Hij hoeft de boete doorgaans niet uit eigen zak te betalen; dat doen uiteindelijk de eigenaars of de aandeelhouders. Hooguit leidt een sanctie tot ontslag of andere disciplinaire maatregelen tegen de betrokken medewerker. Maar dan nog kan vaak een deel van de verantwoordelijkheid op de organisatie worden afgewenteld omdat deze onvoldoende instructies had gegeven of onvoldoende toezicht had gehouden. Kortom, een fors deel van de gevolgen van non-compliance blijft rusten bij de organisatie, zowel voor wat betreft de financiële gevolgen (boetes, dwangsommen, kosten voor aanpassingen, etc.) als qua reputatie (negatieve publiciteit, wegvallen van vertrouwen van de klant, etc). Organisaties hebben daarom een groot aantal ***incentives*** om beheersmaatregelen te nemen om compliance door hun medewerkers af te dwingen. Als de potentiële boete voor non-compliance dan ook nog eens 2% van de jaaromzet bedraagt, dan loont het om deze incentives ook om te zetten in investeringen in compliancemanagement.

Compliance controls

Om compliance te managen kunnen een aantal categorieën ***compliance controls*** worden onderscheiden:

- Risico-inventarisatie
- Beleid en procedures
- Managementverantwoordelijkheid;
- Inschakelen van deskundigen (intern/extern);
- Bewustwording en training van medewerkers;
- Monitoring, audit en rapportage;
- Incidentmanagement; en
- Handhaving.

Deze maatregelen, ook wel het ***compliance programma*** genoemd, dienen afhankelijk van de omstandigheden zoals het type gegevensverwerking en risico's voor de betrokkene en de organisatie in de juiste mix te worden geïmplementeerd in de organisatie.

Risico-inventarisatie

Alvorens beheersmaatregelen te kunnen nemen moet een verantwoordelijke eerst een risico-inventarisatie uitvoeren op zijn organisatie of bedrijfsprocessen: welke persoonsgegevens worden verwerkt, wat is de classificatie van de persoonsgegevens, hoe omvangrijk zijn de verwerkingen, welke belangen staan er voor de betrokkene op het spel, welke externe risico's zijn er (bijv. aandacht van de toezichthouder, de media, de politiek of de ondernemingsraad), welke partijen zijn bij de verwerking betrokken (medeverantwoordelijken, bewerkers), waar en hoe lang worden persoonsgegevens bewaard, etc.? Dit proces wordt ook wel ***data mapping*** of ***privacy quick scan*** genoemd. Voor specifieke gegevensverwerkingsoperaties of bedrijfsprocessen, waar het risico naar verwachting hoog is, kan het uitvoeren van een meer diepgaande ***Privacy Impact Assessment*** raadzaam zijn.

De uitkomst van de risico-inventarisatie bepaalt in principe welke maatregelen moeten worden getroffen, door wie en in welke mate. De aard van de maatregelen en mate waarin deze worden genomen kan derhalve verschillen van organisatie tot organisatie en van afdeling tot afdeling. Soms moet bijvoorbeeld meer nadruk worden gelegd op training, in andere gevallen is het

2 Impact Assessment, Commission Staff Working Paper, SEC(2012) 72, pag. 77.
3 http://peterfleischer.blogspot.nl/2012/11/the-marketplace-of-privacy-compliance.html
4 http://www.nu.nl/economie/3494256/bedrijven-miljard-kwijt-europese-regel.html

verstandig om een FG of privacy officer aan te stellen. Vanuit dat opzicht is het dan ook onbegrijpelijk dat de Verordening hoge boetes zet op de afwezigheid van specifieke beheersmaatregelen, zoals het niet hebben van een FG/DPO (maximaal 2% van de jaaromzet), het niet hebben van een procedure voor inzageverzoeken (0,5%) of het niet bijhouden van de documentatie van de gegevensverwerking (1%).[5]

Beleid en procedures

De wettelijke verplichtingen en de ambitie van de organisatie op het gebied van privacybescherming en compliance moet worden vertaald naar een op de organisatie toegesneden privacybeleid. In beginsel wordt dit beleid schriftelijk vastgelegd. Het beleid kan algemeen zijn, zoals een ***privacy mission statement*** of een ***ethics policy*** waar privacy en dataprotectie deel van uitmaakt, ***Binding Corporate Rules*** (BCRs) of een (sectorale) privacygedragscode. Maar het kan ook meer specifiek en gedetailleerd beleid zijn dat ziet op bepaalde aspecten van de gegevensbescherming of de privacy en gegevensbescherming in specifieke bedrijfsprocessen. Denk bijvoorbeeld aan een informatiebeveiligingsbeleid, een opt-in beleid voor direct-marketing, een beleid voor de afhandeling van privacyklachten en inzageverzoeken, een outsourcingsbeleid of een auditbeleid. Ook kan aanvullend beleid worden geformuleerd voor een of meer specifieke verwerkingen, zoals een privacybeleid voor klantgegevens, bewakingscamera's of personeelsdossiers. In zo'n specifieke privacy policy worden onder meer de doeleinden van de verwerking vastgelegd, de rollen aangewezen die toegang tot de gegevens mogen hebben, specifieke beveiligingsmaatregelen vastgesteld en de bewaartermijnen vastgelegd.
Opgemerkt moet worden dat een goed privacybeleid niet hetzelfde is als het 'privacybeleid' ex artikel 33 WBP dat men vaak op websites aantreft. Dat laatste is eigenlijk niet meer dan een 'privacyverklaring' (in het Engels: ***privacy notice***), waarin de voor de betrokkene relevante ***samenvatting*** van het privacybeleid van de organisatie wordt gepresenteerd.[6] Het echte privacybeleid is vaak veel omvangrijker en bevat vaak gedragsnormen en instructies voor personeel alsmede allerlei interne procedures. Dit soort informatie wordt niet naar buiten toe gecommuniceerd.
Naast beleid zijn er procedures nodig om het beleid te implementeren en non-compliance te voorkomen. Dergelijke procedures kunnen het beleid zelf betreffen, zoals een periodieke evaluatie van het beleid of het vragen van periodieke managementverklaringen dat het beleid daadwerkelijk is geïmplementeerd. Maar de procedure kan ook bepaalde aspecten van de gegevensbescherming betreffen, zoals een procedure voor de afhandeling van inzage- en correctieverzoeken, een procedure voor het melden van beveiligingsincidenten, een procedure voor het beoordelen van de betrouwbaarheid van een bewerker, een procedure voor het toekennen van rollen aan personen in de organisatie of het beëindigen daarvan, een procedure voor het vaststellen van privacyrisico's (PIA), of een procedure voor het updaten en verwijderen van gegevens.

Managementverantwoordelijkheid

Het managen van compliance begint met het beleggen van verantwoordelijkheden. Vanuit ondernemingsrechtelijk perspectief ligt de (eind)verantwoordelijkheid voor compliance per definitie bij de directie van de organisatie. De directie treedt immers op namens de 'verantwoordelijke', waarop formeel de verplichtingen van de wet rusten (zie ook art. 15 WBP).
Deze categorie valt uiteen in een aantal onderdelen:

- Het management moet zich op de hoogte stellen van de geldende regels en inzicht hebben in de inhoud van het complianceprogramma;
- Het management moet toezicht houden op de effectiviteit en implementatie van het complianceprogramma; en
- Waar de verantwoordelijkheid voor het toezicht en implementatie wordt gedelegeerd, moet die worden belegd bij een of meer senior medewerkers, bijvoorbeeld een executive met de titel Chief Privacy Officer.

Het complianceprogramma moet periodiek worden geëvalueerd en waar nodig worden bijgesteld, bijvoorbeeld omdat de regelgeving is veranderd of omdat blijkt dat het programma onvoldoende werkt. Waar de verantwoordelijkheid is gedelegeerd, is het verstandig om belangrijke bijstellingen voor te leggen aan de directie, omdat die steeds de eindverantwoordelijkheid heeft. In veel organisaties is het gebruikelijk om in ieder geval minimaal 1x per jaar de belangrijke beleidsdocumenten, waartoe soms ook het privacybeleid behoort, in de directie te bespreken om te kijken of bijstelling nodig is.

Inschakelen van deskundigen

Je kunt niet overal verstand van hebben, ook niet van privacy en gegevensbescherming. Daarom is het soms nodig om een deskundige te raadplegen. Iemand die verstand heeft van de WBP en het overige privacyrecht; of verstand heeft van informatiebeveiliging; of van de privacyaspecten van direct marketing, outsourcing,

5 Wat dat betreft zijn de *United States Sentencing Guidelines for Organizations (USSG, Chapter 8)* logischer. De USSG werken met een verwijtbaarheidsscore. De basisscore kan worden verhoogd door bijvoorbeeld eerder feiten of het frustreren van het onderzoek, maar de score kan ook worden verlaagd, zoals in geval van het hebben van een effectief complianceprogramma.

6 Nog even daargelaten dat veel privacy policies op websites alleen zien op de verwerkingen via de website zelf en dus een hele beperkte scope hebben.

fusies en overnames, personeelsmanagement, etc. Die deskundige kan intern worden aangesteld, zoals een privacy officer of FG (DPO), een bedrijfsjurist, een ICT-er met verstand van informatiebeveiliging, een internal auditor of een speciaal opgeleide medewerker in de afdeling.[7] Maar de deskundigheid kan ook extern worden gehaald, bijvoorbeeld bij een consultant of advocaat.
Het is belangrijk om te beseffen dat deze deskundigen *niet* verantwoordelijk zijn voor privacybescherming en dataprotectie. Die verantwoordelijkheid rust bij het management van de organisatie zelf. De deskundige is de zogeheten *tweede lijn* (de auditor is zelfs de derde lijn). De eerste lijn is en blijft het management. Het is dan ook verkeerd om bijvoorbeeld de FG of de privacy officer te belasten met de verantwoordelijkheid voor compliance met de WBP. De FG of de privacy officer houdt toezicht op de samenstelling en uitvoering van het complianceprogramma, adviseert het management bij de formulering van het privacybeleid, geeft privacytrainingen, treedt op als deskundige in specifieke casus, behandelt klachten en is betrokken bij onderzoeken naar incidenten en onderzoeken van de toezichthouder.
Wel zie je soms dat een *Chief Privacy Officer (CPO)*, vaak een senior executive, zowel de gedelegeerde managementverantwoordelijkheid draagt (zie vorige paragraaf) als de benodigde deskundigheid organiseert (in grote organisaties heeft de CPO vaak een team van specialisten beschikbaar). Daarnaast treedt de CPO vaak naar buiten als het gezicht van het privacybeleid van de organisatie, bijvoorbeeld richting toezichthouders, de politiek of de pers.
Interne deskundigen moeten hun kennis bijhouden. De WBP eist bijvoorbeeld dat de FG deskundig is (zie art. 63 lid 1 WBP). Dat betekent dat zij door hun werkgever in de gelegenheid moeten worden gesteld om extern trainingen te volgen, certificeringen te behalen, vakliteratuur te lezen en/of lid te worden van professionele verenigingen en (onder werktijd) hun bijeenkomsten bij te wonen. Daarvoor moet de werkgever een apart budget beschikbaar stellen. Dat laatste is niet altijd vanzelfsprekend omdat zo'n budget vaak onderdeel is van een groter budget (bijv. het budget van de juridische afdeling), waardoor de financiële behoeften van het privacyteam dreigen onder te sneeuwen.

Bewustwording en training

Beleid en procedures hebben is één, maar deze zijn niets waard als de medewerkers niet weten dat het beleid bestaat, onvoldoende op de hoogte zijn van de procedures of onvoldoende oog hebben voor privacy en gegevensbescherming. Met behulp van *awareness* campagnes kan de bewustwording voor privacy, gegevensbescherming en compliance worden verhoogd. Dat kan een groots opgezette campagne zijn, compleet met posters en gadgets, maar ook kan het top- en lijnmanagement in toespraken en werkoverleg regelmatig aandacht besteden aan het belang van privacybescherming en dataprotectie. Medewerkers die veel met persoonsgegevens werken worden idealiter getraind in het privacybeleid van de organisatie en de geldende procedures. Deze training wordt zoveel mogelijk toegesneden op de taken van de afdeling of de medewerker. Waar nodig wordt de training periodiek herhaald.

Monitoring, audit en rapportage

Documentatie en controle zijn belangrijke pijlers van een goed privacy compliance programma. Niet alleen moeten het beleid en de procedures alsmede het datamodel (data elementen, doeleinden, autorisaties en bewaartermijnen) zijn vastgelegd, ook de rapportages die voortvloeien uit monitoring, audits en incidenten moeten worden vastgelegd.
Uiteraard moet de naleving van de wet, het beleid en de procedures worden gecontroleerd (*monitoring*). Daarvoor zijn zogeheten *metrics* of *key performance indicators, KPI's* nodig. Het staat de organisatie vrij om te bepalen welke metrics wenselijk zijn. Men kan bijvoorbeeld denken aan het meten van het aantal incidenten, het aantal inzageverzoeken, het aantal privacytrainingen, het aantal klachten over spam, het aantal en type onderzoeken door toezichthouders, etc. Meer geavanceerde metrics zijn bijvoorbeeld het meten van de klanttevredenheid met betrekking tot het privacybeleid van de organisatie, het meten van de toegevoegde waarde van het privacybeleid op de omzet van het bedrijf, etc.
Uiteraard is het wenselijk dat de compliance periodiek getoetst wordt. Auditrapporten worden in beginsel gemaakt voor het management van de betreffende organisatie of afdeling. Het verdient aanbeveling om de rapporten ook te delen met de portefeuillehouder voor privacy en compliance alsmede met de privacy officer of de FG. Waar nodig wordt de audit extern uitgevoerd.
Niet onbelangrijk is ook het periodiek auditen van de bewerkers. Dit volgt ook uit de verplichting voor de verantwoordelijke ex artikel 14 lid 1 WBP om toezicht te houden op de naleving van de beveiligingsmaatregelen.
Zowel de portefeuillehouder als de privacy officer of de FG rapporteren periodiek (in ieder geval 1x per jaar) aan de directie hoe het staat met de naleving van het beleid. Daar waar privacy officers voor afzonderlijke onderdelen van de organisatie zijn benoemd, rapporteren deze aan het management van dat onderdeel. Daarnaast rapporteren zij periodiek aan de Chief/Group Privacy Officer of FG.

Incidentmanagement

Incidenten komen helaas voor. Niet alleen op het gebied van beveiliging (datalekken), maar ook op het

7 Zo iemand krijgt vaak de naam *privacycoördinator, privacy lead,* of *privacy champion* en heeft naast privacy vaak ook nog de 'gewone' taken van de afdeling in zijn functieomschrijving. Deze persoon heeft een signaal- en kennisfunctie en werkt vaak als verlengstuk van het management van de afdeling die uiteraard verantwoordelijk blijft voor privacycompliance.

gebied van compliance. Denk bijvoorbeeld aan het niet tijdig geven van inzage, het niet reageren op een opt-out verzoek, het versturen van reclame e-mail zonder toestemming, het gebruik van gegevens voor een onverenigbaar doel, het langer bewaren van persoonsgegevens dan toegestaan of het doorgeven van persoonsgegevens naar het buitenland zonder modelcontract. Incidenten moeten geadresseerd worden zodra ze bekend zijn geworden. Soms kan dat eenvoudig door het nemen van de ontbrekende maatregelen of het alsnog terstond voldoen aan een verzoek, maar soms is er meer aan de hand en moet onderzoek gedaan worden en/of aanvullende maatregelen worden genomen om te voorkomen dat een dergelijk incident weer gebeurt. Het is van belang dat incidenten zo snel mogelijk worden gerapporteerd bij een daarvoor getrainde medewerker, bij voorkeur via een daartoe ingerichte procedure. Waar en hoe een incident wordt gerapporteerd, is afhankelijk van het soort incident en de ernst van het incident.[8] In principe kan iedere klacht van een betrokkene, over welk onderwerp dan ook, een privacyincident blootleggen. Denk bijvoorbeeld aan iemand die klaagt dat een product niet is geleverd. De achterliggende oorzaak blijkt vervolgens te zijn dat het bestelformulier ergens in de winkel is blijven slingeren. In dat geval is er sprake van: 1) onzorgvuldige omgang met persoonsgegevens bij de bestelling, en 2) een mogelijk datalek omdat ongeautoriseerde derden mogelijk inzage hebben gehad in het formulier. Getrainde medewerkers kunnen (waarschijnlijk) zulke verbanden leggen.
Om incidenten te kunnen managen, is een zogeheten *incident response plan* nodig. Een dergelijk plan bevat onder meer de volgende stappen:

- Beperking van de gevolgen van het incident;
- Een risicoanalyse;
- Eventuele meldingsplichten;[9]
- Het onderzoek naar de oorzaak;
- De te nemen mitigerende maatregelen;
- De te nemen preventieve maatregelen.

Het is van het grootste belang dat een incident niet groter wordt dan het al is. Beperken van de gevolgen is derhalve de eerste prioriteit. Daarnaast dient zo snel mogelijk een (eerste) inschatting van de risico's te worden verkregen. Waar nodig of wettelijk verplicht, wordt het incident gemeld bij de betrokkene en/of de bevoegde autoriteiten in binnen- en buitenland. Het is van belang dat eventuele termijnen zorgvuldig in acht worden genomen en alle vereiste informatie over het incident wordt aangeleverd. Uiteraard dient vervolgens een meer diepgaand onderzoek naar de oorzaak van het incident te worden ingesteld: wat ging mis, waarom, wie was daarvoor verantwoordelijk, enzovoorts. Waar nodig worden mitigerende maatregelen genomen. Die kunnen bijvoorbeeld bestaan uit het nemen van aanvullende beveiligingsmaatregelen, het alsnog voldoen aan het verzoek, het blokkeren van e-mailadressen voor mailings, het op orde brengen van formaliteiten zoals meldingen, vergunningen of contracten en indien nodig het terstond beëindigen van de relatie met de betreffende bewerker. Ten slotte worden waar nodig maatregelen genomen om te voorkomen dat een dergelijk incident zich weer voordoet. Na sluiting van het incident moet er zo spoedig mogelijk een evaluatie plaatsvinden en *lessons learned* worden getrokken.

Daarnaast bevat een incident response plan instructies met betrekking tot:

- De verdeling van taken en verantwoordelijkheden met betrekking tot incidenten;
- De personen die onderdeel moeten zijn van het *incident response team*;
- De informatie die moet worden verkregen over het incident;
- De wijze waarop een incident wordt gerapporteerd;
- De omstandigheden waaronder en hoe een incident moet worden geëscaleerd;
- De wijze waarop een onderzoek verloopt;
- De wijze waarop de betrokkene op de hoogte wordt gesteld van het incident;
- De wijze waarop een incident wordt gesloten en gedocumenteerd;
- De evaluatie van het beleid.

Handhaving

Sluitstuk van een goed privacybeleid is handhaving van het beleid. Dat betekent dat managers en medewerkers moeten kunnen worden aangesproken op gedrag of handelingen die in strijd zijn met de wet en het beleid. Omdat de arbeidsrechtelijke dimensie hierin een grote rol speelt, is het nodig dat het privacy-

8 Soms kunnen ernstige privacyincidenten ook gemeld worden via een intern 'whistleblowing' rapportagesysteem, zeker als privacy onderdeel is van het integriteitsbeleid van de organisatie. Daar kleven echter qua privacywetgeving weer nogal wat haken en ogen aan, zoals u kunt lezen in het artikel van Evita Sips elders in dit nummer.

9 Nu al kent de Telecommunicatiewet een meldplicht voor datalekken bij de ACM. Op 21 juni heeft het kabinet het wetsvoorstel Meldplicht Datalekken, dat verplicht tot het melden van datalekken bij het CBP, naar de Tweede Kamer gestuurd.

beleid ook wordt verankerd in de arbeidsrelatie. Dat kan bijvoorbeeld door hiervoor bepalingen op te nemen in de arbeidsovereenkomst zelf, door het privacybeleid onderdeel te maken van het integriteitsbeleid van de organisatie of door het beleid als een algemene instructie aan het personeel uit te vaardigen. Waar privacy en gegevensbescherming van essentieel belang zijn voor de organisatie, zal overtreding van het privacybeleid of de geldende wettelijke regels tot disciplinaire maatregelen moeten leiden, waaronder eventueel ontslag.
Niet alleen moet het beleid worden gehandhaafd jegens medewerkers, maar ook jegens de bewerkers. Waar kleine overtredingen meestal aanleiding zijn voor aanscherping van het toezicht (bijvoorbeeld door het uitvoeren van een audit of verhogen van de rapportagefrequentie), dienen grove schendingen te leiden tot contractuele boetes of zelfs tot beëindiging van de overeenkomst. Het is dan ook van belang dat de bewerkersovereenkomst bepalingen bevat die de verantwoordelijke de bevoegdheid geven om de overeenkomst te ontbinden in geval van wanprestatie op het gebied van bescherming van persoonsgegevens.

Maturity levels

De maatregelen moeten *effectief* zijn; zij moeten rechtstreeks bijdragen aan de vermindering van het risico op non-compliance. 'Window dressing' is uit den boze. De effectiviteit van maatregelen is mede afhankelijk van het *maturity level* van het complianceprogramma. Volgens het GAPP-rapport[10] kan een privacy-maturity-model er al volgt uitzien:

Initial

De organisatie heeft geen privacybeleid of procedures vastgesteld. Er zijn ongecoördineerde compliance-activiteiten op een laag niveau (bijv. bedrijfsjuristen, IT). Activiteiten overlappen elkaar, er is gebrek aan teamwork en betrokkenheid.

Repeatable

Er is een privacybeleid vastgesteld. Hoger management is enigszins betrokken. Er is enig privacybewustzijn in de organisatie. Er bestaan plannen voor privacycompliance in delen van de organisatie met een hoog risico.

Defined

Er is een privacybeleid vastgesteld en verantwoordelijkheden zijn benoemd. Er worden risico-assessments uitgevoerd. Er vindt een prioritering in de aanpak plaats en middelen worden conform deze prioriteiten toegewezen. Er vinden activiteiten plaats om beheersmaatregelen op het gebied van privacycompliance en gegevensbescherming te coördineren en te implementeren.

Managed

De organisatie heeft een consistent niveau van privacycompliance management en privacyeisen. In een vroeg stadium van ontwikkeling en implementatie van processen en systemen wordt rekening gehouden met privacy en gegevensbescherming (*Privacy by Design / Data Protection by Design*). Privacy is geïntegreerd in functiebeschrijvingen en beoordelingscriteria van medewerkers. Er vindt monitoring van compliance en gegevensbescherming plaats, zowel op organisatie- als op functioneel niveau.

Optimizing

Er vindt continu verbetering plaats van privacybeleid, uitvoering, en beheersmaatregelen. Wijzigingen in processen en systemen worden systematisch gecheckt op hun impact op privacy en gegevensbescherming. Er zijn aparte personen en middelen toegewezen om de doelstellingen van de organisatie op het gebied van privacy en gegevensbescherming te verwezenlijken. Er is sprake van een hoog niveau van functionele integratie en teamwork om die doelstellingen te halen. Het is ondoenlijk om in één klap van Initial naar Optimizing te gaan. Privacycompliance is een reis in volwassenheid; langzamerhand wordt de organisatie daar weer een beetje beter in. Niettemin kan het zinvol zijn om doelstellingen te formuleren met betrekking tot het gewenste maturity level. Op die manier dwingt de organisatie zichzelf om kritisch te blijven kijken naar haar processen.

Tot slot

De nieuwe Europese Verordening bevat voorschriften die organisaties dwingen tot een redelijk hoog maturityniveau. Immers, op het niet naleven van de *accountabilty controls* staan stevige boetes (tot 2% van de wereldwijde bruto jaaromzet). Organisaties doen er dus goed aan om vroegtijdig te beginnen met het ontwikkelen en implementeren van hun privacycompliance programma. De overgangstermijn van de Verordening (er wordt voorgesteld 2 jaar) moet dan ook zo goed mogelijk worden benut om op tijd klaar te zijn voor de Verordening.

10 GAPP staat voor *Globally Accepted Privacy Principles*. Deze zijn uitgewerkt in de Global Technology Audit Guide 5 van het Institute of Internal Auditors (IIA), *Managing and auditing privacy risks*, Juni 2006.