Duthler Associates
law, ICT & organisation

Factsheet

Privacy implementatie en beheer

Wat is de verwachtingskloof?

De dagen dat het beschermen van persoonsgegevens bij bedrijven geïmplementeerd moest worden zijn voorbij. Bedrijven hebben omvangrijke investeringen in opleidingen gedaan, maar hebben nagelaten kennis- en verandermanagement te organiseren en structurele maatregelen in de bedrijfsprocessen "by design" op te nemen. Bedrijven wensen geen budgetten vrij te namen voor het beschermen van persoonsgegevens; het moet onderdeel zijn van andere processen zoals riskmanagement en compliancemanagement. Bovendien zijn er slimme IT-systemen nodig om effectieve beheersmaatregelen te treffen en de operationele kosten binnen de perken te houden.

De Europese toezichthouders blijven richtlijnen uitgeven waarin de verplichtingen uit de Europese Algemene Verordening Gegevensbescherming (AVG) nader worden uitgelegd, zie Guidelines, Recommendations, Best Practices. Wat in de uitleg van de toezichthouders opvalt zijn de verstrekkende beheers- en beschermingseisen.

In haar Focus AP 2020 – 2023 legt de Autoriteit Persoonsgegevens accenten voor toezicht op het effectief beschermen van persoonsgegevens. Wij zien een reeks van boetes bij met name overheidsorganisaties, zie boetes en andere sancties. Uit de jaarverslagen van de AP is het overigens moeilijk een eenduidig beeld te destilleren van de stand bij bedrijven van het georganiseerd zijn voor effectief beschermen van persoonsgegevens.

Bij het organiseren van het effectief beschermen van bedrijfsgeheimen verwacht de rechter een inventarisatie van de bedrijfsgeheimen, een overzicht van de beheersmaatregelen en het bewijs dat de maatregelen effectief hebben gewerkt.

Bij het concretiseren van de wettelijke AVG-eisen door bedrijven en toezichthouders is een verwachtingskloof ontstaan. Dit geldt ook voor bedrijven en rechters bij het beschermen van bedrijfsgeheimen.

Implementatie en het onderhoud

Na verloop van tijd (bijvoorbeeld na drie tot zes jaar) is een beoordeling van de ingerichte organisatie van het effectief beschermen van persoonsgegevens nodig. Het gaat om de volgende toetsing:

- Voldoet de implementatie aan de richtlijnen (guidelines) van de toezichthouders;
- Worden de persoonsgegevens daadwerkelijk effectief beschermd (en waar blijkt dat uit);
- Wat zijn de signalen uit de eigen organisatie en die van partners?
- Kan het beschermen van persoonsgegevens worden verruimd naar het beschermen van persoonsgegevens én bedrijfsgeheimen?

- Zetten wij effectief IT-middelen voor het beschermen van persoonsgegevens (en bedrijfsgeheimen) in en welke zijn op de markt? *en*
- Wat zijn de waardeproposities, businessplannen en realistische plannen van aanpak voor het realiseren van de veranderingen.

Wij kunnen een dergelijk onderzoek zien als een nulmeting of DPIA. De relevante wetgeving én de richtlijnen van de Europese toezichthouders vormen de basis voor de baselines. Bovendien is het uitdrukkelijk de bedoelen een toegankelijke businesscase op te stellen waar niet alleen de noodzaak voor veranderen uit blijkt maak ook de waardeproposities voor het bedrijf.

IT-ondersteuning

Leveranciers van IT-clouddienstverlening zoals Microsoft, Amazon en Google voorzien in rollen voor de riskmanager, compliance officer en functionaris voor de gegevensbescherming (FG). De rollen bezitten bevoegdheden die toegang geven tot functionaliteiten waarmee de FG zich een indruk kan vormen over de effectiviteit van de getroffen beheersmaatregelen. Bepaalde licentietypen geven de FG toegang tot een privacy-administratie (bijvoorbeeld Priva) waarmee het gewenste overzicht en inzicht in de wettelijke verplichtingen worden verkregen. Voorwaarde is wel dat het beheer van de IT-cloud van een bedrijf adequaat moet zijn en de rollen van riskmanager en compliance officer bemenst zijn.

Wat is onze aanpak?

Wij passen steeds de opleiding voor functionaris voor gegevensbescherming en aanpalende trainingen aan voor nieuwe wetgeving en de interpretaties van wetgeving door de toezichthouders. Wij kennen de impact van nieuwe wetgeving en interpretaties van toezichthouders op het organiseren van bedrijfsactiviteiten.

Ziet een bedrijf de interpretaties van het wettelijk kader als een plicht dan kunnen wij ons voorstellen dat “de moed in de schoenen zakt”. Het is ook mogelijk de richtlijnen van de toezichthouders vanuit het perspectief van bedrijfsvoering te bekijken. Dit breder perspectief biedt kansen de bedrijfs- en persoonsgegevens en ook de bedrijfsgeheimen effectief te organiseren en tegelijkertijd de aansprakelijkheids- en kostenrisico’s beheersbaar te houden.

Aan het plan van aanpak implementatie volgende fase beschermen bedrijfs- en persoonsgegevens en bedrijfsgeheimen ligt een businesscase ten grondslag.

Implementatie

Uitgaande van de organisatie van de bedrijfsactiviteiten, de signalen van medewerkers bedrijfsprocessen effectiever te organiseren en de inschatting dat medewerkers bereid zijn de bedrijfsprocessen stellen wij een plan van aanpak op. Het plan van aanpak met duidelijke mijlpalen en producten bespreken wij met de bedrijfsleiding en het afdelingsmanagement. Na een akkoord voeren wij het plan in samenwerking met de medewerkers uit.

De implementatie kan betrekking op verschillende aandachtspunten. In het algemeen kunnen wij noemen:

1. Overzicht en inzicht creëren verantwoordelijkheidsdomein van entiteiten en samenwerkingsverbanden;
2. Met behulp van de bedrijfsjuridische functie met partners (klanten, medewerkers en leveranciers), op een systematische wijzen, regie- en verwerkersovereenkomsten afspreken en het contractmanagement inrichten;

3. Uitgaande van de organisatie van bedrijfsactiviteiten verwerkingen van persoonsgegevens en bedrijfsgeheimen inventariseren en vastleggen, de beheersmaatregelen documenteren en het bewijs van effectieve werking verzamelen;
4. Incidenten als gevolg van het doorbereken van beheers- en beveiligingsmaatregelen vastleggen en al dan niet gedocumenteerd promoveren tot datalekken;
5. Continu medewerkers bewustmaken en trainen;
6. Beheersmaatregelen gericht op beschermen van persoonsgegevens “by design” opnemen in de bedrijfsprocessen waarmee de bedrijfsactiviteiten georganiseerd zijn; en
7. Gericht en inzichtelijk samenstellen van management rapportages.

De scope van de te zetten stappen is het beschermen van bedrijfs- en persoonsgegevens en bedrijfsgeheimen. Het beschermen van gegevens is procesmatig georganiseerd en wordt ondersteund IT-middelen.

Onderhoud

De projectleider belegt de resultaten van de implementatie in de bedrijfsorganisatie. Het afdelingsmanagement en medewerkers nemen de sturing over en zorgen voor het onderhoud. Periodiek stelt de bedrijfsleiding het management en medewerkers in staat kennis te nemen van nieuwe ontwikkelingen op het vlak van het beschermen van persoonsgegevens en bedrijfsgeheimen.

Meer informatie

Het om de drie jaar beoordelen van de organisatie van het beschermen van gegevens leidt veelal tot nieuwe inzichten. Aan de ene kant de constatering van een verwachtingskloof en aan de andere kan de kansen de bedrijfsactiviteiten effectiever te organiseren.

Neem gerust contact met ons op via +31 (0) 70 392 22 09 of info@duthler.nl.

Duthler Associates
law, ICT & organisation

Afspraak maken en contact

Wilt u meer weten? Neem dan contact op met ons op via de onderstaande gegevens. Of bezoek onze website: www.duthler.nl

Kantoor:

Frankenslag 137

2582 HH Den Haag

+31 (0) 70 392 22 09

info@duthler.nl