ICT Academy

Whitepaper

Privacybescherming; nuttig en noodzakelijk

www.iir.nl

Privacybescherming; nuttig en noodzakelijk

Privacy is een ongedefinieerd, moeilijk tastbaar begrip. Als we spreken over de bescherming van persoonsgegevens, dan betreft dit de 'informationele privacy'. In Nederland kennen we namelijk geen 'wet op de privacy' maar beschikken we sinds 2001 over de Wet bescherming persoonsgegevens (Wbp). Deze wet is van toepassing op geautomatiseerde verwerkingen van persoonsgegevens en op sommige vormen van niet geautomatiseerde verwerkingen.

PRIVACYBESCHERMING, SO WHAT?

Wat hebben organisaties aan privacy? Het antwoord hierop is: heel veel. Privacybescherming schept vertrouwen. Een organisatie die zorgvuldig omgaat met de aan haar toevertrouwde persoonsgegevens, straalt vertrouwen uit. Dat vereist transparant handelen en waarborgen bieden aan degenen wiens persoonsgegevens het betreft. Regel je dit goed als organisatie, dan kun je daarmee reputatieschade voorkomen. Privacybescherming bewerkstelligt ook dat een organisatie de eigen werkprocessen inzichtelijk inricht en ze daarmee beheersbaar maakt. Goede informatiebeveiliging en adequaat autorisatiebeheer staat of valt immers met het al dan niet aanwezig zijn van witte of zwarte vlekken. De witte vlekken staan voor de 'gaps' die wel gesignaleerd zijn, maar nog niet verholpen en de zwarte vlekken staan voor de nog onbekende 'gaps' in de processen, met bijbehorende risico's tot gevolg. Privacybescherming gaat echter verder dan het zorgvuldig omgaan met persoonsgegevens. Privacybescherming zorgt ook voor de inbedding van een aantal grond- en mensenrechten, zoals het recht op gelijke behandeling en het recht op bescherming van de persoonlijke levenssfeer. Privacybescherming is bovendien een middel om organisaties een integere bedrijfsvoering te laten hebben. Met vertrouwen, transparantie, beheersbaarheid en een goed fatsoen ben je een heel stap in de goede richting om 'onkreukbaar' en 'eerlijk' te zijn.

PRIVACYBESCHERMING DRINGT DOOR TOT IN DE KERNPROCESSEN

Om te beginnen raakt de Wbp bijna alle processen binnen organisaties. Van de werving en selectie van personeel, het gebruik van een wereldwijd personeelssysteem (doorgifte naar derde landen!), het invoeren van personeelsreglementen waarvoor de instemming van de ondernemingsraad noodzakelijk is, het toepassen van marketing, het gebruik van de bedrijfswebsite, het gebruik van social media en cloud applicaties, het gebruik van 'Big Data', het samenwerken met andere (keten)organisaties, de inrichting van ICT, controle van personeel, het gebruik van personeelsinformatiesystemen, fraudepreventie, tot cameratoezicht en nog veel meer. Maar denk ook eens aan de informatiebeveiliging van de bergen gegevens die binnen organisaties opgeslagen liggen. Informatiebeveiliging vloeit bijvoorbeeld voort uit artikel 13 Wbp. Transparantie wordt gewaarborgd door onder andere de artikelen 33 en 34 (informatieverplichtingen) en 35 (het inzagerecht) Wbp. Het recht van verzet tegen (online) marketing vloeit voort uit artikel 41 Wbp.

WAAR TE BEGINNEN?

De toezichthouder – het College bescherming persoonsgegevens (Cbp) –heeft een aantal compliance-instrumenten ontwikkeld die gebruikt kunnen worden voor zelfregulering:

- *een quickscan:* hulpmiddel voor het bevorderen van het privacybewustzijn in de organisatie van de verantwoordelijke. De quickscan helpt ook om te bepalen wat de plaats van de organisatie is op de kwaliteitsschaal van de gegevensverwerking;
- *een Wbp Zelfevaluatie:* hulpmiddel bij het verkrijgen van inzicht in het toepassen van de Wbp in de organisatie van de verantwoordelijke en het eveneens nader bepalen van de plaats van de organisatie op de kwaliteitsschaal van de gegevensverwerking; Raamwerk Privacy Audit: basis voor het beoordelen van de kwaliteit van de bescherming van persoonsgegevens over de gehele verwerkingsketen;
- *een Handreiking bij het Raamwerk Privacy Audit:* handreiking bij het beoordelen van de kwaliteit van de bescherming van persoonsgegevens over de gehele verwerkingsketen. De handreiking is gebaseerd op het Raamwerk Privacy Audit en geeft aan hoe een concretisering van de wettelijke norm kan plaatsvinden. Ook marktpartijen hebben instrumenten ontwikkeld, zoals het Privacy Governance Raamwerk (Capgemini), dat elementen combineert van al bestaande (IT-) governancemodellen voor interne controle en interne beheersing, zoals COSO, CobiT, ITIL, ASL/BiSL. Of het Information Security Governance Model, aangevuld met best practice-ervaringen. Of een privacyvolwassenheidsmodel (Mitopics), dat aansluit bij modellen die zich richten op het inrichten en vormgeven van organisaties.

PRIVACY RISK APPETITE

Het is geen sinecure om alle aspecten van de Wbp adequaat te implementeren. De normen in de Wbp zijn veelal open en vaag geformuleerd. 'Proportionaliteit', 'subsidiariteit' en 'noodzakelijkheid' zeggen een doorsnee jurist al weinig, laat staan een niet-jurist. De formele verplichtingen van de wet

zijn nu nog weliswaar eenvoudig na te leven (meldplicht openbaar register van gegevensverwerkingen), maar de pakkans is laag (kleine toezichthouder) en de sancties zijn vooralsnog mild (boete voor niet melden of bestuursdwang voor materiële schendingen van de Wbp). De verleiding om niets te doen was dus vaak aanwezig. Met een schuin oog op de ontwikkelingen rondom privacyregelgeving, biedt implementatie van de Wbp echter ook kansen. Als 'business enabler' om processen inzichtelijker en beter beheersbaar te maken, als instrument om organisaties te veranderen en een uitgesproken gelegenheid om na te denken over de na te streven moraal binnen organisaties. Privacybescherming is daarmee een wezenlijk onderdeel geworden van een goede risk governance.

ONTWIKKELINGEN PRIVACYREGELGEVING

Privacy staat steeds meer in de belangstelling van de media. Deels komt dit door wat een groeiende toename aan privacy gerelateerde incidenten lijkt te zijn, deels komt dit ook door de verhoogde aandacht binnen de politiek voor privacy. In 2014 wordt een aantal wetsvoorstellen behandeld: het wetsvoorstel meldplicht datalekken, het wetsvoorstel tot aanpassing van de cookiewet en het wetsvoorstel tot intrekking van de bewaarplicht van communicatiegegevens. Ook is in mei 2014 door het Europese Parlement een tekst aangenomen die moet leiden tot de totstandkoming van een Europese Privacy Verordening. Deze ontwikkelingen zullen niet alleen leiden tot een nieuw en nog meer gereguleerd privacylandschap door de verwachte invoering van een verplichte privacy officer voor het merendeel van de organisaties in Nederland, een documentatieplicht van verwerkingen of de verplichting tot het uitvoeren van 'privacy impact assessments' bij de inrichting van processen, om maar enkele aansprekende verplichtingen te noemen. Ook is een verruiming van toezichthoudende bevoegdheden aanstaande door onder meer verstrekkende boetebevoegdheden.

DE PRIVACY OFFICER 2.0 / FUNCTIONARIS GEGEVENSBESCHERMING

De Wbp biedt de mogelijkheid om een functionaris voor de gegevensbescherming (FG) aan te stellen. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wbp. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie, vergelijkbaar met die van leden van de ondernemingsraad. Daarnaast is het ook mogelijk om een privacy officer te benoemen. Deze persoon heeft veelal dezelfde taken als een FG, met dien verstande dat een privacy officer zijn werkzaamheden niet in een wettelijk verankerde onafhankelijkheid vervult. Voor beide rollen geldt dat ze in beweging zijn. Zijn privacy officers bijvoorbeeld eigenlijk compliance officers of moeten compliance officers ook een privacy officer zijn? Is het een meedenkende jurist of juist meer een gedragswetenschapper of organisatiepsycholoog? De rol van de privacy officer van vandaag en van gisteren lijkt mee te moeten veranderen met de veranderende rollen binnen organisaties. Zo bezien groeit de behoefte aan een nieuw soort privacy officer: de privacy officer 2.0.

Auteur: mr. Jean Paul van Schoonhoven. Docent opleiding Privacy Officer 2.0.

Vragen

Heeft u vragen of opmerkingen naar aanleiding van deze whitepaper? Neem dan contact met ons op via info@iir.nl.