Opzetten van een privacyrisicoanalyse: be prepared!

Marit Klapwijk

Op 12 maart 2014 heeft het Europees Parlement haar standpunt over de Algemene Verordening Gegevensbescherming gepubliceerd (eerste lezing) en het gewijzigde voorstel is toen met grote meerderheid aangenomen. Hoewel het nog even zal duren voor de verordening daadwerkelijk in werking treedt, is het verstandig om hier nu al op te anticiperen. In deze verordening staan veel ingrijpende veranderingen op het gebied van privacy, die een grote impact zullen hebben op de bedrijfsvoering. Door de verordening komt privacy bij veel organisaties (weer) hoger op de agenda te staan.

Daarnaast heeft het initiatief van ING om in de toekomst klantgegevens voor commerciële doeleinden te verstrekken aan derden veel stof doen opwaaien. De discussie over 'big data' is hierdoor in een versnelling gekomen. Gegevensbescherming en big data zijn onderwerpen die door de Verordening en door initiatieven van het bedrijfsleven meer in de belangstelling komen te staan Daarom wil ik in deze bijdrage een aantal handige tips bespreken voor het maken van een privacyrisicoanalyse.

Waarom nu?

Zoals al aangestipt laat de Algemene Verordening Gegevensbescherming nog even op zich wachten. Toch is het aan te raden nu al een inventarisatie van privacyrisico's te maken. Het maken van een risicoanalyse op basis van slechts de Wbp en de gedragscode is al zeer tijdrovend. De winst die de organisatie kan behalen met de privacyrisicoanalyse is dat de organisatie nu al een beeld heeft van hoe deze ervoor staat op het gebied van de verwerking van persoonsgegevens. Dat is nuttig omdat in de verordening een Privacy Impact Assessment verplicht is gesteld. De risicoanalyse die dan al is gemaakt, maakt het maken van deze impact assessment dan ook veel gemakkelijker, omdat de bedrijfs- en verwerkingsprocessen al in kaart zijn gebracht.

De Algemene Verordening Gegevensbescherming

Hoewel de exacte inhoud van de verordening nog niet bekend is, zijn er wel een aantal onderwerpen waarvan de kans groot is dat deze in de verordening terug zullen komen. Alleen de exacte invulling ervan is nog niet bekend. Een aantal voorbeelden zijn:

- verplichting tot het aanstellen van een privacy officer;
- verhoging van de boetes tot € 100.000.000,- of 5% van de wereldwijde jaaromzet;
- verplichting tot het uitvoeren van een Privacy Impact Assessment;
- melden van datalekken binnen 72 uur;
- 'right to erasure': recht om gegevens te laten wissen;
- oestemming CBP nodig voor doorgifte persoonsgegevens aan overheidsorganen buiten de EU;
- zelfstandige verantwoordelijkheid van bewerkers.

Het CBP

In Nederland houdt het College bescherming persoonsgegevens toezicht op de Wet bescherming persoonsgegevens en zal straks eveneens toezicht gaan uitoefenen op grond van de Algemene Verordening Gegevensbescherming.

Wetgeving
Op het moment dat je als organisatie een privacyrisico-analyse wil uitvoeren, is het verstandig om de huidige wetgeving als uitgangspunt te gebruiken. In dit geval zijn dat de Wbp en eventuele van toepassing zijnde gedragscodes.

Gedragscodes zijn niet vrijblijvend
Het CBP kan op verzoek een goedkeurende verklaring afgeven voor een bepaalde gedragscode. Deze gedragscode vormt dan een nadere uitwerking van de bepalingen uit de Wbp. Het CBP houdt een register bij van gedragscodes waar het een goedkeurende verklaring voor heeft afgegeven, waaronder bijvoorbeeld de Gedragscode verwerking persoonsgegevens financiële instellingen. Deze gedragscode is van toepassing op banken die lid zijn van de Nederlandse Vereniging van Banken (NVB), aangesloten zijn bij Rabobank Nederland en op verzekeraars die lid zijn van het Verbond van Verzekeraars. De bepalingen uit deze gedragscode zullen daarom ook moeten worden meegenomen in de risicoanalyse indien deze van toepassing is.

Hulpmiddelen
Het CBP heeft op haar website een aantal handige hulpmiddelen staan om een risicoanalyse te maken of aan de hand waarvan de risicoanalyse opgezet kan worden:

- De Quickscan: is bedoeld voor het bevorderen van het privacybewustzijn in de organisatie en het bepalen van de plaats van de organisatie op de kwaliteitsschaal van de gegevensverwerking.
- WBP Zelfevaluatie: is bedoeld voor het verkrijgen van inzicht in het toepassen van de Wbp in de organisatie en het nader bepalen van de plaats van de organisatie op de kwaliteitsschaal van de gegevensverwerking.
- Raamwerk Privacy Audit: is bedoeld als basis voor het beoordelen van de kwaliteit van de bescherming van persoonsgegevens over de gehele verwerking. Hier hoort ook een handreiking bij.

Daarnaast heeft ook het Verbond van Verzekeraars voor hun leden een Model Zelfevaluatie ontwikkeld op basis van de Gedragscode verwerking persoonsgegevens financiële instellingen. In deze zelfevaluatie zijn de normen uit de Wbp en de gedragscode verder uitgewerkt en specifiek voor verzekeraars aangepast. Aan de hand daarvan kan men direct het risico benoemen wat hieruit voort vloeit.

Voor compliance officers van verzekeraars is de opzet dus iets gemakkelijker te maken, maar voor andere compliance officers biedt naar mijn mening de WBP Zelfevaluatie het meeste houvast. Het Raamwerk Privacy Audit is geschikter voor compliance officers die al audit ervaring hebben of de internal auditors binnen de organisatie. De Quickscan is te globaal om een risicoanalyse mee op te zetten.

Verschillende risicocategorieën
De meeste risico's uit een privacyrisicoanalyse zijn te verdelen in reputatierisico's en toezichthouderrisico's. Hierbij kan bij reputatierisico gedacht worden vanuit het klantperspectief of het risico dat de organisatie in het (landelijke) nieuws komt door verkeerd gebruik of verlies van persoonsgegevens. Het toezichthouderrisico bestaat uit bijvoorbeeld een onderzoek, een dwangsom of een boete van het CBP. Waar bij het bepalen van de impact in de risicoanalyse mijns inziens ook rekening mee gehouden moet worden, is het soort gegevens dat verwerkt wordt. Bijzondere gegevens zoals strafrechtelijke en medische gegevens vereisen bijzondere aandacht. Bij verlies van deze gegevens bestaat ook het risico dat klanten hiervoor gecompenseerd willen worden.

Ik adviseer organisaties om nu al met de privacyrisicoanalyse te beginnen. De Verordening lijkt nog ver weg, maar gezien de hoeveelheid aan extra werk die de Verordening de organisaties brengt, ben je als organisatie al snel te laat gestart.

Marit Klapwijk is junior compliance officer bij het Nederlands Compliance Instituut. Voor meer informatie kunt u contact met haar opnemen. Tel. 088 99 88 100 of klapwijk@compliance-instituut.nl.