Drs. Piet Goeyenbier RE RA RO

Door ontwikkelingen, zoals e-commerce, apps, big en open data en 'internet of things', nemen de risico's voor de privacy toe. Het Nederlandse en het Europese parlement spelen op deze ontwikkelingen in met nieuwe wetgeving. 1 januari 2016 werd de meldplicht datalekken van kracht en later volgt de Algemene Verordening Gegevensbescherming (AVG). NOREA ontwikkelde een nuttig hulpmiddel in de vorm van een Privacy Impact Assessment (PIA).

Belangrijke ontwikkelingen in de **privacywetgeving**

Medio 2015 is de meldplicht datalekken aangenomen en is de ingangsdatum van deze wet vastgesteld op 1 januari 2016. Hiermee is aan de Wet bescherming persoonsgegevens (Wbp) een meldplicht voor inbreuken op beveiligingsmaatregelen voor persoonsgegevens toegevoegd. Met de meldplicht datalekken wordt beoogd de gevolgen van een datalek voor de betrokkenen zoveel mogelijk te beperken en hiermee een bijdrage te leveren aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

Meldplicht

De meldplicht datalekken schrijft voor dat de verantwoordelijke voor de verwerking van persoonsgegevens bij een datalek, waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens, een melding moet doen bij de toezichthouder, de Autoriteit Persoonsgegevens (AP), maar ook de betrokkene(n) moet informeren. Deze meldplicht geldt voor alle verantwoordelijken voor de verwerking van persoonsgegevens, zowel in de private als publieke sector. Als er geen melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijke boete, opgelegd door de AP. In dit kader heeft met deze wetsuitbreiding ook een uitbreiding van de bevoegdheid van de AP tot het heffen van bestuurlijke boetes plaatsgevonden.

Met de inwerkingtreding van de wetsaanpassing is de naam van het College bescherming persoonsgegevens (CBP) gewijzigd in Autoriteit Persoonsgegevens. Met deze nieuwe naam komt de uitbreiding van de bestuurlijke bevoegdheid van de toezichthouder beter tot uitdrukking. De AP heeft eind september 2015 in concept richtsnoeren aangereikt over de nadere invulling van de meldplicht datalekken. De AP geeft verder aan dat zij begin 2016 met een formulier en een website komt zodat dan de meldingen ook daadwerkelijk plaats kunnen vinden.

Concreet betekent de uitbreiding van de Wbp het volgende: de verantwoordelijke voor de verwerking van persoonsgegevens dient de AP onverwijld in kennis te stellen van een inbreuk op de beveiliging die leidt tot (een) aanzienlijke (kans op) ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. Ook dient de verantwoordelijke de betrokkene(n) te informeren (art. 34a). In artikel 34a is de wijze waarop invulling moet worden gegeven aan deze meldplicht nader uitgewerkt. Bij het niet of onvoldoende invulling geven aan het voorgaande kan de AP een bestuurlijke boete opleggen van 10% van de omzet van de betreffende organisatie. Het maximumbedrag van deze bestuurlijke boete is € 810.000 (dit was onder de oude wetgeving € 4500).

Het moge duidelijk zijn dat het opleggen van een bestuurlijke boete naast de financiële gevolgen ook de nodige negatieve gevolgen heeft voor de reputatie van de betreffende organisatie.

Privacy officer

Naast de meldplicht is nog een belangrijke verandering voor de privacywetgeving aanstaande, de vervanging van de Wbp door de AVG. Dit betreft een Europese verordening die directe werking heeft in de Europese lidstaten. Voor overheid en bedrijfsleven houdt deze nieuwe verordening in dat expliciet aandacht moet worden geschonken aan het onderwerp

privacy door bijvoorbeeld het inrichten van privacybeleid en het beschikken over een privacy officer. Het doel hiervan is zorgdragen dat een individu zijn rechten op het gebied van privacy ook daadwerkelijk kan effectueren.
Voor een organisatie leidt de meldplicht datalekken tot de volgende drie vragen:

- Beschikt de organisatie over registraties met privacygevoelige persoonsgegevens waarvoor zij verantwoordelijk kan worden gesteld?
- Worden met de betreffende persoonsregistratie(s) risico's gelopen op het gebied van datalekken?
- Indien zich onverhoopt een datalek voordoet is dan het proces van ontdekking, melding en oplossing in voldoende mate ingericht?

Privacy Impact Assessment (PIA)
Met de PIA heeft NOREA in een hulpmiddel voorzien waarmee een organisatie kan inventariseren in welke mate privacy bij een persoonsregistratie van belang is en of er toereikende maatregelen zijn getroffen. Voor overheidsorganisaties is het uitvoeren van een PIA verplicht. De rijksoverheid heeft hiervoor een eigen PIA ontwikkeld. Hier wordt verder ingegaan op de PIA die ontwikkeld is door NOREA.
Allereerst kan een organisatie een quickscan PIA uitvoeren met een 'privacychecker' (beschikbaar via internet). Via tien vragen wordt dan vlot inzicht verkregen of het uitvoeren van een PIA zinvol is. Is dit het geval, dan kan de PIA worden uitgevoerd (per persoonsregistratie) aan de hand van de vragenlijst die is opgenomen in het NOREA-document. Een praktische werkwijze is om dat gezamenlijk te doen met een aantal betrokkenen (zoals de verantwoordelijke voor de persoonsregistraties, de privacy officer en de bewerker). Door de discussie van deze betrokkenen ontstaat een breder en gedeeld beeld. Het vastleggen van de onderbouwing van de antwoorden is belangrijk voor later (onderhoudbaarheid en overdracht). De internal auditor kan in dit proces bijvoorbeeld een rol vervullen op het gebied van het toezien op de kwaliteitsborging.
De onderdelen van de PIA vragenlijst (NOREA):
1. Het type project.
2. De gegevens.
3. Betrokken partijen.
4. Verzamelen van gegevens.
5. Gebruik van gegevens (inclusief verstrekken).
6. Bewaren en vernietigen van gegevens.
7. Beveiliging.

Door het uitvoeren van de PIA worden de eerste twee van de hiervoor genoemde drie vragen beantwoord. Een toereikend informatiebeveiligingsplan kan (voor de betreffende persoonsregistratie) inzicht bieden in de getroffen beveiligingsmaatregelen (de opzet). Om daadwerkelijk zicht te krijgen op de risico's die samenhangen met de persoonsregistratie, de getroffen beheersmaatregelen en mogelijke datalekken, zou een onderzoek uitgevoerd moeten worden naar de opzet, het bestaan en de werking van het beheer en de beveiliging van

Als er geen melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijke boete

de betreffende persoonsregistratie. Het komt overigens vaak voor dat de verwerking van de persoonsregistratie (of delen daarvan) door een serviceorganisatie plaatsvindt (de bewerker). Door middel van een bewerkersovereenkomst moeten dan de eisen en de plichten van de verantwoordelijke worden doorvertaald naar de betreffende dienstverlener.
De derde vraag, het proces van ontdekking van het datalek tot melding (en de registratie van die meldingen), is niet geadresseerd in de PIA-vragenlijst. Zo'n proces moet door iedere organisatie worden ingericht, waarbij wel aangesloten kan worden op de aanwezige procedures op het gebied van melden van incidenten en calamiteiten.

Te treffen acties
Nadat door middel van analyse is vastgesteld dat de Wbp en de meldplicht datalekken relevant zijn, dient de organisatie de relevante processen en beheersingsmaatregelen te inventariseren, te optimaliseren en te borgen. Ook dienen de bewerkersovereenkomsten te worden aangepast zodat de bewerker (de serviceorganisatie) eventuele datalekken zo spoedig mogelijk meldt bij de verantwoordelijke organisatie. Hierdoor kan deze invulling geven aan de wettelijke meldplicht en de bijbehorende vereisten, zoals de registratie van incidenten en calamiteiten.
Maatregelen in het kader van de meldplicht datalekken:
1. Benoem de verantwoordelijke(n) voor de registratie.
2. Pas de bewerkersovereenkomsten aan.
3. Pas het incident- en calamiteitenproces aan.
4. Zorg voor een meldprocedure (datalekprotocol).
5. Zorg van registraties van de gedane meldingen.

Naast de inrichting moet ook een meldprocedure (of datalekprotocol) worden ingericht. Zo'n meldprocedure kan uit de volgende stappen bestaan:
- Intern melden, registreren en analyseren van een incident.
- Vaststellen of sprake van een datalek is.
- AP informeren en deze melding registreren.
- Betrokkenen informeren en deze melding registreren.
- Oplossen datalek.
- Evalueren.

Zolang er nog geen heldere regels zijn die voorschrijven wanneer wel en niet gemeld moet worden, kunnen de volgende vuistregels worden gehanteerd:
- Hoe zou u geïnformeerd willen worden als het uw eigen persoonsgegevens betreft?
- Bij twijfel melden!

De rol van Internal Audit
Zoals al is aangegeven heeft de aangepaste privacywetgeving consequenties voor de organisatie. Door het uitvoeren van een PIA kan de organisatie nagaan of kwetsbaarheden voorkomen bij persoonsregistraties. Is dit het geval, dan dient de organisatie in actie te komen om te voldoen aan de eisen van de nieuwe privacywetgeving. Internal Audit kan hierbij verschillende rollen vervullen. Zij kan de organisatie bewust maken van de (komende) wetswijzigingen zodat de organisatie daar tijdig op kan anticiperen (de signalerende rol). Tijdens het analyse- en het implementatieproces van de beheersingsmaatregelen kan zij de rol vervullen van facilitator dan wel toezicht houden op de kwaliteitsborging van het proces. Na de implementatie kan Internal Audit een audit uitvoeren naar de nieuwe processen. Daarnaast kan de internal auditor ook een onderzoek uitvoeren naar de kwaliteit van het beveiligingsstelsel. <<

Relevante websites

- http://www.norea.nl/norea/actueel/nieuws/presentatie+pia.aspx
- https://cbpweb.nl/nl/over-privacy/persoonsgegevens/beveiliging-van-persoonsgegevens#faq
- http://www.cip-overheid.nl
- http://www.IBDgemeenten.nl
- http://privacychecker.eu/nl
- http://www.justitia.nl/privacy/

Piet Goeyenbier is auditmanager bij de Auditdienst Rijk (ADR) van het ministerie van Financiën. Hij is lid van de Commissie Professional Practices van IIA Nederland. Verder is hij als extern deskundige betrokken bij de AITAP (post-master IT-auditopleiding) aan de Amsterdam Business School (UvA).
p.j.m.goeyenbier@minfin.nl

Dit artikel is geschreven op persoonlijke titel.