Privacy Impact Analyse: uw privacyrisico's in beeld

Een verplichting onder de Europese privacyverordening

Digitalisering helpt organisaties wereldwijd bij het verzamelen, opslaan en delen van persoonsgegevens. Zo bezien is digitalisering een geschenk. Maar aan al dit gemak kleven ook privacyrisico's: bij een datalek kunnen persoonsgegevens in één klap op straat terecht komen. Met de Privacy Impact Analyse (PIA) van Aon heeft u snel in kaart waar in uw organisatie de grootste privacyrisico's liggen en welke maatregelen u moet treffen voor 2018.

Een zorgvuldige omgang met gevoelige data, niet alleen ICT-technisch maar ook beleidsmatig, is meer dan alleen een blijk van goed werkgeverschap. Bij onvoldoende bescherming van uw data loopt u ook het risico op privacyschending van uw klanten en werknemers. Dat leidt al snel tot reputatieschade, claims en boetes van toezichthouders. Uiteindelijk kunt u zelfs het vertrouwen van klanten en medewerkers verliezen. Daartegenover staat dat het aantoonbaar goed beheren van data uw bedrijf kan onderscheiden van de concurrentie

Cruciaal is een privacystrategie waarin u beschrijft hoe uw organisatie persoonsgegevens gebruikt, verwerkt en beschermt – zowel nu als in de toekomst. Wees u ervan bewust dat privacy-risico's niet alleen ontstaan door moedwillige cybercrime, maar ook door onbedoelde incidenten als gevolg van menselijke fouten of technisch falen. Dat vraagt om technische én organisatorische beveiligingsmaatregelen.

De nieuwe Europese privacyverordening is vanaf mei 2018 van kracht.

Dit betekent nog strengere regels inzake privacybescherming. U dient als organisatie onder andere in beeld te hebben welke gegevens worden verwerkt, hoe ze worden verwerkt, wie toegang heeft tot de gegevens en ook met wie de gegevens worden gedeeld. Onze ervaring is dat veel bedrijven nu reeds aan de slag moeten om aan de verplichtingen van de General Data Protection Regulation (GDPR) te voldoen. Denk hierbij aan organisatorische maatregelen, maar ook aan het aanpassen van langlopende contracten met leveranciers.

Europese privacyverordening

De Europese privacyverordening is vanaf mei 2018 van kracht en raakt elke organisatie die met persoonsgegevens werkt. De meeste organisaties zijn daarom verplicht om een PIA uit te voeren om de privacyrisico's en alle gegevensverwerkingen in kaart te brengen voor de regelgeving van kracht is.

Belangrijkste verplichtingen Europese privacyverordening

- boetes lopen op tot 20M EUR of 4% van de wereldwijde omzet;
- gegevens niet langer dan strikt noodzakelijk bewaren en het recht om vergeten te worden;
- datalek binnen 72 uur melden bij de Autoriteit Persoonsgegevens;
- passende technische en organisatorische maatregelen nemen, zoals:
  - encryptie van bestanden;
  - risicoanalyse om kwetsbaarheden te ontdekken.
- strengere eisen aan toestemming om gegevens te bewaren;
- strengere eisen aan de informatieverplichting richting de betrokkene(n).

Wilt u ook een helder beeld van de privacyrisico's die uw organisatie loopt?

Neem voor meer informatie over onze PIA contact op met:

Leslie Clement
Consultant AGRC Cyber Practice
010 448 7802
06 463 422 94
leslie.clement@aon.nl

aon.nl/cyber

Nederland kent deze verplichting reeds onder de aangepaste Wet bescherming persoonsgegevens (Wbp, zie kader). Organisaties dienen passende maatregelen te treffen tegen verlies of onrechtmatige verwerking van data. Onze PIA helpt u daarbij.

U krijgt een gestructureerd en helder beeld van uw privacyrisico's, de (financiële) impact en welke acties u moet nemen om deze risico's weg te nemen of op een acceptabel niveau te krijgen.

Wet meldplicht datalekken

De Wet meldplicht datalekken, die sinds 1 januari 2016 van kracht is, raakt elke organisatie die met persoonsgegevens werkt. Wist u dat u de Autoriteit Persoonsgegevens al moet inlichten bij een kwijtgeraakte USB-stick met persoonsgegevens en zelfs bij het vermoeden van een lek?

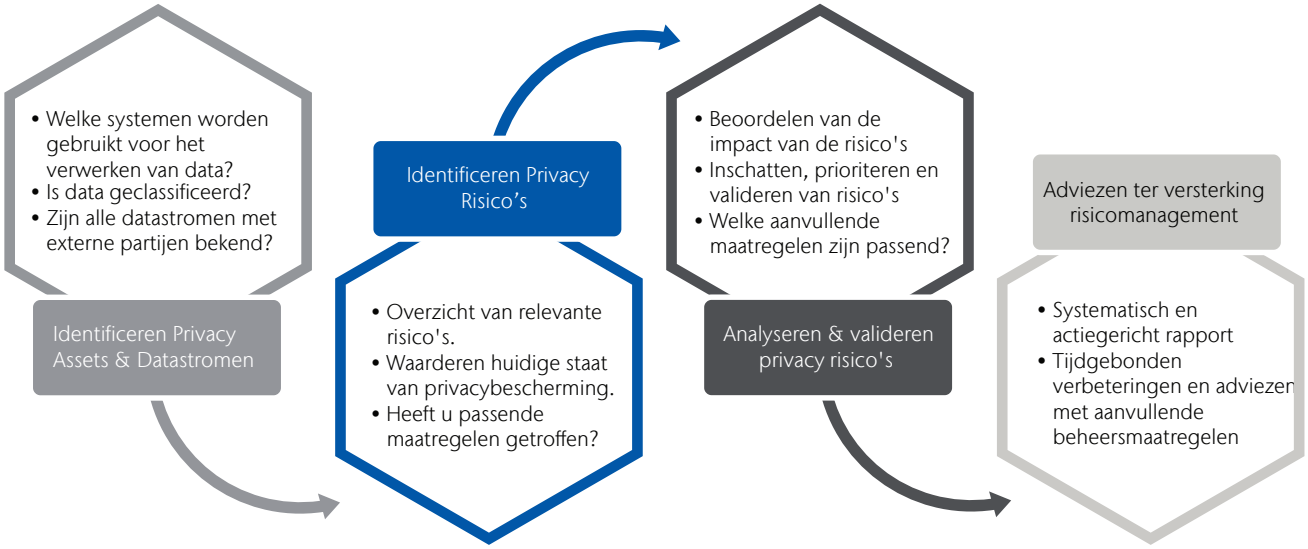
Belangrijkste verplichtingen meldplicht datalekken

- gerechtvaardigd doel voor het opslaan van privacygevoelige gegevens;
- gegevens niet langer dan strikt noodzakelijk bewaren;
- datalek binnen 72 uur melden bij de Autoriteit Persoonsgegevens;
- passende technische en organisatorische maatregelen nemen, zoals:
  - encryptie van bestanden;
  - risicoanalyse om kwetsbaarheden te ontdekken.
- betrokkene(n) op de hoogte stellen (bij ernstig nadelige gevolgen voor betrokkene(n)).

Hoe werkt de Privacy Impact Analyse?

Met de PIA legt Aon systematisch uw privacygerelateerde risico's bloot en ziet u in hoeverre een lek betrokkenen schaadt. Daarmee vormen de resultaten een vertrekpunt voor gerichte acties om privacyrisico's te verminderen. De PIA staat niet op zichzelf, maar moet onderdeel zijn van uw informatiebeveiligings- en risicomanagementbeleid. We gaan na welke gegevens u opslaat/verwerkt, welke privacyrisico's uw organisatie bedreigen, welke passende maatregelen u moet nemen en hoe het actieplan eruit moet zien om de verplichtingen vanuit het wettelijk kader op te volgen om zodoende te voldoen aan een passend niveau van privacybescherming.

Onze PIA bestaat uit de volgende stappen:



De PIA is gebaseerd op de nationale en Europese vereisten uit bovenstaande privacywetgeving en geaccepteerde normen omtrent informatiebeveiliging. Belangrijke vragen zijn bijvoorbeeld:

- Weet u welke gevoelige gegevens u beheert en verwerkt, en wie intern verantwoordelijk is voor de verwerking van die gegevens?
- Weet u of deze gegevens veilig zijn en kunnen ze bij verlies worden teruggehaald?
- Hebben derden (leveranciers) ook toegang tot deze gegevens?
- Heeft u data geclassificeerd en daarop passende maatregelen genomen?

De PIA is zowel richtinggevend als corrigerend bedoeld. In onze dienstverlening combineren we onze kennis van digitalisering, wet- en regelgeving, risico's en risicobeheersing voor u. Zo zorgen wij er samen met u voor dat uw organisatie de grip op privacyrisico's versterkt, voldoet aan wet- en regelgeving en het vertrouwen van uw stakeholders behoudt.

1023-01-PIA-V7