Bescherming persoonsgegevens

Wat is de impact op uw organisatie?

Het opslaan, bewerken en verzenden van persoonsgegevens is een steeds gevoeliger wordend onderwerp in de samenleving. Door de digitalisering en de toenemende mate van toegankelijkheid van systemen en informatie, wordt de noodzaak tot het reguleren van de verwerking van persoonlijke gegevens ingezien door overheden.

MELDPLICHT DATALEKKEN

Vanaf 1 januari 2016 is de meldplicht datalekken in werking getreden.[1] Dit betekent dat organisaties binnen 72 uur na het optreden van een datalek deze dienen te melden bij de Autoriteit Persoonsgegevens. In sommige gevallen dienen ook de personen waarvan de gegevens zijn gelekt te worden geïnformeerd. Indien er niet aan de criteria van de meldplicht datalekken wordt voldaan, riskeren bedrijven boetes oplopend tot 820.000 euro. De meldplicht geldt zowel voor private ondernemingen als voor organisaties actief in de publieke sector én voor overheden.

EUROPESE PRIVACYVERORDENING

Van gelijke strekking als de meldplicht datalekken is de Europese Privacyverordening; officieel de Algemene Verordening Gegevensbescherming (AVG).[2] Deze treedt op 25 mei 2018 in werking. De belangrijkste onderwerpen uit de Europese Privacyverordening zijn:

- Melding van datalekken aan de toezichthouder
- Bewerkersovereenkomst tussen de verantwoordelijke voor de persoonsgegevens en degene die de persoonsgegevens voor hem verwerkt
- Privacy als leidraad bij de ontwikkeling en inrichting van processen en diensten (“Privacy by Design” en “Privacy by Default”)
- Aanstelling van een Functionaris Gegevensbescherming
- Opstellen van een Privacy Impact Assessment
- Bijhouden van een register voor de verwerking van persoonsgegevens
- Toestemming en informeren van betrokkene bij verwerking gegevens
- Voorwaarden voor profilering
- Verwijderen van informatie: “Vergeetrecht”

Ook voor de AVG geldt dat er hoge boetes kunnen worden opgelegd bij het niet nakomen van de verordening door organisaties.[3] Het gaat dan om bedragen tot 20 miljoen euro, of 4% van de wereldwijde jaaromzet van een onderneming als die hoger uitvalt. Vanuit een compliance perspectief en mogelijke controles dient met name aandacht te worden geschonken aan werknemers- en salarisadministraties, klantenadministraties (CRM) en patiëntenadministraties / medische gegevens.

WAT DOET UW ORGANISATIE OM PERSOONSGEGEVENS TE BESCHERMEN?

Dit is vandaag de dag een zeer belangrijke vraag voor alle bedrijven. Niet alleen kan een datalek leiden tot financiële consequenties, ook kan er aanzienlijke reputatieschade worden opgelopen. Dat nog niet alle bedrijfstakken goed zijn voorbereid op het omgaan met datalekken blijkt wel uit de volgende onderzoeken.

---

[1] De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp); 8 december 2016; *https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf*

[2] Justitia.nl; *http://www.justitia.nl/privacy/europese-privacyverordening.html*

[3] Justitia.nl; *http://www.justitia.nl/privacy/europese-privacyverordening.html*

"Datalekken bij gemeenten: het is een beetje een zooitje"[4]

In het NRC van zaterdag 28 januari en zondag 29 januari 2017 staat een artikel met bovengenoemde titel. Hierin staat dat uit onderzoek van Mary-Jo de Leeuw naar informatieveiligheid bij gemeenten blijkt dat tweederde van de gemeenten een datalek van persoonlijke gegevens meldden in 2016. De ernst van de meldingen verschilt per gemeente. Het feit blijft wel dat vijftien procent van de gemeenten slachtoffer is van computercriminaliteit.

"De 5 security-uitdagingen voor onderwijsinstellingen"[5]

Door Watchguard is een whitepaper opgesteld waarin wordt gesteld dat leerlingen en ouders er altijd op moeten kunnen rekenen dat educatieve instellingen zorgvuldig met hun data en dus privacy omgaan. De uitdagingen van de meldplicht datalekken op de onderwijssector worden uiteengezet, met als uitgangspunt een onderzoek van het ministerie van Onderwijs, Cultuur en Wetenschappen en PWC.[6] Uit dit onderzoek blijkt namelijk dat scholen in het primair en secundair onderwijs met name gebruikmaken van 'gezond verstand' als het gaat om privacy en informatiebeveiliging. Veelal is dus niet bekend of er aan de nieuwe wet- en regelgeving wordt voldaan. Ook is er onvoldoende inzicht in de ICT-beveiliging die is ingeregeld en wordt toegepast.

CONCLUSIE

Er zijn legio voorbeelden van situaties waarin de kans op een datalek zeer groot is. Niet alleen in de publieke sectoren die benoemd zijn in de onderzoeken waarnaar dit artikel refereert, ook in het commerciële bedrijfsleven gaat het regelmatig mis. De vraag is wat de impact is op uw organisatie; zowel voor de inrichting van uw processen en 'risk & control-framework', als voor de financiële consequenties en reputatieschade bij een daadwerkelijk datalek.

[4] "Datalekken bij gemeenten: het is een beetje een zooitje"; Liza van Lonkhuyzen; NRC; 28 januari & 29 januari 2017

[5] "De 5 security-uitdagingen voor onderwijsinstellingen" (Whitepaper); Watchguard; www.watchguard.com

[6] "Nulmeting Privacy en Informatiebeveiliging in het Primair en Voortgezet Onderwijs"; Ministerie van Onderwijs, Culltuur en Wetenschappen en PWC; 2014