Auteur: drs. Ruud Buurma is als adviseur informatiebeveiliging en AVG werkzaam voor HODARI B.V.

AVG in relatie tot informatiebeveiliging

In mei 2018 ging in de gehele Europese Economische Ruimte (EER) de General Data Protection Regulation 2016/679 (GDPR) van kracht. In Nederland vertaald naar de Algemene Verordening Gegevensbescherming (AVG). Wat hebben organisaties in de afgelopen twee jaar geleerd? Een antwoord hierop halen we uit het nieuws. Naast een relatie die direct is te leggen met de AVG, is er ook een relatie met de beveiliging van informatie in het algemeen en persoonsgegevens in het bijzonder.

Een greep uit het nieuws:

juni 2018: uitspraak van Autoriteit Persoonsgegevens rondom gebruik van BSN- en BTW- nummers van zelfstandigen.
juni 2019: gemeente Deventer moet € 500 schadevergoeding betalen aan een man die een aantal WOB-verzoeken had ingediend.
juli 2019: eerste boete van € 460.000 opgelegd op grond van de AVG aan het Haga Ziekenhuis vanwege de onzorgvuldige omgang met patiëntgegevens.
januari 2020: flinke stijging online-fraude.
februari 2020: Universiteit Maastricht betaalt € 197.000 nadat ze het slachtoffer waren geworden van ransomware.
februari 2020: gegevens van 80.000 passagiers Transavia gestolen.
maart 2020: tennisbond KNLTB krijgt een boete van € 525.000 voor het verstrekken van gegevens van leden aan twee sponsoren.
maart 2020: privacy van bestuurders van (veelal elektrische zelfrijdende) auto's niet goed geregeld.

Zit de Autoriteit Persoonsgegevens stil?

Wat opvalt is dat het nieuws ten aanzien van de AVG, als het gaat om boetes, nog te overzien is. Het aantal boetes is tot nu toe nog letterlijk op een hand te tellen. Dat wil niet zeggen dat de Autoriteit Persoonsgegevens (AP) stilzit.

- Zelf geeft de AP in haar 'Toetsingskader 2018-2019' aan dat zij in die jaren 'guidance' willen bieden aan de invoering, en de bekendheid met de AVG willen vergroten. Een groot deel van 2018 en 2019 is dan ook gebruikt om organisaties en particulieren te informeren over hun rechten en plichten.
- Daarnaast heeft de AP een onderzoek gedaan bij dertig organisaties, groot en klein en uit diverse sectoren, naar de naleving van de AVG bij die organisaties. Dit onderzoek was voornamelijk gericht op verwerkersovereenkomsten en verwerkingsregisters. De uitkomsten van die onderzoeken zijn overigens niet publiekelijk bekend gemaakt.
- Ook onderzocht de AP of overheidsorganisaties, ziekenhuizen, verzekeraars en banken een functionaris voor de gegevensbescherming hebben. Tevens is de Autoriteit Persoonsgegevens in een groot deel van 2019 bezig geweest de eigen organisatie op sterkte te krijgen. Deze was nog niet voorbereid op het grote aantal meldingen die zij hebben ontvangen: 27.000 in 2019 tegenover ruim 8.000 in 2018.
- Uit 'Focus Autoriteit Persoonsgegevens 2020-2023', de opvolger van het 'Toetsingskader 2018-2019', blijkt dat de nadruk onder meer zal komen te liggen op illegale datahandel en gebrekkige beveiliging.

Wat eveneens opvalt is dat het nieuws in toenemende mate wordt gevuld met aspecten van cybercrime. Het gaat daarbij om zaken als hacking, identiteitsfraude, phishing, pinpasfraude en ransomware, Niet alleen particulieren worden hier in toenemende mate het slachtoffer van, maar ook organisaties.

De dagelijkse praktijk

Wat is de ervaring van HODARI in de praktijk? Wij zien een opvallende inzet op informatiebeveiliging sinds de invoering van de AVG. Door de toenemende rol van privacy staat voor veel grote organisaties het inzetten op informatiebeveiliging nu nog hoger op de agenda ter voorkoming van schade aan de financiële positie, de reputatie en het imago.
Voor kleinere organisaties gold vaak dat informatiebeveiliging veelal tot een minimum werd beperkt om op die wijze de hoogste risico's (zoals bijvoorbeeld uitval van systemen en verlies van data) te vermijden. Blijkbaar kwam dit doordat de bewustwording voor eventuele andere gevolgen er nog niet was. Met de invoering van de 'melding datalekken', als onderdeel van de Wet bescherming persoonsgegevens, werd een eerste kentering zichtbaar. Geleidelijk groeide het besef dat er meer moest worden gedaan om de IT-omgeving te beveiligen en zo de rechten ten aanzien van de privacy van natuurlijke personen te waarborgen.

Invloed van de AVG op informatiebeveiliging

Waarom is de AVG een belangrijke aanjager geworden voor het optimaliseren van informatiebeveiliging?

Naast de AVG is er ook vanuit andere invalshoeken aandacht voor informatiebeveiliging

Het antwoord op die vraag ligt besloten in de AVG zelf. Teneinde de privacy van natuurlijke personen optimaal te beschermen heeft men in de AVG enkele bepalingen opgenomen die betrekking hebben op informatiebeveiliging. Het gaat daarbij onder meer om de artikelen 5, 5f, 25 en 32 waarin is vastgelegd dat een organisatie passende organisatorische en/of technische maatregelen neemt teneinde persoonsgegevens te beveiligen tegen van buitenaf komend onheil. Ook wordt aangegeven dat een organisatie prudent dient om te gaan met het verlenen van toegang tot systemen waarin persoonsgegevens zijn vastgelegd (toegangsautorisatie).

Rol van certificering

Naast de AVG is er ook vanuit andere invalshoeken aandacht voor informatiebeveiliging. In ISO 27001, ISO 27002, NEN 7510 en voor de overheid de BIO, wordt expliciete aandacht gegeven aan informatiebeveiliging.

In relatie tot de AVG kan hier nog het volgende over worden vermeld: artikel 42 AVG spreekt over certificering als een middel om aantoonbaar te maken dat aan de AVG wordt voldaan. Het mechanisme van certificering is niet verplicht maar kan een organisatie een (concurrentie)voordeel en haar klanten zekerheid opleveren indien zij gecertificeerd is.

Genoeg werk

Concluderend stellen wij vast dat de AVG een aanjager is voor informatiebeveiliging. Gezien het feit dat we vrijwel dagelijks worden geconfronteerd met vormen van cybercrime, datalekken en dergelijke, kan worden gesteld dat er nog genoeg werk is om informatiebeveiliging naar het juiste niveau te brengen en daarmee onder andere aan de AVG te voldoen. Houd hierbij rekening met het feit dat kwaadwillenden niet stilzitten en een permanente bedreiging vormen. De Autoriteit Persoonsgegevens zal met argusogen de vorderingen volgen die organisaties maken. Met name de inspanning die organisaties aantoonbaar hebben gemaakt om hun persoonsgegevens te beschermen, en zo te voldoen aan de in de AVG vastgelegde eisen, zal bepalend zijn voor de mate waarin tekortkomingen worden bestraft.

Maatregelen en risico in balans

Bovenstaande tips zijn beperkt. Iedere specifieke casus vraagt om een goede analyse van de actuele situatie. Op basis van die analyse kan vervolgens worden bepaald welke noodzakelijke maatregelen er genomen dienen te worden om te voldoen aan de AVG en om voldoende beschermd te zijn tegen calamiteiten. Maatregelen dienen qua inzet van middelen in balans te zijn met het risico dat wordt gelopen.

Neem minstens de volgende stappen:

- Draag zorg voor een actueel informatiebeveiligingsbeleid, inclusief de daarbij behorende procedures, en toets deze regelmatig.
- Koppel het informatiebeveiligingsbeleid aan de eisen van de AVG.
- Zorg dat je medewerkers bekend zijn met het beleid en procedures.
- Stuur op houding en gedrag zodat de zwakste schakel (de mens) de risico's herkent en erkent.
- Test frequent of je beveiligingsmaatregelen (nog) werken (via zogenoemde pentest).
- Houd de in de loop van de jaren verzamelde data eens tegen het licht, veel 'unstructured' data bevat mogelijk gegevens die organisaties volgens de AVG niet langer in bezit mogen hebben.
- Draag zorg voor passende organisatorische en technische maatregelen waaronder de verleende toegang tot systemen.