BMC
YACHT GROUP

Handhaving van de AVG en de eerste boete

Wat kan de lokale overheid daarvan leren?

Partners in verbetering

Doorontwikkelen op privacy en informatiebeveiliging is nodig

Bij de invoering van de AVG zijn veel organisaties druk bezig geweest een aantal basisvereisten in te vullen. Daarna is de aandacht soms verslapt of ontbreekt er een goed kader om te beoordelen in hoeverre de organisatie voldoet. En toch is het nodig om het voldoen aan de AVG en de beveiliging van gegevens verder uit te bouwen. De Autoriteit Persoonsgegevens (AP) heeft met handhavings-maatregelen duidelijk gemaakt dat zij er niet voor terugdeinst boetes en dwangsommen op te leggen. Dat is een (financieel) risico voor organisaties, dat alleen beperkt kan worden door een betere beheersing van privacy en beveiliging. Zonder deze beheersing is de kans op een datalek met deze gevoelige gegevens groot. Dat heeft gevolgen voor uw inwoners, maar ook voor uw organisatie en haar relatie met toezichthouders. Bij een incident is het na de handhaving van de afgelopen periode moeilijk aan inwoners uit te leggen dat de noodzaak van deze maatregelen in uw organisatie niet bekend was. Datzelfde geldt natuurlijk voor de pers en voor toezichthouders.

Daar komen dan ook nog de kosten bij die bij een datalek ontstaan voor communicatie en schade-vergoedingen. Onlangs heeft de rechter bepaald dat de gemeente Deventer een schadevergoeding van 500 euro moet betalen aan een burger voor geleden immateriële schade op basis van de AVG. Wanneer meerdere inwoners slachtoffer zijn van een datalek, kan dat behoorlijk oplopen, los van eventuele boetes. Zowel voor de rechter als voor de AP zal het ontbreken van de genoemde beveiligingsmaatregelen uw organisatie als verzwarend worden aangerekend na de publiciteit van de afgelopen periode.

Het valt te verwachten dat de AP bij datalekken ook op deze aspecten zal letten en daarover - als daar aanleiding toe is - aanvullende vragen zal stellen. Dan is het beter om de maatregelen voorafgaand aan een incident in te voeren dan achteraf, wanneer het spreekwoordelijke kalf verdronken is.

Verschuiving in de handhaving door de AP

Tot juni 2019 heeft de AP vooral gehandhaafd door regelmatig te publiceren en te adviseren over specifieke onderwerpen. Daarnaast wordt er ook gehandhaafd met dwangsommen voor de politie en voor het UWV, maar nog niet met boetes. Voorbeelden zijn een dwangsom van maximaal 900.000 euro voor het UWV in juli 2018 en een voor de politie van maximaal 320.000 euro in november 2018.

In juni 2019 heeft de AP een boete van bijna een half miljoen euro opgelegd aan het HagaZiekenhuis, waarbij aanvullend een dwangsom is opgelegd van nog eens maximaal 300.000 euro. De boete laat zien dat de AP bereid is om al haar bevoegdheden in te zetten en dat zij niet alleen de zachte weg van adviseren en aandacht vragen gebruikt om de toepassing van de AVG te bevorderen.

Handhaving door de AP met publicaties over:

- Registers van Verwerkingen
- datalekregisters
- de aanstelling van FG's
- privacybeleid
- privacy bij internet of things-apparaten
- over schuldhulpverlening

Een aantal malen heeft de AP voor de publicaties onderzoek gedaan bij verschillende organisaties.

De AP handhaaft op beveiliging

De AP heeft voorafgaand aan een aantal publicaties eerst onderzoek gedaan bij meerdere organisaties. In de regel ontvangen circa 30 organisaties dan een enquête. Het vervolg daarop is tot dusver beperkt tot adviezen, maar dat hoeft niet zo te blijven. Dat maakt de handhaving op beveiliging duidelijk. De dwangsommen en de boete maken ook duidelijk dat beveiliging voor de AP een prioriteit is. Alle dwangsommen en boetes gaan over beveiliging, meer specifiek over het ontbreken van tweefactorauthenticatie, autorisatiebeleid en logging.

Bij de overheid zijn deze maatregelen verplicht op basis van de BIO.

Waarvoor zijn dwangsommen en boetes gegeven?

Bij de dwangsom voor het UWV gaat het om de toegangsbeveiliging, waarbij tweefactor-authenticatie in het werkgeversportaal ontbreekt. Bij de politie gaat het om de autorisatie van toegang tot gegevens: te veel mensen konden te veel gegevens inzien.

De achtergrond van de boete voor het HagaZiekenhuis was het inzien van gegevens van een bekende Nederlander door nieuwsgierige medewerkers, die niets met de behandeling van de patiënt te maken hadden. De boete is gegeven voor het voortduren van de overtreding en het uitblijven van structurele maatregelen om oneigenlijke inzage te voorkomen, zoals tweefactorauthenticatie en een deugdelijke controle van logbestanden.

Werken op basis van risico's en prioriteiten

Uw organisatie kan niet alles tegelijk. Mogelijk bent u al bezig met de invoering van de BIO. Daarom is het belangrijk om prioriteiten te stellen. Het bovenstaande vormt daarvoor een goede basis. Daarvoor heeft u inzicht en overzicht nodig.

U kunt overzicht en inzicht verkrijgen door:

- een eendaagse quickscan AVG: U krijgt dan overzicht over de mate waarin onderdelen van de AVG in uw organisatie zijn geborgd én u adviezen over waar te beginnen. De quickscan is een zelfevaluatie, waarin we prioriteiten zoals het Register van Verwerkingen, privacyverklaringen en datalekken meenemen.
- een AVG-assessment: BMC doet hiermee nader onderzoek en geeft een onafhankelijk oordeel over beleid, procedures en richtlijnen en de borging daarvan in uw organisatie. Naast de resultaten uit de quickscan ontvangt u ook een inhoudelijke beoordeling en adviezen.
- een eendaagse quickscan Informatiebeveiliging: U krijgt dan een overzicht over de mate waarin onderdelen van de BIO in uw organisatie zijn geborgd én adviezen over waar te beginnen. De quickscan is een zelfevaluatie.
- een assessment Informatiebeveiliging: BMC doet hiermee nader onderzoek en geeft een onafhankelijk oordeel over beleid, procedures en richtlijnen en de borging daarvan in uw organisatie. Ook nemen we daarin de prioriteiten van de AP mee, zoals toegangsbeveiliging van een aantal door u te selecteren informatiesystemen. Naast de resultaten uit de quickscan ontvangt u ook een inhoudelijke beoordeling en adviezen.

BMC heeft ervaring met de richting van informatiebeveiliging bij gemeenten en andere overheids-organisaties.

Op basis van deze adviezen stelt BMC met u een plan van aanpak op. Natuurlijk is dit in eerste instantie een investering in tijd en aandacht. Eenmaal op orde is het alleen een kwestie van bijhouden.

We gaan voor resultaat

Na het uitvoeren van het plan van aanpak hebt u een grote stap gemaakt in het veiliger maken van gegevens van inwoners en medewerkers. De kans op een datalek is daarmee beduidend kleiner geworden en een correcte afhandeling is geborgd. U heeft daarmee ook delen van de BIO ingevoerd. U kunt uw budget inzetten voor inwoners in plaats van voor communicatie, schadevergoedingen en boetes naar aanleiding van datalekken. Mocht het toch misgaan, dan kunt u zich verantwoorden door te laten zien dat u deze basisbeveiliging op orde heeft.

Waarom BMC?

BMC geeft integraal advies door kennis en ervaring van gemeenten en andere overheidsorganisaties, privacy en informatieveiligheid te combineren. BMC verstaat de taal van verschillende disciplines, van bestuursniveau tot op de werkvloer. BMC neemt de organisatie mee in haar ontwikkeling en stemt haar advies daarop af.

Meer informatie & contact

Voor meer informatie over dit aanbod en voor het maken van een (vrijblijvende) afspraak kunt u contact opnemen met onze (senior) adviseur(s) via telefoonnummer (033) 496 52 00 of per e-mail.

Ir. Julius Duijts CiSSP CiPP/E
senior adviseur
julius.duijts@bmc.nl

Mr. Alex Commandeur
senior adviseur
alex.commandeur@bmc.nl

Drs. Willem de Vries
adviseur
willem.de.vries@bmc.nl

Kijk voor meer informatie ook eens op onze website **www.bmc.nl**