



Wat betekent de meldplicht voor mijn organisatie?

Help: een meldplicht datalekken!

Sinds 1 januari 2016 geldt de meldplicht datalekken. Maar wat is een datalek precies? Welke implicaties heeft dit voor bedrijven, organisaties en instellingen? Wanneer moet een datalek worden gemeld bij de Autoriteit Persoonsgegevens? Wat moet er exact worden gemeld? Op deze en andere vragen geeft de auteur in dit artikel antwoord.

TEKST MIRJAM ELFERINK

Sinds 1 januari 2016 geldt de meldplicht datalekken. De vraag is niet zozeer óf u ermee te maken krijgt, als wel wánneér dat het geval is. Deze meldplicht houdt namelijk in dat organisaties, instellingen en bedrijven die persoonsgegevens verwerken een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) direct nadat zij een datalek hebben ontdekt.

In bepaalde gevallen moet de datalek ook aan betrokkenen worden gemeld. Een betrokkene is degene van wie de persoonsgegevens zijn gelekt. De meldplicht is opgenomen in de Wet Bescherming Persoonsgegevens (Wbp). Voorbeelden van datalekken zijn: uitlekken van medische gegevens naar het internet, klantgegevens van twitteraars uitgelekt via een app, een gestolen laptop met persoonsgegevens, een zoekgeraakte usb-stick of een inbraak in een databestand.

De vraag is niet zozeer óf u met de meldplicht datalekken te maken krijgt, als wel wánneér dat het geval is

Sinds 1 januari jl. zijn er circa 1000 meldingen bij de Autoriteit Persoonsgegevens gedaan (stand van zaken: april 2016).

Wat is een datalek?

Wanneer is er sprake van een datalek? Een datalek is een inbreuk op de beveiliging van persoonsgegevens waarbij persoonsgegevens zijn blootgesteld aan verlies of onrecht-

matige verwerking. In feite zijn deze dan blootgesteld aan datgene waartegen beveiligingsmaatregelen nu juist bescherming hadden moeten bieden. Een datalek is meestal het gevolg van een beveiligingsprobleem. Overigens moet een datalek niet worden verward met een beveiligingslek. Dit is namelijk een inbreuk op de beveiliging, waarbij persoonsgegevens niet worden blootgesteld aan verlies of onrechtmatige verwerking. In dat geval is er dus ook geen sprake van een datalek.

Elk bedrijf verwerkt data en dus ook persoonsgegevens, zowel van klanten als medewerkers. Door het toenemende risico dat er data worden 'gelekt', bijvoorbeeld door een menselijke fout, ontoereikende beveiliging, fraude binnen de eigen organisatie en/of een bewuste criminele aanval van buitenaf, kunnen data in verkeerde handen vallen of verloren gaan.

Welke implicaties heeft dit voor bedrijven, organisaties en instellingen? Wanneer moet een datalek worden gemeld bij de Autoriteit Persoonsgegevens? Wat moet er exact worden gemeld? Welke preventieve maatregelen kunnen er worden getroffen? Welke afspraken kunnen en moeten er met medewerkers worden gemaakt? Op wie rust de meldplicht en wat als er niet – of niet tijdig – wordt gemeld?

Voor wie geldt de meldplicht datalekken?

De meldplicht geldt voor degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Deze wordt in de Wet bescherming persoonsgegevens (hierna: Wbp) aangeduid als de verantwoordelijke. Denk bijvoorbeeld aan de volgende situatie: een bedrijf houdt een klantenbestand van haar klanten bij in haar computersysteem. Deze gegevens zijn door NAW-gegevens te herleiden tot een individuele natuurlijke persoon, de betrokkene, dat wil zeggen degene op wie de persoonsgegevens betrekking hebben. Het bedrijf dat de persoonsgegevens bijhoudt, is in dit voorbeeld de verantwoordelijke. Onder persoonsgegevens vallen alle gegevens die herleidbaar zijn tot een geïdentificeerde of identificeerbare natuurlijke persoon (bijv. naam, e-mailadres, foto, medische gegevens, maar soms óók een IP-adres).

Onder het begrip 'verwerking' valt elke handeling die betrekking heeft op persoonsgegevens, van het moment

van verzameling tot vernietiging. Daaronder valt ook het opslaan van gegevens door een derde. Deze derde 'verwerkt' de gegevens in opdracht van de verantwoordelijke en wordt aangeduid als 'bewerker'. De verplichtingen van de bewerker moeten nauwgezet worden vastgelegd in een bewerkersovereenkomst. Het afsluiten van een bewerkersovereenkomst is een wettelijk vereiste dat volgt uit artikel 14 Wbp. De AP eist bovendien dat het contract tot in detail vermeldt welke instructies de verantwoordelijke aan de bewerker oplegt, welke beveiliging de bewerker zal toepassen, welke persoonsgegevens verwerkt zullen worden en voor welke doeleinden.

Beveiligingsverplichting Wbp

Op grond van artikel 13 Wbp is de verantwoordelijke verplicht om passende technische en organisatorische maatregelen ten uitvoer te (laten) leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. De maatregelen moeten bovendien een passend beschermingsniveau garanderen, gelet op de stand van de techniek en de kosten van de tenuitvoerlegging en gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De AP geeft in *Richtsoenen Beveiliging van Persoonsgegevens* aan wanneer er sprake is van een blijvend, passend beveiligingsniveau. Kijk op de website van de AP voor meer informatie: www.autoriteitpersoonsgegevens.nl.

Meldplicht

De meldplicht houdt in dat de verantwoordelijke een datalek moet melden bij de Autoriteit Persoonsgegevens. Altijd? Nee, alleen indien er kans is op verlies van gegevens of onrechtmatige verwerking van gegevens. Daarnaast moet degene die het betreft – de betrokkene – geïnformeerd worden. Het niet naleven van de meldplicht kan bestraft worden met een forse boete van de AP.

De betrokkene moet geïnformeerd worden indien er sprake is van "een inbreuk als bedoeld in eerste lid, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer." Indien de data echter effectief en up-to-date versleuteld zijn, heeft de verantwoordelijke geen meldplicht richting de betrokkene.

Inhoud van de melding

De melding aan het AP moet in elk geval de volgende informatie omvatten:

- 1 aard van de inbreuk;
- 2 instanties waar meer informatie over de inbreuk kan worden verkregen;
- 3 aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken (bijvoorbeeld: het veranderen van gebruikersnamen en wachtwoorden);
- 4 een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
- 5 maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.

Het risico op een boete

De Autoriteit Persoonsgegevens kan boetes tot 820.000 euro of tien procent van de jaaromzet opleggen voor over-

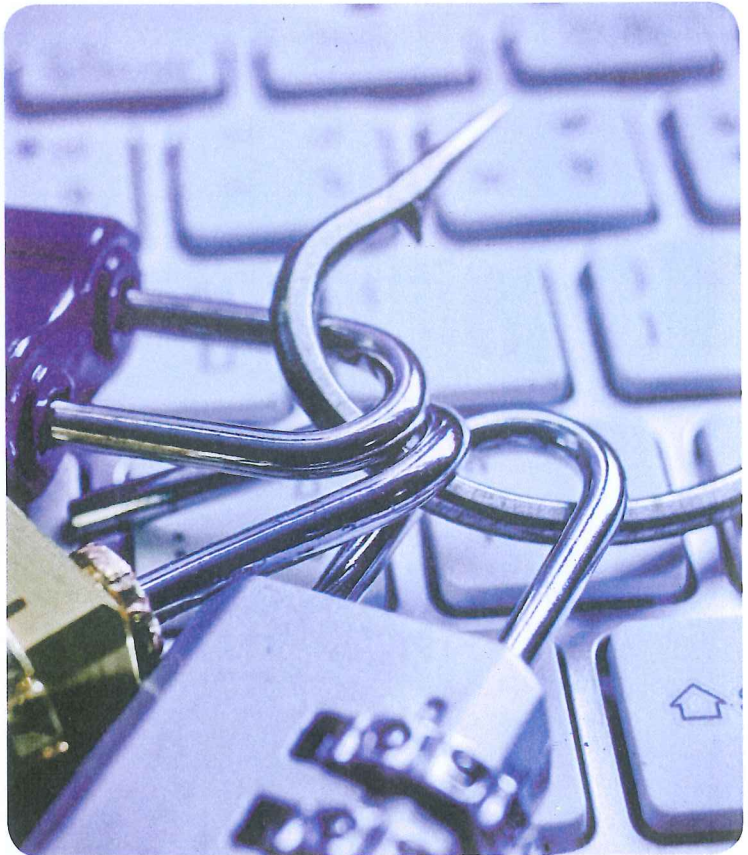


Foto: wk1003mike | shutterstock

trekking van diverse bepalingen van de Wet bescherming persoonsgegevens. De AP kan bijvoorbeeld een boete opleggen indien uw organisatie:

- persoonsgegevens verwerkt zonder hiervoor te beschikken over een vooraf vastgesteld gerechtvaardigd doeleinde en een grondslag (bijvoorbeeld de toestemming van de betrokkene);
- persoonsgegevens langer bewaart dan noodzakelijk is voor het doeleinde;
- onvoldoende beveiligingsmaatregelen neemt ter bescherming van persoonsgegevens tegen verlies of onrechtmatige verwerking;
- het verbod op verwerking van gevoelige persoonsgegevens – zoals ras, gezondheid of BSN – overtreedt, zonder een beroep te kunnen doen op een uitzonderingsgrond;
- een datalek niet meldt of geen overzicht bijhoudt van alle inbreuken op de beveiliging van persoonsgegevens.

De Autoriteit Persoonsgegevens kan voor overtredingen boetes tot 820.000 euro of tien procent van de jaaromzet opleggen

In principe zal de AP bij constatering van een overtreding eerst een bindende aanwijzing aan de overtreder geven. Dit geldt tenzij de overtreding opzettelijk is gemaakt of wanneer er sprake is van ernstig verwijtbare nalatigheid van de overtreder. De boete kan in dat geval direct worden opgelegd.



Logboek datalekken

Iedere organisatie dient verplicht een overzicht (logboek) bij te houden van datalekken die dusdanig ernstig waren dat ze aan de AP gemeld zouden moeten worden. Dit overzicht moet in ieder geval feiten en gegevens omtrent de aard van de inbreuk alsmede de tekst van de kennisgeving aan de betrokkene vermelden.

Wat moeten bedrijven en instellingen doen?

- Er is de noodzaak tot het afsluiten c.q. het aanpassen van bewerkersovereenkomsten. Verwerkt een externe partij persoonsgegevens voor u? Dan bent u verplicht een bewerkersovereenkomst te sluiten. Zet hierin dat hij de gegevens alleen in opdracht van u mag verwerken, en volgens uw instructies. Vermeld ook dat hij de boel goed moet beveiligen en een datalek aan u móet melden.
- Richt processen binnen uw organisatie in naar de regels op het gebied van privacy.
- Maak een datalekprotocol! Bedenk daarbij vooraf mogelijke scenario's bij datalekken en wat u in voorkomende gevallen kunt doen om mogelijke schade te beperken. Vermeld daarbij ook de punten die u moet doorgeven aan de AP, zoals hiervoor opgesomd onder het kopje 'inhoud van de melding'.
- Houd een logboek bij met een overzicht van de inbreuken.
- Zorg dat uw beveiliging op orde is, zowel technisch als ook organisatorisch.
- Versleutel gegevens indien dit tot de mogelijkheden behoort.

Conclusie

Datalekken zijn haast niet uit te sluiten dan wel te voorkomen, het treffen van adequate beveiligingsmaatregelen ten spijt. Organisaties kunnen echter veel ondervangen met goede contracten en het creëren van bewustzijn bij werknemers. Daarmee kan de schade, die ontstaat als gevolg van het datalek, zo veel mogelijk worden beperkt en tonen organisaties hun goede wil, wat bij een aansprakelijkheidsstelling en/of boete mee kan wegen. Duidelijk mogen zijn dat aspecten rondom beveiliging, datalekken en privacy vóór in een overeenkomst geregeld moeten worden. Het risico bij achterover leunen en niets doen is dat u als verantwoordelijke aansprakelijk kunt zijn voor alle schade die voortvloeit uit een datalek. Daarnaast kunt u een boete van de AP opgelegd krijgen. Om nog maar te zwijgen van de reputatieschade en mogelijke claims van betrokkenen. ●



Mirjam Elferink

mirjam.elferink@kienhuishoving.nl

Mirjam Elferink is werkzaam bij Kienhuis Hoving Advocaten.

Zie ook www.od-online.nl

brancheberichten



Gemeentelijk gebruik van big data

Big en open data zijn buzzwoorden en klinken ook bij gemeenten door. Er is overal informatie te vinden, maar hoe gebruiken gemeenten deze data voor hun dienstverlening? De afgelopen maanden inventariseerde KING door het hele land de data-innovatie bij gemeenten.

Zo krijgt Amsterdam een beter inzicht in het functioneren van de stad door het in kaart brengen van alle beschikbare data over water-, energie-, voedsel-, en materiaalstromen die door de stad lopen. Deze informatie benut de gemeente om tot duurzame strategieën te komen waarmee zij toe werkt naar een circulaire economie.

Een andere vraag werd in Nijmegen gesteld: burgers betrekken bij het aanpakken van luchtvervuiling, hoe doe je dat? Samen met de Radboud Universiteit bedacht de gemeente Nijmegen een plan. Met de samenwerking van burgers installeerden ze bij mensen thuis betaalbare sensoren. Dit maakt het mogelijk voor de gemeente om samen met haar inwoners de metingen van luchtkwaliteit, geluid, trillingen en meteorologische indicatoren uit te voeren.

Nederlanders helpen elkaar graag

In Nederland helpen we elkaar graag. Ruim twee op de vijf volwassenen deed het afgelopen jaar vrijwilligerswerk. Daarnaast voelt 89% van alle Nederlanders zich thuis in zijn of haar buurt en bijna twee derde helpt dan ook buurtgenoten met boodschappen of klusjes doen.

Dit blijkt uit het onderzoek Maatschappelijke veerkracht en vitaliteit van buurten. Het onderzoek laat een overwegend positief beeld zien over de gezondheid van buurten en de rek in de maatschappij. Uit de resultaten blijkt dat mensen van wie je het niet verwacht zich graag inzetten voor hun medemens. Opmerkelijk is ook dat de inzet voor leefbaarheid en veiligheid van de buurt hoog is onder inwoners met 'geen vertrouwen' in de gemeente en tevens hoog is onder inwoners met 'veel vertrouwen' in de gemeente.

Maar ook een aantal zorgwekkende uitkomsten komt naar voren uit het onderzoek. Zo heeft 6% van alle Nederlanders het gevoel 'er niet bij te horen', voelt 2% van de volwassenen in Nederland zich bijna altijd eenzaam en is tien procent van de mantelzorgers overbelast.