DePrivacyGuru

Datalekken

Hoe bereid je je voor, wanneer heb je er een en wat moet je dan doen?

Mr. Nico J. Mookhoek CIPP/E

Inhoudsopgave

Uit een onderzoek van DLA Piper blijkt dat Nederland in de periode mei 2018 tot 27 januari 2020 koploper is in het aantal gemelde datalekken (40.647). Duitsland en de U.K. komen met respectievelijk 37.636 en 22.181 gemelde datalekken op plaats 2 en 3.
Dit wil niet zeggen dat in deze landen minder datalekken plaatsvinden, het betreft hier het aantal gemelde incidenten bij de toezichthouders. Het kan dus heel goed dat in de landen die niet in de top 3 staan even veel of meer datalekken plaats vinden maar dat deze niet gemeld worden.

Hoe dan ook, de kans dat je met een datalek te maken krijgt is vrij groot. Zorg daarom dat je daar op voorbereid bent Deze White paper helpt je daarbij. We leggen je uit wanneer een beveiligingsincident een datalek is, wat je aan voorbereiding moet doen, wat je dan moet doen als je een datalek hebt, of je moet melden bij de toezichthouder en betrokkenen.

Wanneer is een beveiligingsincident een datalek?

Niet elk beveiligingsincident hoeft een datalek te zijn. Een aanval van hackers op je website waar geen persoonsgegevens worden achter gelaten is wel een beveiligingsincident, maar nog geen datalek.
Van een datalek is sprake als persoonsgegevens gecompromitteerd zijn geraakt. De AVG heeft het over "inbreuk in verband met persoonsgegevens".

In de AVG (art. 4.12) is gedefinieerd wanneer er sprake is van een inbreuk in verband met persoonsgegevens. Dat is het geval als ze:

- Vernietigd zijn
- Verloren zijn
- Gewijzigd zijn
- Verstrekt zijn
- Toegankelijk zijn geweest

zonder dat de organisatie die de persoonsgegevens verwerkt dit bewust heeft gedaan of hiertoe een wettelijke plicht bestaat.
Kort gezegd: er heeft zich een beveiligingsincident voor gedaan waardoor de persoonsgegevens komen op een plek waar ze niet horen.

Onder "Inbreuk in verband met persoonsgegevens" valt ook, zo bepaalde de WP 29 in één van haar guidelines, het niet toegankelijk zijn van de gegevens. geeft op haar website een
Op de voorbeeldlijst datalekken wel/ niet melden geeft de Autoriteit Persoonsgegevens ook voorbeelden van cases waarbij de gegevens niet meer toegankelijk.

Van een datalek is alleen sprake als de beveiliging van persoonsgegevens daadwerkelijk geschonden is. Het risico op een datalek bijvoorbeeld door een zwakke plek in de beveiliging is nog geen datalek. De persoonsgegevens moeten door dat lek daadwerkelijk in het ongerede geraakt zijn.

De manieren waarop dit kan gebeuren, zijn legio. Vaak wordt bij een datalek gedacht aan het hacken van bijvoorbeeld een database. Maar veel vaker ontstaat een het door een fout in een verzendlijst van een email. In plaats van het BBC veld waarbij de adressen niet zichtbaar zijn, wordt het CC veld gebruikt waardoor alle geadresseerden de mail adressen kunnen zien.

Dit is maar een van de voorbeelden. In de praktijk kom ik ook vaak de onderstaande oorzaken tegen.

- Slordig om gaan met wachtwoorden, helemaal geen of een te eenvoudig wachtwoord gebruiken.
- Gebruik van een USB stick waar persoonsgegevens op staan of een overzicht met wachtwoorden en dat voor de veiligheid van werk mee naar huis genomen wordt
- Het hacken van systemen en phishing mails
- Computerbestanden die in onbevoegde handen zijn gekomen
- Een geprinte leerlingenlijst die gestolen of verloren is
- Een laptop met persoonsgegevens die gestolen is of de toegang geeft tot persoonsgegevens
- Afgedankte niet-schoongemaakte computers met persoonsgegevens
- Een gestolen zakelijke mobiele telefoon
- Brand in de serverruimte (ja, echt mee gemaakt)

De toelichting op de AVG geeft aan dat het datalek kan resulteren in lichamelijke, materiele of immateriële schade voor natuurlijke personen. Dat kan bijvoorbeeld zijn verlies van controle over de persoonsgegevens, reputatieschade discriminatie, identiteitsdiefstal, verlies van vertrouwelijkheid van de door het beroepsgeheim beschermde persoonsgegevens, of enig ander aanzienlijk economisch of maatschappelijk nadeel.

Let op: voorde vraag of je een datalek hebt is het niet relevant dat die schade zich ook daadwerkelijk voordoet. Het risico erop is al voldoende.

Haal de schaamte weg

Zowel bij medewerkers als directies heerst er nog vaak onterechte schaamte over beveiligingsincidenten, zeker als daarbij persoonsgegevens zijn gecompromitteerd. De cijfers in de inleiding geven aan dat die schaamte onterecht is: veel organisaties krijgen met een datalek door een beveiligingsincident te maken. Kortom: je bent in goed gezelschap

De eerste stap is dan ook om mogelijke schaamte weg te halen. Immers als men zich schaamt voor een beveiligingsincident met mogelijk een datalek is de kans groot dat deze weg gemoffeld wordt. Het is dan een onbeheerst risico: het datalek kan op een ander moment toch opeens boven water komt.
Om beveiligingsincidenten en datalekken in kaart te krijgen is een veilige omgeving nodig. Een omgeving waarbij medewerkers fouten toe durven geven en samen met het management/ directie daarvan proberen te leren.

Ter afsluiting van dit deel nog wat voorbeelden van spraakmakende datalekken, en zeker niet van de eerste beste organisaties.

Tadaah: door een onbeveiligde, publiek toegankelijke server bij deze dienstverlener in de zorg waren ID bewijzen, VOG's (Verklaring Omtrent Gedrag), verzekeringen en diploma's van enkele honderden mensen in te zien.
EasyJet werd getroffen door een zoals ze zelf zeggen "zeer geavanceerde cyberaanval". Daarbij werden e-mailadressen en reisplannen van negen miljoen klanten gestolen. Daarnaast wisten de daders de creditcardgegevens van 2.208 klanten in handen te krijgen. heeft de database uit de lucht gehaald.

Rijksinstituut voor Volksgezondheid en Milieu (RIVM): de Infectieradar waar Nederlanders aan kunnen geven of ze last hebben van coronaklachten, bevatte een ernstig datalek.

Europees Parlement, de Europese Raad en de Europese Commissie: gegevens en wachtwoorden van tweehonderd leden waren toegankelijk voor onbevoegden.

Universitair Medisch Centrum Utrecht: harde schijven met medische gegevens van zo'n zevenhonderd patiënten zijn gestolen.

Het CIBG, een uitvoeringsorganisatie van het ministerie van Volksgezondheid, ontdekte dat twee externe harde schijven niet meer in de daarvoor bestemde kluis lagen. Op deze harde schijven staat een back-up van 6,9 miljoen donorformulieren van de periode februari 1998 tot juni 2010.

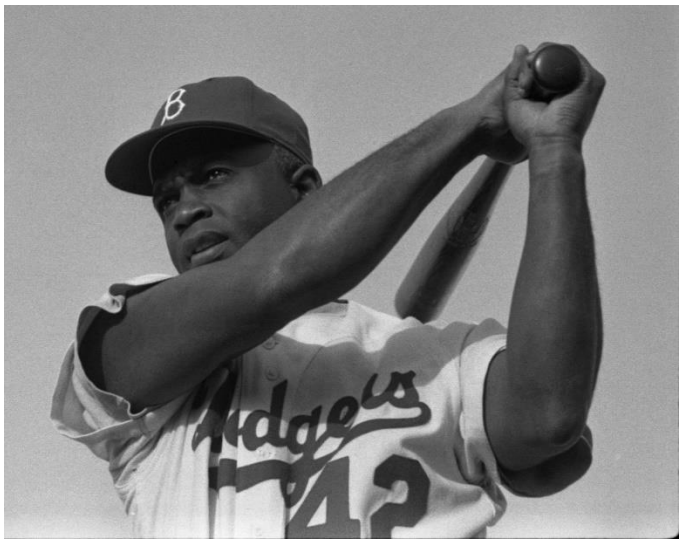
Procedure beveiligingsincidenten & datalekken

Zorg dat je voorbereid bent voor het geval je gebeld wordt dat er een beveiligingsincident is dat mogelijk een datalek is.

Dat doe je door op voorhand een procedure beveiligingsincidenten op te stellen. Daarin leg je onder andere vast bij wie het incident moet worden gemeld als een medewerker dat ontdekt. Wie de afweging maakt of ook sprake is van een datalek, wie maatregelen treft, wie verantwoordelijk is voor de melding bij de AP etc.
Zorg er voor dat medewerkers op de hoogte zijn bij wie het incident moet worden gemeld en dat ze incidenten met een mogelijke inbreuk op de persoonsgegevens herkennen en meteen melden.

In het pakket "datalekken" dat je in onze webshop kunt bestellen, is ook een model procedure opgenomen.

Wat te doen bij een datalek?



Als je een datalek gemeld krijgt, is de eerste stap overzicht krijgen over het lek. Stel daarbij de volgende vragen:

- Hoe zijn persoonsgegevens gelekt?
- Hoe zijn de gegevens gecompromitteerd geraakt (zie het lijstje boven)
- Wat is de aard van de gegevens? Zijn er bijzondere persoonsgegeven gelekt?
- Wie zouden door de lek toegang tot de gegevens kunnen krijgen?

Bij de melding ga je direct kijken wat je kunt doen om de schade te beperken en het lek te stoppen. Denk daarbij aan:

- De database offline zetten
- Het systeem down brengen
- De laptop op afstand wissen

Nadat je deze first response acties hebt uitgevoerd, ga je beoordelen wat je met het datalek moet doen.
Moet je het melden bij de toezichthouder? Melden aan betrokkenen?

Echt duidelijke regels wanneer je een datalek moet melden aan de AP en aan de betrokkenen zijn er niet. Als je twijfelt, kun je altijd een voorlopige melding bij de AP doen. Deze kun je later weer intrekken. Hiermee voorkom je dat een

datalek dat na nadere analyse meldingsplichtig blijkt niet binnen de 72 uur hebt gemeld.

Voor de melding aan de AP geldt de volgende vuistregel. Altijd melden als;

- het gaat om een datalek van bijzondere gegevens of gegevens van gevoelige aard
- er om een andere reden sprake van ernstige nadelige gevolgen voor bescherming van de verwerkte persoonsgegevens van betrokkenen?

Voor de melding aan de betrokkenen geldt dat gemeld moet worden als:

- de gegevens niet goed versleuteld waren
- het datalek om andere redenen ongunstige gevolgen heeft voor de persoonlijke levenssfeer van betrokkenen moet je ook melden.

De Autoriteit Persoonsgegevens geeft op haar website een voorbeeldlijst wanneer je een datlek wel/ niet moet melden.

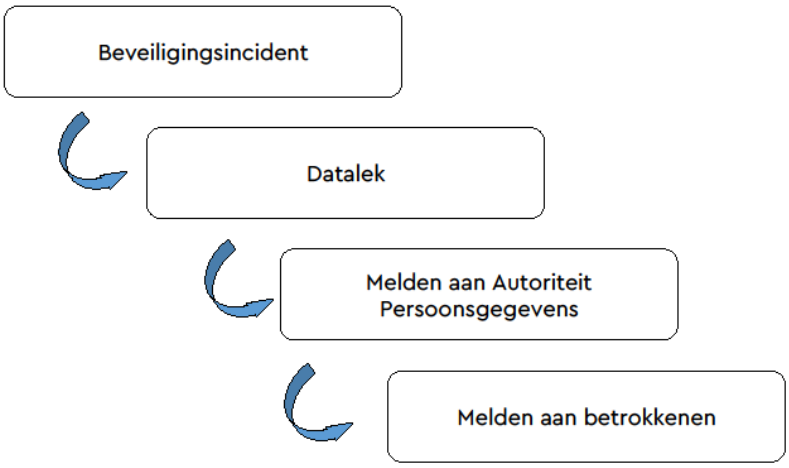
De melding aan zowel de AP als aan de betrokkenen kennen dus beide een open norm waarbij je zelf de afweging moet maken of je meldt of niet.

Dat betekent dat je goede afweging moet maken die aantoonbaar is. Leg die afwegingen waarom je wel of niet gemeld hebt, vast in het register datalekken, eventueel indien nodig separaat met een uitvoeriger toelichting.

Hieronder vind je stapsgewijs de afwegingen die je moet maken.

Bijlage bij procedure datalekken: stappen onderzoek beveiligingslek

Heeft zich een beveiligingsincident voorgedaan?



Zijn bij het incident persoonsgegevens verloren gegaan of is onrechtmatige verwerking niet uit te sluiten? (*Denk niet alleen aan elektronisch verlies maar ook fysiek: diefstal laptop, verlies USB-stick etc.)*

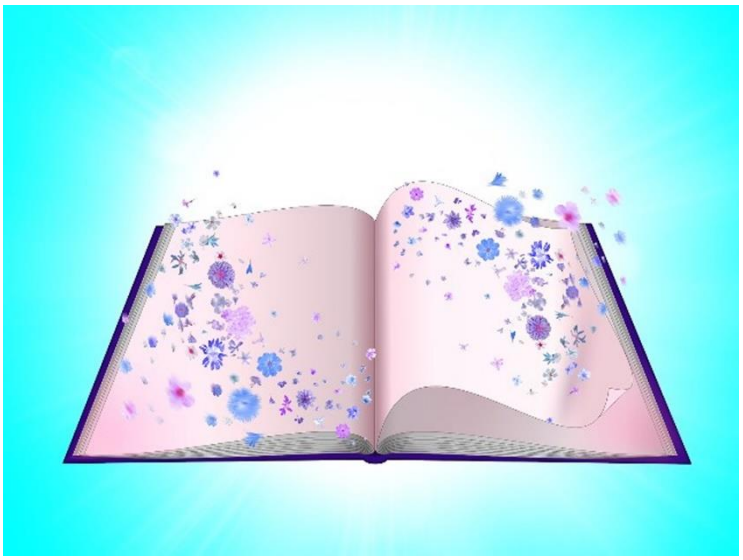
Gaat het om persoonsgegevens van gevoelige aard of is er om een andere reden sprake van ernstige nadelige gevolgen voor bescherming van de verwerkte persoonsgegevens van betrokkenen?
(Zie p.2)

Waren alle gelekte gegevens niet goed versleuteld of heeft de het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkenen?

(Bron: Autoriteit Persoonsgegevens: Beleidsregels meldplicht datalekken)

1

Register datalekken
&
PDCA-cyclus



Van alle datalekken doe je verslag in je Register Datalekken, dus ook de datalekken die je niet meldt aan de AP of aan de betrokkenen.

Het doel van het register is tweeledig je maakt je inspanningen voor de AVG op het gebied van datalekken aantoonbaar, wat een eis is van de AVG. Je laat zien welke maatregelen getroffen zijn en je motiveert waarom het datalek wel of niet is gemeld bij de AP en betrokkenen.

Maar het register is vooral een middel om de PDCA-cyclus te doorlopen. Het helpt je om de bescherming van persoonsgegevens te vergroten. Periodiek, bijvoorbeeld jaarlijks, of bij grotere organisaties maandelijks, analyseer je het register. Je kunt bij die analyse de datalekken categoriseren op basis van:

- het soort datalek
- de maatregelen die je hebt getroffen
- de betrokkenen
- de gevolgen van het datalek

Bij die analyse kijk je of de getroffen maatregelen gewerkt hebben of aanpassing behoeven, of dat op basis van de analyse nieuwe preventieve maatregelen nodig zijn. Die voer je vervolgens in. In de volgende analyse doorloop je dezelfde cyclus: je kijkt of getroffen maatregelen aangepast moeten worden, eventueel nieuwe preventieve maatregelen nodig zijn etc.

In het register omschrijf je de beveiligingsincidenten die zijn voorgevallen, de gevolgen en de maatregelen die getroffen zijn. De maatregelen categoriseer in je in corrigerende en preventieve maatregelen.
Met een corrigerende maatregel wordt meteen in gegrepen. Dat kan bijvoorbeeld zijn het isoleren van de database die gelekt heeft.
Een preventieve beoogt het beveiligingsincident in de toekomst te voorkomen. Een voorbeeld van een preventieve maatregel is het installeren van andere beveiligingssoftware.
Per incident neem je ook op of de FG betrokken is. En zoals boven gezegd je neemt je onderbouwing op waarom een datalek wel of niet gemeld is aan is bij de AP en de betrokken personen.
Als laatste leg je vast welke andere organisaties eventueel betrokken zijn geweest bij de inbreuk. Bijvoorbeeld medeverwerkingsverantwoordelijken, verwerkers of sub verwerkers.

In onze webshop kun je in het pakket "datalekken" bestellen, dat bevat:

- een register dat voldoet aan de eisen van de AP,
- een model procedure datalekken
- een stappenplan bij een datalek

DePrivacyGuru

Wij helpen je graag met het opstellen en implementeren vaan goede procedure datalekken zodat jij weet wat je moet doen als een beveiligingsincident een inbreuk op de persoonsgegevens blijkt te zijn.

Daarnaast worden we ook regelmatig ingeschakeld voor een second opinion in het geval er een datalek heeft plaats gevonden. Wij helpen dan op basis va n onze ervaring de benodigde afwegingen te maken.

Meer informatie: www.deprivacyguru.nl

info@deprivacyguru.nl

085-2223232

DePrivacyGuru: "Privacy zonder gedoe"