TOOLKIT

Stappenplan datalekprotocol

DPO Consultancy
Experts in Data Privacy

MEI 2021

Organisaties zijn wettelijk verplicht om datalekken direct te melden bij de Autoriteit Persoonsgegevens. In sommige gevallen zijn organisaties ook verplicht een datalek te melden bij de personen van wie de persoonsgegevens zijn gelekt. Dit is afhankelijk van de ernst van het datalek en de gevolgen voor de betrokkenen. Een datalek kan iedere organisatie overkomen, het belangrijkste is hoe dit datalek wordt afgehandeld en welke vervolgstappen er worden genomen om datalekken in de toekomst te voorkomen.

Wat is een datalek?

Een datalek is volgens de Algemene Verordening Gegevensbescherming (AVG) een inbreuk op de beveiliging van persoonsgegevens. Persoonsgegevens zijn gegevens die direct of indirect te herleiden zijn naar een persoon. We spreken van een datalek als persoonsgegevens worden verloren, vernietigd of gewijzigd zonder dat dit de bedoeling is van een organisatie, of als onbevoegden toegang krijgen tot persoonsgegevens.

Voorbeelden van datalekken zijn:

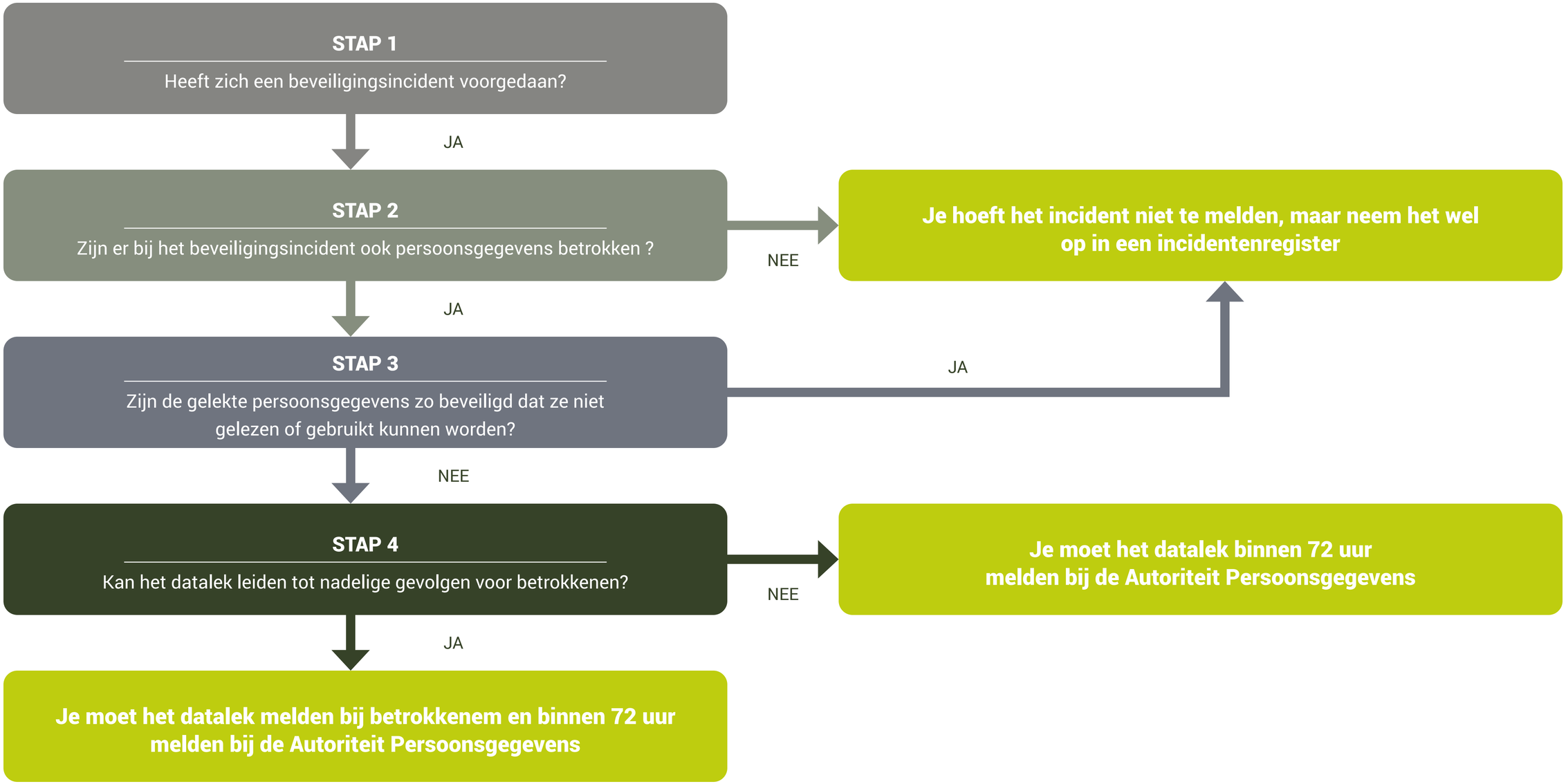
- Een kwijtgeraakte usb-stick met daarop persoonsgegevens
- Een gestolen werklaptop, tablet of mobiele telefoon zonder encryptie;
- Een inbraak door een hacker
- Verzending van een e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;
- Een besmetting met ransomware
- Het verstrekken van persoonsgegevens aan een onbevoegde persoon buiten de organisatie
- Papieren documenten met persoonsgegevens die op straat belanden
- Een kwetsbaarheid in een applicatie waardoor persoonsgegevens door alle gebruikers te zien zijn

Datalekprotocol

Bij een datalek is het belangrijk om als organisatie te weten welke stappen je moet zetten, wanneer je dat moet doen en aan wie je een datalek moet melden. Die stappen zijn beschreven in een datalekprotocol. Het doel van een datalekprotocol is om op gecontroleerde wijze om te gaan met de gevolgen van een datalek. Het is een plan waarmee organisaties kunnen bepalen of een datalek gemeld moet worden, hoe dit moet gebeuren en wie welke rol vervult als er een datalek is.

Met dit stappenplan helpen we je organisatie om een datalekprotocol op te stellen. We leggen je uit welke procedures er in het protocol moeten staan en welke stappen je moet doorlopen. Zo houd je altijd controle over de situatie.

“Passwords are like underwear: don’t let people see it, change it very often, and you shouldn’t share it with strangers.” Chris Pirillo


STAP 1
Heeft zich een beveiligingsincident voorgedaan?
JA
STAP 2
Zijn er bij het beveiligingsincident ook persoonsgegevens betrokken ?
NEE
Je hoeft het incident niet te melden, maar neem het wel op in een incidentenregister
JA
STAP 3
Zijn de gelekte persoonsgegevens zo beveiligd dat ze niet gelezen of gebruikt kunnen worden?
JA
NEE
STAP 4
Kan het datalek leiden tot nadelige gevolgen voor betrokkenen?
NEE
Je moet het datalek binnen 72 uur melden bij de Autoriteit Persoonsgegevens
JA
Je moet het datalek melden bij betrokkenem en binnen 72 uur melden bij de Autoriteit Persoonsgegevens

De stappen van het datalekprotocol

In het datalekprotocol worden verschillende stappen opgenomen die een organisatie moet doorlopen als een datalek ontdekt wordt. Om je te helpen bij het opstellen van een protocol, staan in de onderstaande flowchart de verschillende vragen die je als organisatie moet beantwoorden bij een datalek. Per vraag geven we een toelichting, waarmee je alle informatie hebt om voor jouw organisatie een datalekprotocol op te stellen.

STAP 1

Heeft zich een beveiligingsincident voorgedaan?

Als organisatie probeer je de persoonsgegevens die je bewaart zo goed mogelijk te beveiligen. Maar soms gaat er is iets mis. Je hebt bijvoorbeeld zelf geen toegang meer tot je gegevens of buitenstaanders krijgen onbedoeld toegang. Dan is er sprake van een beveiligingsincident. Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of kan komen.

STAP 2

Zijn er bij het beveiligingsincident ook persoonsgegevens betrokken?

Er is sprake van een datalek als door een inbreuk op de beveiliging of ander incident, de vertrouwelijkheid, integriteit en/of beschikbaarheid van persoonsgegevens niet gegarandeerd kan worden. Bijvoorbeeld als de gelekte gegevens namen, e-mailadressen, adresgegevens of burgerservicenummers bevatten.

Niet ieder beveiligingsincident leidt direct tot een datalek. Als er geen sprake is van een datalek, neem dit incident dan wel op in een intern incidentenregister. Iedere organisatie is verplicht om zo'n incidentenregister bij te houden. Hierin wordt bijgehouden welke incidenten er hebben plaatsgevonden. Het doel van dit register is om te leren van eerdere incidenten en maatregelen treft om de kans op nieuwe datalekken te verkleinen. Daarnaast helpt dit register je organisatie om te voldoen aan de verantwoordingsplicht die in de AVG is opgenomen. De Autoriteit Persoonsgegevens kan vragen om dit register te delen.

Meldplicht datalek

Als er sprake is van een datalek wil je als organisatie weten wanneer en hoe je het datalek moet melden. Daarvoor maken we onderscheid tussen de meldplicht aan de Autoriteit Persoonsgegevens en de meldplicht aan de betrokkenen.

STAP 3

Zijn de gelekte persoonsgegevens zo beveiligd dat ze niet gelezen of gebruikt kunnen worden?

Wanneer de informatie door de organisatie geanonimiseerd, gepseudonimiseerd of op een andere wijze versleuteld is, kan het zijn dat het geen datalek betreft. Bijvoorbeeld een beveiligde verloren usb-stick met persoonsgegevens is geen datalek, omdat de data op de usb-stick niet kan worden geraadpleegd zonder de decryptiesleutel. De norm die je hierbij moet hanteren is zeer streng. Gegevens mogen pas als onbegrijpelijk of ontoegankelijk beschouwd worden als ze aan één van de volgende voorwaarden voldoen:

- De gegevens zijn op een veilige manier versleuteld met een algoritme. De sleutel voor decryptie is door geen enkele inbreuk in gevaar en wordt zodanig gegenereerd, dat personen zonder geautoriseerde toegang de sleutel - met de beschikbare technologische middelen - niet kunnen vinden.
- De gegevens zijn vervangen met hashwaarden, die cryptografisch zijn versleuteld met een hashfunctie. De sleutel die hiervoor wordt gebruikt is door geen enkele inbreuk in gevaar en is zodanig gegenereerd, dat personen zonder geautoriseerde toegang de sleutel niet kunnen vinden met de beschikbare technologische middelen.

Naast encryptie wordt ook het op afstand wissen van de gegevens die op een apparaat staan (remote wiping) genoemd als technische beschermingsmaatregel van persoonsgegevens. Hiervoor moet echter aan een aantal randvoorwaarden worden voldaan.

- De remote wipe wordt op tijd in gang gezet, zodat onbevoegden geen kans hebben gehad om kennis te nemen van de gegevens.
- Het apparaat waarvan de gegevens worden gewist, moet nog intact zijn en werken, zodat de remote wipe uitgevoerd kan worden.
- De toepassing voor het wissen van de gegevens moet correct werken, zodat alle persoonsgegevens daadwerkelijk worden verwijderd en er ook geen sporen achterblijven waarmee de oorspronkelijke gegevens kunnen worden gereconstrueerd.

Indien het incident leidt tot een incident met persoonsgegevens dient het lek te worden gemeld bij de Autoriteit Persoonsgegevens binnen 72 uur nadat de organisatie kennis heeft genomen van het datalek.

STAP 4

Kan het datalek leiden tot nadelige gevolgen voor betrokkenen?

Het datalek moet worden gemeld aan betrokkenen als de inbreuk waarschijnlijk een hoog risico zal hebben voor de rechten en vrijheden van de betrokkenen. Hierbij kan de schade fysiek, materieel of immaterieel zijn. Fysieke schade gaat bijvoorbeeld over het wissen van medische gegevens, waardoor iemand niet de benodigde zorg krijgt. Bij materiële schade bestaat de kans dat iemand financieel verlies lijdt of het slachtoffer wordt van identiteitsfraude. En bij immateriële schade gaat het bijvoorbeeld over onrechtmatige publicatie, aantasting in eer en goede naam of discriminatie.

Bij persoonsgegevens van gevoelige aard (ook wel bijzondere categorieën persoonsgegevens volgens de AVG) is het risico dat de rechten en vrijheden van de betrokkenen worden geschonden veel hoger. Zo kan verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering, uitsluiting, schade aan de gezondheid, financiële schade of tot (identiteits)fraude van betrokkenen. Voorbeelden van bijzondere categorieën van persoonsgegevens zijn:

- Gegevens over iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, geaardheid of lidmaatschappen.
- Strafrechtelijke persoonsgegevens. Denk bijvoorbeeld aan een gebiedsverbod of verkeersboetes.
- Financiële of economische gegevens over schulden, salaris- en betalingsgegevens.
- Gegevens over bijvoorbeeld verslavingen, school- of werkprestaties of relatieproblemen die kunnen leiden tot stigmatisering of uitsluiting van personen.

- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen hangen af van waar de inloggegevens toegang toe geven. Met inachtneming dat veel mensen wachtwoorden hergebruiken voor verschillende accounts.
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Hierbij gaat het onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en burgerservicenummers.

De omvang en de aard van het datalek kunnen ook leiden tot ernstige nadelige gevolgen voor betrokken. Datalekken bij overheidsinstellingen, banken of verzekeraars kunnen onder andere leiden tot financiële schade voor betrokkenen. Daarom moet je als organisatie ook vaststellen of een datalek ernstige nadelige gevolgen heeft voor personen óf dat de kans op ernstige gevolgen aanzienlijk is toegenomen. Daarbij zijn de volgende zaken relevant:

- Bij een datalek moet altijd bepaald worden hoe aantrekkelijk de gegevens zijn voor misbruik. Als er persoonsgegevens zijn gelekt van grote groepen kwetsbare mensen of meerdere gegevens van één individu – zoals een publiek figuur – neemt de kans toe dat gegevens worden misbruikt of doorverkocht. Met als gevolg dat betrokkenen op langere termijn last kunnen hebben van het datalek.
- Indien een organisatie persoonsgegevens verwerkt om beslissingen te nemen die gevolgen hebben voor de betrokkenen personen, neemt ook het risico op de rechten en vrijheden van deze betrokkenen toe. Bijvoorbeeld: als een organisatie financiële persoonsgegevens gebruikt om iemands kredietwaardigheid te bepalen zijn de gevolgen van verlies en onrechtmatige verwerking van de gegevens ingrijpender dan bij gebruik van persoonsgegevens voor marketingdoeleinden.
- Bij de overheid worden persoonsgegevens vaak tussen verschillende instanties gedeeld, waardoor een datalek op verschillende plekken in de keten gevolgen kan hebben. Voor betrokkenen wordt het daardoor moeilijker om de mogelijke gevolgen van een datalek te overzien en zich daartegen te beschermen.

Als de aard en omvang van het datalek voldoen aan één van de bovenstaande criteria, dan is er een aanzienlijke kans dat het datalek ernstige nadelige gevolgen heeft voor de betrokkenen.

Aan de hand van de criteria uit stap 4 kan je organisatie een inschatting maken of de betrokkenen geïnformeerd moeten worden over het datalek. Het is geen eenvoudig vraagstuk, omdat de impact van een datalek (bijna) nooit te vergelijken is met andere datalekken. Je moet als organisatie echt goed kijken naar de mogelijke impact die het datalek heeft op het leven van de betrokkenen. Behandel daarom ieder datalek als een unieke gebeurtenis en beoordeel (leg dit ook schriftelijk vast) per incident of een melding aan de betrokkenen moet plaatsvinden.

Aan de slag

Door het volgen van bovenstaande stappen ben je als organisatie in staat om zelf een datalekprotocol op te stellen. Naast het opstellen is de implementatie van het protocol van groot belang, zodat alle betrokken partijen weten wat er van hen verwacht wordt bij een beveiligingsincident.

Kom je er niet helemaal uit, of heb je nog aanvullende vragen bij specifieke onderwerpen? Neem dan contact met ons op via info@dpoconsultancy.nl of +31 85 0711080

Australiëlaan 12a
5232 BB 's-Hertogenbosch
the Netherlands

Rue du Congres 35
1000 Brussel
Belgium

1 Lyric Square
London, W6 0NB
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com