Procedure Meldplicht Datalekken

Inhoud

Versie: 1.0

1. Wat is de meldplicht datalekken?

Sinds 1 januari 2016 is in Nederland het wetsvoorstel voor een brede meldplicht datalekken in werking getreden. Dat houdt in dat Amnesty Nederland (AINL) o.l.v. de Manager Fondsenwerving & Marketing (MF&M) en de Data Protection Officer (DPO) (nog te benoemen) binnen 72 uur na het ontdekken van een datalek hiervan melding moet doen bij de Autoriteit Persoonsgegevens (AP) en mogelijk bij de betrokkene als het lek (kans op) ernstige nadelige gevolgen heeft voor de privacy van de betrokkenen.

Naast een meldplicht introduceert het wetsvoorstel een protocolplicht. De protocolplicht houdt in dat AINL een overzicht moet bijhouden van alle datalekken die zijn ontdekt, met daarbij de overweging waarom deze wel of niet gemeld zijn bij de AP en/of bij betrokkenen (de mensen die het betreffende bestand staan).

Hoe een organisatie betrokkenen over een datalek informeert kan consumentenvertrouwen en reputatie schaden of juist verstevigen. Het is daarom zaak dat AINL voorbereid is:

- om te voldoen aan de wettelijke meldplicht bij de AP en de notificatieverplichting aan de betreffende personen.
- op aandacht van de media. Data en privacy zijn onderwerpen die in een brede belangstelling staan.

2. Melden van beveiligingsincidenten

In de interne instructie en externe instructie van AINL is opgenomen dat beveiligingsincidenten binnen respectievelijk 1 uur en 4 uur moeten worden gemeld op **compliance@amnesty.nl**.

Bewerkers hebben doorgaans meer tijd dan AINL medewerkers nodig voordat zij de melding kunnen doen, omdat zij een incident graag eerst kort onderzoeken. Het is echter zaak dat zowel medewerkers als (medewerkers) van bewerkers zelf géén melding doen bij de AP en/of betrokkenen. Een beveiligingsincident kwalificeert pas als een datalek als er daadwerkelijk persoonsgegevens bij zijn betrokken.

Zodra een beveiligingsincident wordt gemeld, draagt de afdeling IT in samenwerking met de externe helpdesk van OGD zorg voor de technische afhandeling en voor passende beveiligingsmaatregelen. Deze procedure wordt nader beschreven in het (nog op te stellen) informatiebeveiliging- en privacybeleid.

Contactpersonen betrokken bij de technische afhandeling van beveiligingsincidenten bij Amnesty Nederland zijn:

Ed van Velzen	Senior IT Medewerker	020-77 33 770	e.vanvelzen@amnesty.nl
OGD	Helpdesk	(extern) 088-6500000, (intern) 777	servicedesk@ogd.nl
Michael Salemink	Manager Ondersteuning	020-77 33 805	m.salemink@amnesty.nl

3. Beoordeling beveiligingsincidenten: datachecks

Binnen AINL zijn de Manager F&M en de DPO verantwoordelijk voor het beoordelen van beveiligingsincidenten in het kader van de Meldplicht Datalekken.

Alle incidenten van (personeel van) bewerkers en van medewerkers van AINL worden gemeld op **compliance@amnesty.nl**. Zodra hier een melding op binnenkomt dient de beoordeling van het incident te starten. Er is immers maximaal slechts **72 uur** de tijd om, als het beveiligingsincident kwalificeert als datalek, waarvan melding moet worden gemaakt, de melding ook daadwerkelijk uitgevoerd te hebben.

Om goed te kunnen beoordelen of een beveiligingsincident gemeld dient te worden bij de AP en bij betrokkenen heeft de AP in haar beleidsregels voor toepassing van de meldplicht datalekken een aantal checks opgenomen. Deze checks zijn:

1. **Is er sprake van verwerking van persoonsgegevens?**
2. **Is er sprake van een datalek?**

De meldplicht datalekken is alleen van toepassing op een beveiligingslek waarbij persoonsgegevens gecompromitteerd zijn. Dit zijn gegevens die betrekking hebben op of herleid kunnen worden naar een persoon in onze database. Als persoonsgegevens door een beveiligingsincident in handen (kunnen) komen van een onbevoegde is er sprake van een inbreuk op de beveiliging van persoonsgegevens. Ook in het geval persoonsgegevens verloren zijn gegaan of niet kan worden uitgesloten dat deze onrechtmatig verwerkt zijn, treedt de procedure Meldplicht Datalekken in werking.

3. **Moet het datalek gemeld worden aan de toezichthouder?**

Indien sprake is van (een kans op) nadelige gevolgen voor de privacy van de mensen in het bestand dan moet het datalek gemeld worden aan de AP. Hiervan is sprake wanneer er risico is op misbruik en fraude. Dit risico is groter naarmate de gegevens gevoeliger

zijn of als het gaat om grote datasets. Bij grote datasets of datasets met gegevens van gevoelige aard moet een lek gemeld worden aan de AP.

4. Moet het datalek gemeld worden aan de betrokkenen?

Alleen een datalek dat aan de AP gemeld moet worden, moet potentieel ook gemeld worden aan de betrokkenen. Alleen voor financiële ondernemingen geldt een uitzondering.

Wanneer er als gevolg van een datalek persoonsgegevens zijn vernietigd of aangetast moet dit gemeld worden aan de betrokkenen. Dit kan echter achterwege blijven als er afdoende technische beveiligingsmaatregelen zijn getroffen waardoor de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden. Of als dit noodzakelijk is voor de bescherming van de betrokkenen. In dit geval moet bij de melding aan de autoriteit worden aangegeven wat de reden is om melding aan de betrokkenen achterwege te laten.

Voor meer informatie over de datalek checks zie de stroomdiagrammen en toelichting in de bijlagen.

4. Procedure melding datalek

Direct na het ontdekken van een datalek informeren de Manager F&M en de Data Protection Officer, de directie, Manager Media & Politieke zaken en de Manager Ondersteuning. En zorgen zij voor de melding aan de AP (binnen 72 uur na het ontdekken van een datalek).

In het geval een datalek (kans op) ernstige nadelige gevolgen heeft voor de privacy van de betrokkenen, vormen zij een crisisteam met hierin de directie, Manager Media & Politieke zaken en Manager Ondersteuning. In overleg wordt dan bepaald hoe en door wie over het datalek gecommuniceerd wordt naar de belanghebbenden.

De communicatiedoelgroepen bij een datalek zijn:

- Servicedesk
- Donateurs
- Publiek
- Overige medewerkers
- Vrijwilligers
- Media
- Toezichthouders
- Politiek

Standaardteksten voor een notificatie en voor communicatie naar de media zijn vermeld in de bijlagen.

In het geval de ernst van het datalek dusdanig groot is en mogelijk leidt tot negatieve publiciteit en risico op imagoschade treedt het Crisiscommunicatieplan in werking. Het call center van Ditmeijer kan worden ingeschakeld voor de afhandeling van inkomende telefoontjes.

Contactpersonen betrokken bij de procedures omtrent de beoordeling van datalekken bij Amnesty Nederland zijn:

(nog te benoemen)	Data Protection Officer	x	x
Dhr. B. van Kuijk	Manager Fondsenwerving & Marketing	06-28883825	b.vankuijk@amnesty.nl
Dhr. P. Jordens	Consultant DMCC	06-15058797	patrick.jordens@dmcc.nl
Mw. J. van Doodewaerd	Consultant DMCC	06-25516373	jitty.van.doodewaerd@dmcc.nl

5. Melding datalek bij de Autoriteit Persoonsgegevens

Indien sprake is van een datalek dat dient te worden gemeld bij de Autoriteit Persoonsgegevens, dient het lek te worden gemeld op de website van de AP. Dat kan via de volgende link:

https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Onderaan de pagina vinden we de volgende mogelijkheden terug:

Zoals uit bovenstaande figuur blijkt kan een melding in een later stadium ook worden **gewijzigd** of **ingetrokken**.

De meldingspagina wijst zichzelf, maar het is van groot belang dat er voor het doen van de daadwerkelijke melding is nagedacht over alle aspecten van het datalek. Er dient tenminste duidelijk te zijn:

1. Wie de interne contactpersoon is bij AINL voor de Autoriteit Persoonsgegevens.
2. Wat de omvang van het lek is.
3. Welk type persoonsgegevens er bij het lek betrokken zijn.

4. Wat de aard van de inbreuk is.
5. Welke gevolgen het lek kan hebben voor de betrokkenen.
6. Wat de vervolgacties zijn (geweest) naar aanleiding van het lek.
7. Of de betrokkenen zijn (of worden geïnformeerd) en hoe.
8. Als betrokkenen niet worden geïnformeerd, waarom niet.
9. Welke technische beveiligingsmaatregelen van kracht waren toen het lek ontstond.

Bij alle contacten met de Autoriteit Persoonsgegevens is het van belang dat AINL laat zien dat zij in control is.

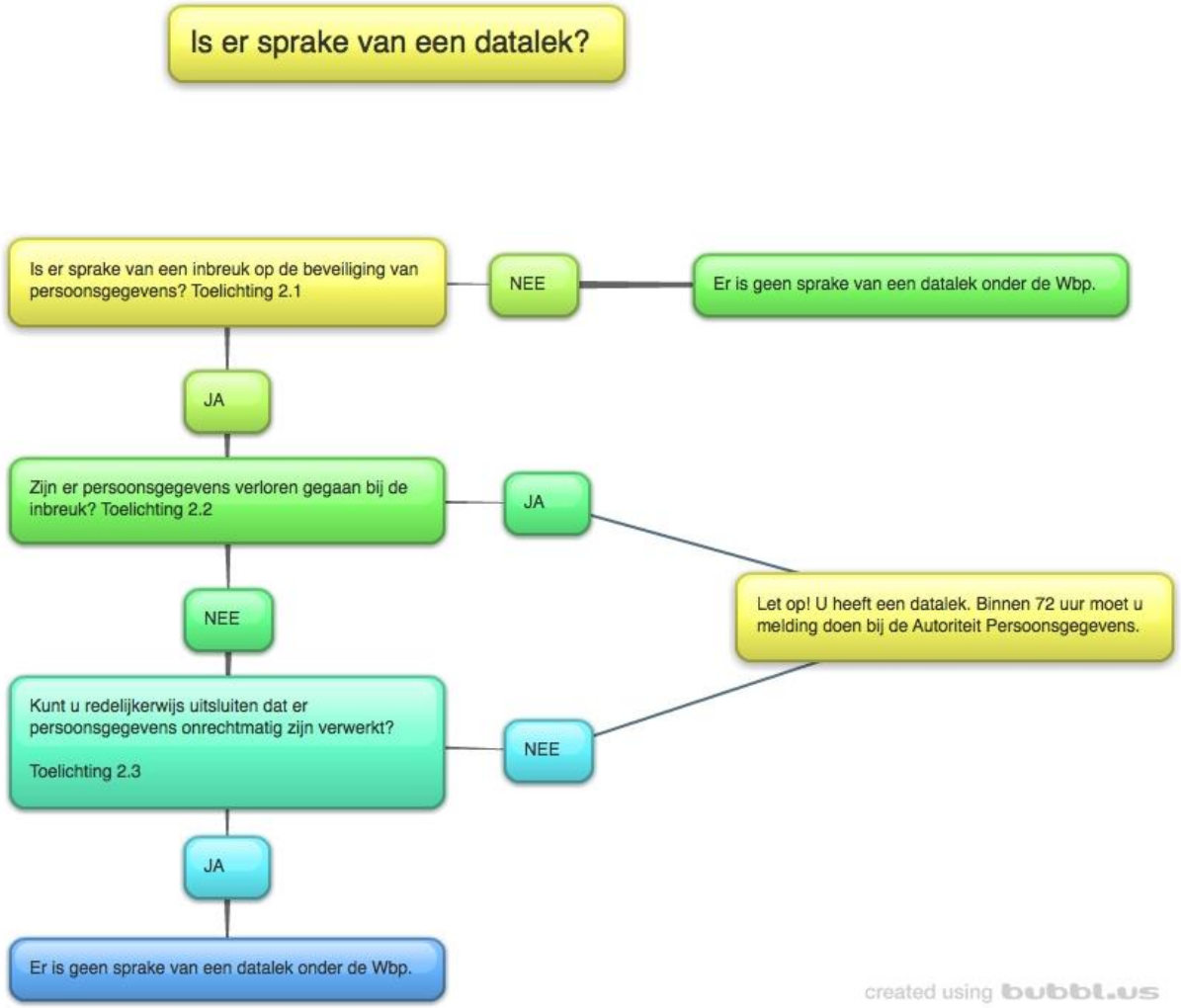
6. Verslaglegging van beveiligingsincidenten (protocolplicht)

De protocolplicht houdt in dat AINL een overzicht moet bijhouden van alle datalekken die zijn ontdekt, met daarbij de overweging waarom deze wel of niet gemeld zijn bij de AP en/of bij betrokkenen (de mensen die in het betreffende bestand staan).

In praktijk wil AINL van alle beveiligingsincidenten (ook degene die niet als datalek kwalificeren) een overzicht bijhouden. Amnesty International moet immers ook kunnen aantonen dat een bepaald beveiligingsincident geen datalek was.

BIJLAGEN

Datalek check: Is er sprake van een datalek?



Toelichting 2.1

De meldplicht datalekken is alleen van toepassing op een beveiligingslek waarbij persoonsgegevens gecompromitteerd zijn. Dit zijn gegevens die betrekking hebben op of herleid kunnen worden naar een persoon in uw database. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. De toezichthouder hanteert een breed begrip van persoonsgegevens. Beschouw daarom in het kader van deze check ook gegevens die herleidbaar zijn tot een huishouden of randapparatuur van een webbezoeker (IP-adres, cookiedata, unieke identifier) als persoonsgegeven. Een inbreuk op de beveiliging kan zijn dat er een USB-stick of andere digitale drager met informatie is gestolen of verloren, er op systemen is ingebroken, er een laptop is gestolen, maar ook dat er bijvoorbeeld door brand informatie is vernietigd.

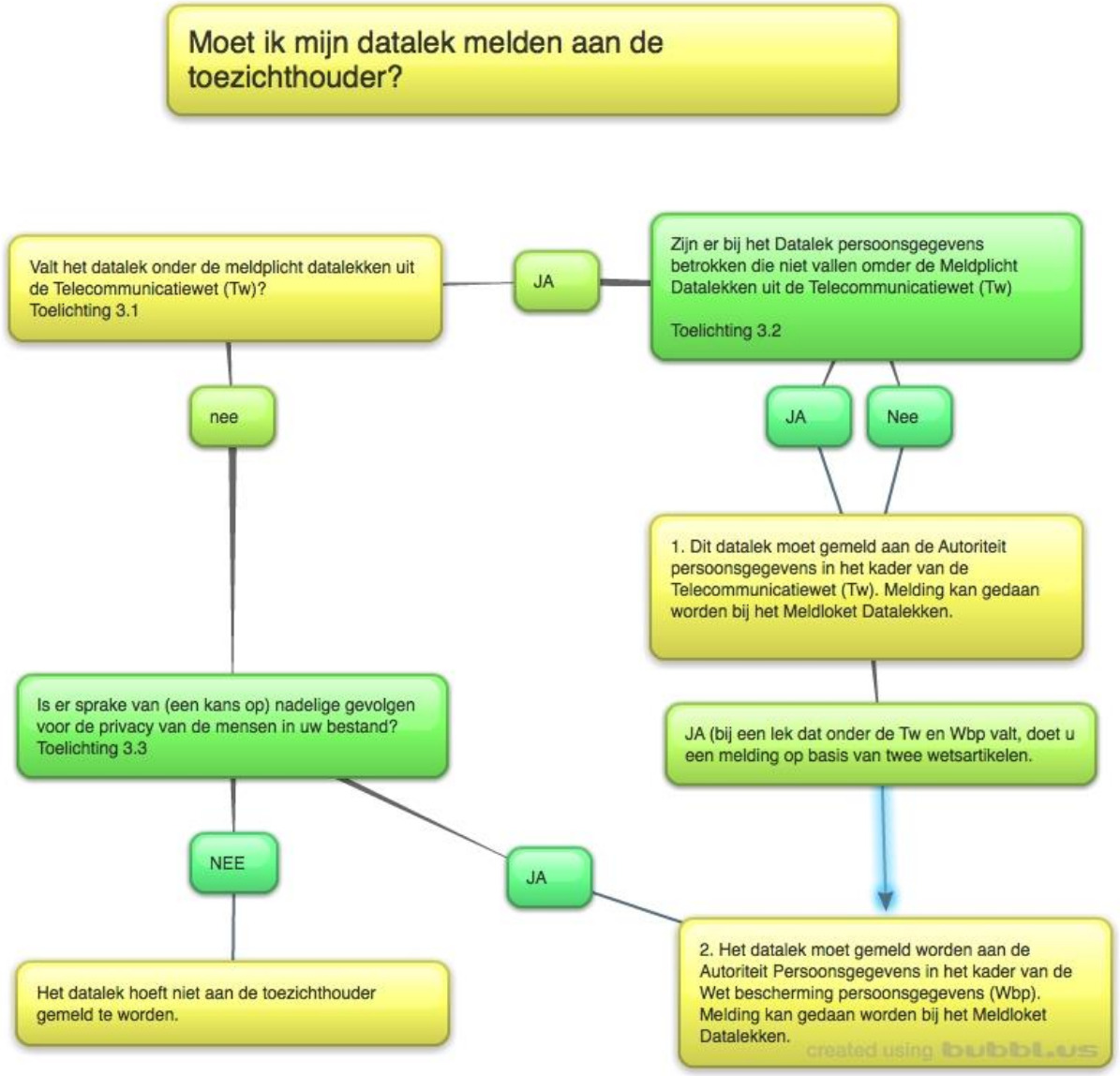
Toelichting 2.2

Als persoonsgegevens door een beveiligingsincident in handen (kunnen) komen van een onbevoegde is er sprake van een inbreuk op de beveiliging van persoonsgegevens. Dat kan zijn door het verlies van een USB-stick, laptop of andere digitale drager, maar bijvoorbeeld ook als op een systeem of database wordt ingebroken. Ook als er persoonsgegevens zijn gewist of op een andere manier zijn vernietigd bijvoorbeeld door brand en er is van deze persoonsgegevens geen actuele back-up gemaakt, is er sprake van een inbreuk op de beveiliging van persoonsgegevens.

Toelichting 2.3

Het is lastig om uit te sluiten dat persoonsgegevens onrechtmatig zijn verwerkt na een beveiligingsincident. Hiervan is namelijk al sprake als iemand een blik heeft geworpen op de gegevens die dit normaliter niet zou kunnen of mogen. Bij verlies, diefstal of een hack kan je dit eigenlijk alleen uitsluiten als de gegevens goed zijn versleuteld. De veilige keuze is hier dus 'nee'.

Datalek check: Moet ik het lek melden aan de toezichthouder?



Toelichting 3.1 toepasselijkheid

De Telecommunicatiewet (Tw) kent al een Meldplicht Datalekken die geldt voor aanbieders van openbare elektronische communicatiediensten. Als er sprake is van een datalek bij internetproviders en telefoonaanbieders waarbij persoonsgegevens door onbevoegden zijn ingezien, moet dit lek gemeld worden bij de AP.

Toelichting 3.1.1 toepasselijkheid

Het kan voorkomen dat een datalek deels betrekking heeft op persoonsgegevens die onder de meldplicht in de Tw vallen, maar deels ook op persoonsgegevens die daarbuiten vallen. Denk aan diefstal van een laptop van een medewerker van een Telco waarop zowel klantgegevens als personeelsgegevens staan. De klantgegevens vallen onder de meldplicht uit de Tw en de personeelsgegevens vallen onder de meldplicht datalekken uit de Wet Bescherming Persoonsgegevens (Wbp). In dit geval moet er één melding worden gedaan, waarbij wordt aangegeven in het formulier aan dat het een datalek is op basis van zowel de Tw als de Wbp.

Toelichting 3.2 nadelige gevolgen

Er is sprake van kans op nadelige gevolgen voor de privacy van mensen wanneer er risico is op misbruik en fraude. Dit risico is groter naarmate de gegevens gevoeliger van aard zijn. Gevoelig van aard zijn in ieder geval financiële data, inloggegevens en BSN-achtige gegevens. Gevoelig zijn ook gegevens die kunnen leiden tot discriminatie of uitsluiting, zoals informatie over verslavingen, levensovertuiging, seksuele voorkeur, ras, of gezondheid. De kans op misbruik is ook groter als het om een grote dataset gaat, dus indien Amnesty International veel gegevens per persoon verzamelt, of gegevens van veel personen. Bij grote datasets of datasets met gegevens van gevoelige aard moet een lek gemeld worden aan de AP. De definitie van groot is niet gegeven. Dit wordt aan de beoordeling van Amnesty International overgelaten.

Datalek check: Moet ik het lek melden aan de betrokkenen?


Moet ik mijn datalek melden aan de betrokkene/ degene in het gelekte bestand?
Moet u uw datalek melden aan de Autoriteit Persoonsgegevens? U kunt dit vaststellen op basis van de CheckDatalek melden aan de AP. (Toelichting 4.1)
NEE
U hoeft uw datalek op basis van de Meldplicht Datalekken niet te melden aan de betrokkene omdat deze niet leidt tot (een kans op) nadelige gevolgen voor de mensen in uw bestand.
JA
Bent u een financiële onderneming zoals bescherven in de Wet op het financieel toezicht (Wft)? Toelichting 4.2
JA
Het datalek hoeft niet aan de betrokkenen gemeld te worden op basis van de Meldplicht Datalekken uit de Wet bescherming persoonsgegevens (Wbp).
Let op: controleer of de betrokkenen alsnog geinformeerd moeten worden op basis van uw zorgplicht als financiële onderneming.
NEE
Is er sprake van vernietiging of aantasting van persoonsgegevens? Toelichting 4.3
JA
NEE
Is cryptografie toegepast op alle gelekte gegevens waardoor deze ontoegankelijk of onbegrijpelijk zijn voor onbevoegden? Toelichting 4.4.
JA
Het Datalek hoeft niet aan de betrokkenen gemeld te worden.
Let op: Indien de Autoriteit Persoonsgegevens (AP) van oordeel is dat het datalek waarschijnlijk toch ongunstige gevolgen zal hebben voor de betrokkenen, kan de AP verlangen dat het lek alsnog gemeld wordt.
NEE
Zijn er andere beveiligingsmaatregelen getroffen die een dusdanige bescherming bieden dat melding aan de betrokkenen achterwege gelaten kan worden? Toelichting 4.5.
JA
NEE
Zijn er zwaarwegende redenen om melding aan de betrokkene achterwege te laten? Toelichting 4.6.
JA
Het Datalek hoeft niet aan de betrokkenen gemeld te worden.
Let op: De Autoriteit Persoonsgegevens beoordeelt uiteindelijk of de redenen die zijn opgegeven om melding aan de betrokkenen achterwege te laten steekhoudend zijn. In bepaalde gevallen kan de AP toch verlangen dat het datalek gemeld wordt aan de betrokkenen.
NEE
Let op! U moet dit datalek melden aan de betrokkenen.

Toelichting 4.1 melden aan betrokkene of niet

Alleen een datalek dat aan de AP gemeld moet worden, moet potentieel ook gemeld worden aan de betrokkenen: de gedupeerde personen.

Toelichting 4.2 financiële onderneming

Voor financiële ondernemingen geldt een uitzondering: Zij hoeven een datalek niet aan de betrokkenen te melden op basis van de Meldlicht Datalekken uit de Wbp. Zij moeten een eventueel datalek wel melden bij de Autoriteit Persoonsgegevens. In artikel 1:1 van de Wet op het financieel toezicht (Wft) is beschreven wat de definitie van een financiële onderneming is en welke ondernemingen onder dit begrip vallen.

- een afwikkelonderneming;
- een bank;
- een beheerder van een beleggingsinstelling;
- een beheerder van een icbe;
- een beleggingsinstelling;
- een beleggingsonderneming;
- een betaaldienstverlener;
- een bewaarder;
- een clearingsinstelling;
- een entiteit voor risico-acceptatie;
- een financiële dienstverlener;
- een icbe;
- een kredietunie;
- een pensioenbewaarder;
- een premiepensioeninstelling;
- een verzekeraar; of
- een wisselinstelling.

Toelichting 4.3 aantasting, vernietiging en encryptie

Er is vaak sprake van vernietiging of aantasting van gegevens wanneer er malware, ransomware of virussen zijn gebruikt. Dit is software met 'kwade opzet' die de controle over gegevens uit handen kan nemen van de bestandseigenaar door computersystemen te verstoren of te gijzelen, en/of gegevens te wijzigen of te vernietigen. Wanneer er als gevolg van een datalek persoonsgegevens zijn vernietigd of aangetast moet dit in principe gemeld worden aan de betrokkenen.

Melding van een datalek aan de betrokkenen kan achterwege blijven als er afdoende technische beveiligingsmaatregelen zijn getroffen waardoor de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden. Dit is bijvoorbeeld het geval wanneer u gebruik maakt van cryptografie in de vorm van gegevensencryptie (versleuteling) of hashing (het omzetten van gegevens in een unieke code). Wanneer niet alle gegevens geencrypt of gehasht zijn moet het datalek mogelijk gemeld worden aan de betrokkenen.

Toelichting 4.4 andere beveiligingsmaatregelen

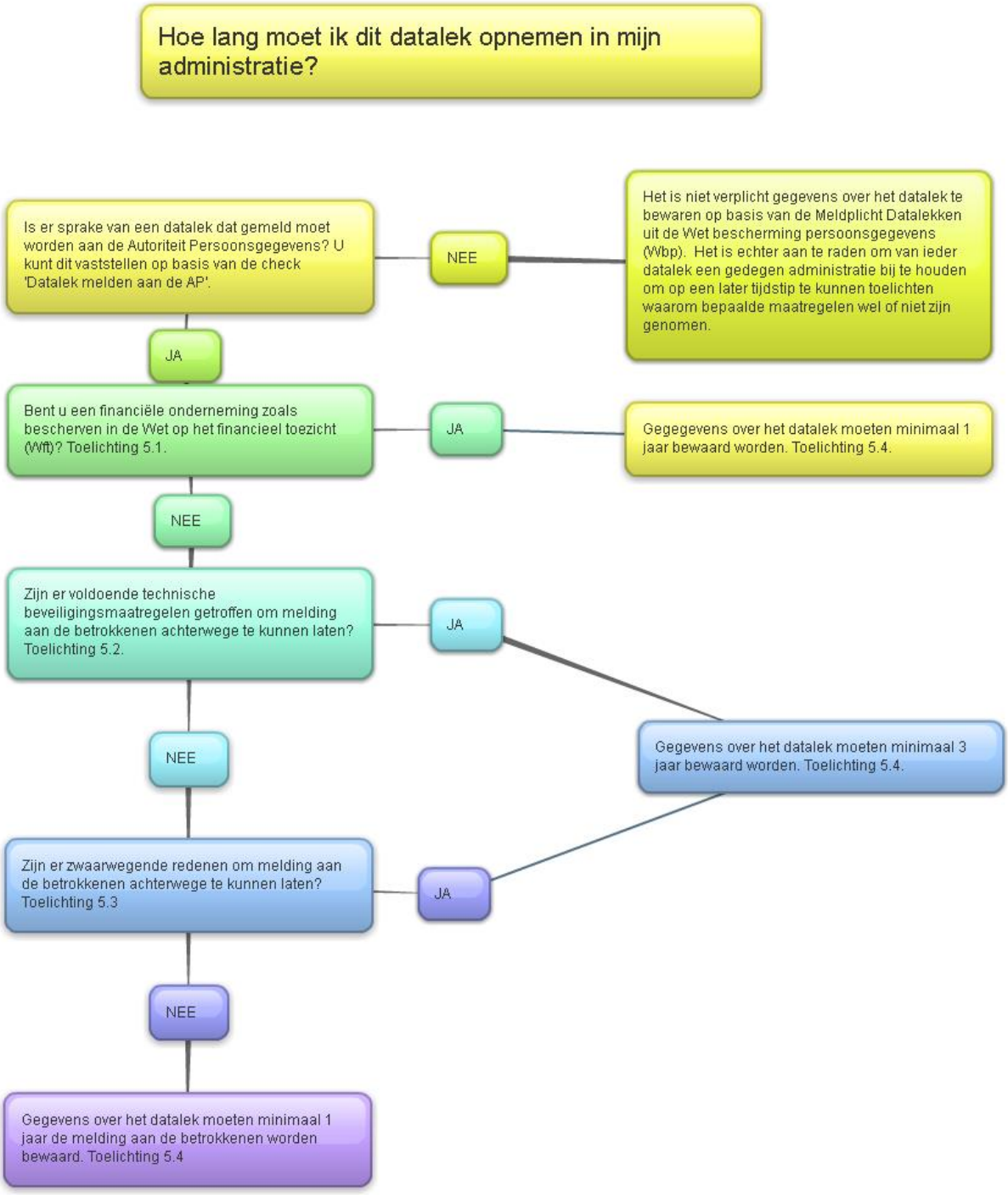
Een andere doeltreffende manier om persoonsgegevens te beveiligen tegen toegang of gebruik door onbevoegden is een zgn. remote wipe. Hierbij wordt data op afstand van een mobiel apparaat zoals een laptop, tablet of telefoon device gewist. Gegevens kunnen ook onbegrijpelijk gemaakt zijn voor onbevoegden door pseudonimisering. Hierbij kunnen persoonsgegevens niet meer aan een betrokkene worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt. Deze aanvullende gegevens dienen dan wel apart bewaard te worden. U moet een inschatting maken of u tijdig de remote whipe heeft uitgevoerd en/of u gegevens adequaat hebt gepseudonimiseerd.

Toelichting 4.5 zwaarwegende redenen

Melding van een datalek aan een betrokkene kan achterwege blijven als dit noodzakelijk is voor de bescherming van de betrokkene. Er mag van melding worden afgezien als daarvoor zwaarwegende redenen aanwezig zijn. Bijvoorbeeld als er gegevens zijn gelekt over medische en psychosociale hulpvragen die kinderen buiten medeweten van hun ouders hebben gedaan.

In dit geval meldt u het datalek aan de Autoriteit Persoonsgegevens en geeft u aan wat de reden is om melding aan de betrokkenen achterwege te laten. In het bovenstaande voorbeeld is de reden dat de ouders door de melding op de hoogte zouden kunnen komen van de hulpvraag van hun kind.

Datalek check: Hoe lang moet ik het datalek opnemen in mijn administratie?



<u>Toelichting algemeen</u>

Naast een de meldplicht hebben organisaties op grond van de wetgeving omtrent datalekken ook een protocolplicht. De protocolplicht houdt in dat organisaties een overzicht moeten bijhouden "van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens". Amnesty International moet een overzicht

bijhouden van alle lekken. De lekken waarvan zij heeft geconcludeerd dat deze gemeld moeten worden aan de toezichthouder, maar ook de datalekken die niet gemeld zijn en welke overwegingen daarbij genomen.

De toelichtingen bij 5.1 tot en met 5.4 zijn gelijk aan de toelichtingen bij datalek check nummer 4.1 tot 4.4.

Voorbeeld notificatie naar betrokkenen

Belangrijke mededeling over databeveiliging. Leest u alstublieft het volledige bericht.

Geachte **[NAAM]**,

Onze organisatie heeft ontdekt dat een ongeautoriseerde partij zich toegang heeft verschaft tot **onze systemen / persoonsgegevens van donateurs van relaties / etc**. Hierbij is mogelijk persoonlijke informatie van u gecompromitteerd. Het gaat hierbij om de volgende gegevens **[OPSOMMING DATASOORTEN]**.

In reactie op deze inbreuk hebben wij de volgende stappen ondernomen:

1. Een extern erkende beveiligingsspecialist is ingeschakeld om het lek grondig te onderzoeken en aanbevelingen te doen voor verbeteringen in de databeveiliging.
2. **De betreffende dienst is tijdelijk offline gehaald/ accounts zijn op non actief gesteld/ gecompromitteerde bestanden zijn geïsoleerd.**
3. Er is melding gemaakt van het lek bij de wettelijke toezichthouder: de Autoriteit persoonsgegevens.

Op dit moment onderzoeken wij exact welke gegevens uit de systemen zijn ingezien of gedownload. Wij zullen u hierover zo snel mogelijk uitsluitsel geven. **Wij geven u later vandaag of uiterlijk morgenochtend een nieuwe update over de stand van zaken.** Wij adviseren u in de tussentijd preventief de volgende stappen te ondernemen:

- Wijzig uw wachtwoord. U kunt dit eenvoudig doen via **deze link**.
- Indien u voor andere diensten gebruik maakt van hetzelfde wachtwoord, adviseren wij u ook deze wachtwoorden opnieuw in te stellen.

Wij betreuren deze inbreuk zeer en bieden onze excuses aan voor het ongemak dat dit voor u met zich meebrengt. Mocht u vragen hebben naar aanleiding van deze mededeling, neemt u dan contact op met onze servicedesk via **[e-mailadres en telefoonnummer invoegen]**.

Groet,

[Naam en functietitel]

Toelichting bij notificatie
De notificatie dient altijd aangepast te worden aan de specifieke situatie en kan niet standaard zoals bovenstaand verzonden worden. De **vetgedrukte** woorden dienen in elk geval op maat gemaakt te worden.

Richtlijnen voor communicatie

WE REAGEREN ACCURAAT EN SNEL

1. Amnesty International meldt indien mogelijk een datalek zo snel mogelijk aan de betrokkenen, ook al zijn nog niet alle details bekend. We vertellen wat we weten en wat we gaan doen.
2. We geven een tijdsindicatie indien nog niet alle details bekend zijn.
3. We vertellen de details die wel bekend of waarschijnlijk zijn, wat Amnesty International doet om de ontbrekende informatie te achterhalen en wanneer we met een update komen.
4. We benadrukken dat de situatie kan veranderen. Omdat datalekken complex van aard kunnen zijn, is het van belang aan te geven dat de situatie kan veranderen met kwalificaties als 'op dit moment' en 'zoals de situatie er nu voor staat'.
5. We richten de servicedesk in.

WE ZIJN OPEN EN EERLIJK

1. We brengen het nieuws feitelijk en simpel en geven aan hoe Amnesty International de betrokkenen op de hoogte brengt en houdt.
2. Informatie over de omvang van een datalek is veelal niet meteen voor handen. We vermijden daarom onvoorwaardelijke en absolute uitspraken.
3. Betrokkenen willen de ernst van een incident kunnen inschatten. Amnesty International wil daarom zo goed en compleet mogelijk een indicatie te geven van de omvang van een lek.

WE NEMEN VERANTWOORDING

1. Amnesty International accepteert alle verantwoordelijkheid.
2. We vermijden voorwaardelijke excuses. Excuses aanbieden is cruciaal in het nemen van verantwoordelijkheid. Vermijd voorwaardelijke excuses als 'Wij geloven dat deze inbreuk geen negatieve gevolgen heeft gehad voor onze gebruikers, maar willen ons toch verontschuldigen voor eventuele ongemakken'.
3. We benadrukken dat consumenten niet aansprakelijk zijn voor eventuele schade die voortvloeit uit het lek. We nemen ongerustheid weg door aan te geven dat consumenten niet verantwoordelijk zijn voor eventuele frauduleuze praktijken die voortvloeien uit het lek.

Mediawoordvoering en - monitoring

Tips ten behoeve van mediawoordvoering:

1. Het is belangrijk dat afhankelijk van de aard van het incident een expert van de werkvloer en een lid van de directie betrokken is bij de mediawoordvoering.
2. Intern is extern. We houden er rekening mee dat alle informatie over het datalek, die aan medewerkers van Amnesty International, bewerkers en betrokkenen wordt verstrekt, ook bij externen terecht komt.
3. We publiceren een FAQ over de feiten voor de medewerkers en geven de contactgegevens van de klantenservice, waar zij naar kunnen doorverwijzen.
4. We blijven actueel en tijdig communiceren. We blijven tijdig en eventueel op afgesproken tijdstippen met updates te komen.
5. We monitoren social media. Eventueel introduceren we zelf een hashtag op Twitter, we vermijden discussie, benoemen en ontkrachten onjuistheden, verwijzen naar relevante online bronnen, bijvoorbeeld de website van Amnesty International.