Protocol beveiligingsincidenten en datalekken

NLNet
Nederlands netwerk voor lymfoedeem & lipoedeem

Inleiding

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken. Stichting NLNet is zich ervan bewust dat incidenten nooit zijn uit te sluiten. Daarom worden ook afspraken vastgelegd voor gevallen waarin een data- lek is opgetreden en voor de evaluatie van een dergelijk incident.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek**; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken. NLNet is op grond van de AVG verplicht om datalekken te melden bij de Autoriteit Persoonsgegevens (AP) en de betrokkenen.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.
- **Privacy officer;** de secretaris die toeziet op de omgang met persoonsgegevens binnen de organisatie en controleert of de organisatie voldoet aan de wet en eventuele andere toepasselijke regelgeving.

1. Wet- en regelgeving datalekken

Op 1 januari 2016 is de wet op de meldplicht datalekken & privacy in werking getreden. Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf die datum geldt dezelfde privacywetgeving in de hele EU. Iedere organisatie die persoonsgegevens verwerkt, is verplicht om een datalek te melden bij de Autoriteit Persoonsgegevens (AP).

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. De AVG geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.

Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers en mailadressen zijn persoonsgegevens.

Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten dat persoonsgegevens verloren zijn gegaan. Als een data-lek het gevolg blijkt te zijn van nalatigheid of opzet, kan de Autoriteit Persoonsgegevens een boete opleggen. De boete valt hoger uit als er sprake is van nalatigheid en slecht geregelde ICT-beveiliging. Het is daarom belangrijk dat onze organisatie klaar is om dergelijke sancties te voorkomen.

Als er gebruik wordt gemaakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen, dan moet er met deze verwerkers aanvullende afspraken gemaakt worden over het melden van datalekken.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het bestuur. Een leverancier is een verwerker voor de stichting. Er kan worden afgesproken dat een verwerker **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het bestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Als er een datalek is, moet daarvan binnen 72 uur na ontdekking melding worden gedaan bij de Autoriteit Persoonsgegevens.

2. Afspraken met leveranciers

Het bestuur maakt als verantwoordelijke voor de persoonsgegevens afspraken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Afgesproken wordt:

- Hoe verwerkingsverantwoordelijke en verwerker elkaar informeren over datalekken.
- Hoe de bereikbaarheid is geregeld. (bijvoorbeeld tijdens het weekend en vakanties)
- Wie melding doet bij de Autoriteit Persoonsgegevens.
- Welke informatie de verwerker aan de verwerkingsverantwoordelijke moet geven bij een data-lek.
- Welke informatie nodig is voor het doen van een melding en hoe de andere partij wordt geïnformeerd over die melding (bijvoorbeeld door het maken van een kopie of het doorsturen van de melding).
- Binnen welk tijdsbestek de verwerker de gegevens moet aanleveren.
- Wie de communicatie met de betrokkenen voor haar rekening neemt als dat nodig is.

De schriftelijke afspraken die Stichting NLNet maakt met haar verwerker(s) over datalekken worden vastgelegd in een (verwerkers)overeenkomst.

3. WERKWIJZE

De vier rollen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of data-lek succesvol af te handelen:

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of data-lek op het spoor komt en het proces in werking stelt.
2. **Meldpunt (beleidsmedewerker ICT)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. Bij Stichting NLNet worden alle beveiligingsincidenten gemeld bij de secretaris van het bestuur via secretaris@lymfoedeem.nl
3. **Melder (privacy officer)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens. Binnen Stichting NLNet is dit de secretaris van het bestuur.
4. **Technicus (netwerkbeheerder/ ICT-coördinator)**; degene die de oorzaak van het data-lek kan vinden en kan (laten) repareren.

De acht stappen

1. **Ontdekken**
   De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. Dit kan een ICT-gerelateerd beveiligingsincident zijn, of een beveiligingsincident dat betrekking heeft op papieren documenten. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt via secretaris@lymfoedeem.nl

2. **Inventariseren**
   Het Meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd in het document *Register beveiligingsincidenten*:
   - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een data-lek):
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen
     - Type persoonsgegevens in kwestie
     - Worden de gegevens binnen een keten gedeeld

3. Beoordelen

Wanneer het Meldpunt voldoende informatie heeft verzameld, en een data-lek vermoedt, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkenen vereist is.

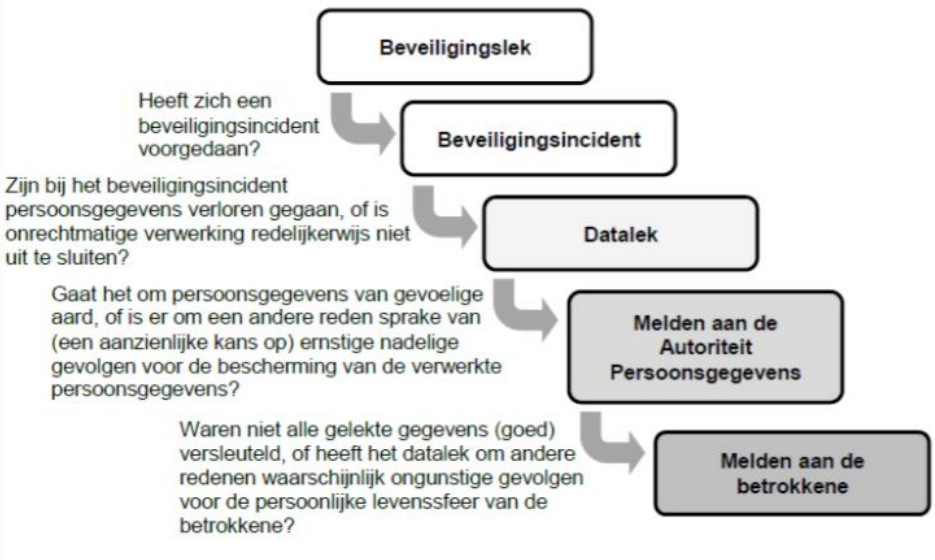
De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het data-lek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het data-lek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Melder beoordeelt in samenspraak met de secretaris van NLNet of er sprake is van een ‘meldingsplicht data-lek’. Bij de beoordeling of er sprake is van een ‘melding plichtig data-lek’, wordt rekening gehouden met het type gegevens, en met de hoeveelheid gegevens. Indien het data-lek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, móet er gemeld worden.

Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens “gevoelig” zijn, zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene.

De onderstaande beslisboom kan gebruikt worden



4. **Repareren**
   De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van Stichting NLNet legt onderstaande vast:

   - Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
   - Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

5. **Melden**
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit in samenspraak met de secretaris van NLNet binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de secretaris van het bestuur waarmee het incident is afgesloten. Het Meldpunt geeft terugkoppeling van de genomen maatregelen aan de Ontdekker.

7. **Informeren betrokkene:**
   Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het data- lek ook aan de betrokkenen zelf worden gemeld. In principe kan ervan uit worden gegaan dat het lekken van gevoelige aard gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat níet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

   8. Evaluatie

   Binnen twee weken na een datalek vindt, op initiatief van de secretaris van NLNet, een evaluatie van het dossier met de betrokkenen plaats, met als doel beveiliging, melding en nazorg te verbeteren. De resultaten van de evaluatie worden door de secretaris schriftelijk vastgelegd en aan het bestuur gemeld.

4. Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van Stichting NLNet maakt twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de functionaris gegevensbescherming.

In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Het bestuur wordt geïnformeerd over de uitkomsten van de analyse.

De rapportage wordt opgenomen in de jaarplanning.

5. Communicatie

Melding beveiligingsincidenten door derden

Via de mail is het mogelijk om een melding beveiligingsincidenten door te geven. Op deze wijze kunnen ook personen van buiten de organisatie een vermoeden van een beveiligingsincident melden.

Interne en externe communicatie bij datalek

De beleidsmedewerker ICT is verantwoordelijk voor de juiste interne en externe communicatie bij een data-lek. Uiteraard wordt binnen de organisatie overleg gevoerd met de dagelijks bestuur van NLNet voordat berichten ‘naar buiten’ gaan.

Informeren van medewerkers

Al onze medewerkers en relaties worden door de secretaris geïnformeerd over de meldplicht bij datalekken & privacy.

Hierbij dient voor medewerkers helder gemaakt te worden welke vormen van datalekken kunnen voorkomen.

Hierbij worden de volgende facetten benadrukt:

1. *Vermoeden van onterecht uitwisselen van gegevens*

2. *Data-lek door verlies/diefstal van apparatuur en/of inloggegevens*. Al onze apparatuur kan gegevens bevatten, die niet toegankelijk mogen zijn voor anderen. Denk hierbij bijvoorbeeld aan het gebruik van apps op een tablet of smartphone. Diefstal of verlies van deze apparatuur kan leiden tot een data-lek, als de apparatuur of de apps niet goed beveiligd zijn.

3. *Clean desk en screen policy (inclusief wachtwoordbeleid)*. Wachtwoorden die toegang verschaffen tot applicaties waarin persoonsgegevens zijn opgeslagen mogen niet opgeschreven worden. Medewerkers van derden en leden van NLNet zorgen ervoor dat ze geen privacygevoelige informatie open laten staan op onbeheerde apparatuur. Digitale bestanden met persoonsgegevens worden opgeslagen op daarvoor bestemde locaties, rekening houdend met beveiliging en autorisatie. Papieren documenten met persoonsgegevens worden op verantwoorde wijze opgeborgen.

4. *Toestemming voor gebruik applicaties aanvragen*. Om te voorkomen dat er applicaties gebruikt worden waarbij persoonsgegevens worden verstrekt aan leveranciers waar geen verwerkersovereenkomst mee is afgesloten, mogen alleen applicaties in gebruik worden genomen die door de secretaris zijn goedgekeurd.

5. *Veilig mailverkeer*. Het versturen van documenten met persoonsgegevens via e-mail is uitsluitend toegestaan als de data voldoende beveiligd is én als er wordt voldaan aan de vijf vuistregels uit de AVG: doelbinding, grondslag, dataminimalisatie, transparantie en data-integriteit.

Alle medewerkers van Stichting NLNet zijn verplicht om kennis te nemen van het *Protocol beveiligingsincidenten en datalekken* en dit protocol te lezen en onderschrijven.

Dit protocol treedt per 6.11.2024 in werking.