



Protocol datalekken

25-4-2024
Handboek IBP
Leon van Lare RI

Inhoud

Inleiding	3
Wet- en regelgeving datalekken	3
Afspraken met leveranciers	3
Werkwijze.....	4
Uitgangssituatie.....	4
De vier rollen	4
De zeven stappen	4
Monitoring beveiligingsincidenten en datalekken.....	6
Extra informatie.....	6

Inleiding

Het Protocol datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van SOML. 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. Dit protocol is van toepassing op de gehele organisatie van SOML.

Gebruikte termen:

- **Beveiligingsincident;** een beveiligingsincident is een gebeurtenis die er voor 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.
- **Betrokkene;** de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd (op 25 mei 2018 is de AVG ingevoerd). Door deze meldplicht is SOML verplichting melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in je leerling-administratie of digitale leermiddelen. Als een school gebruik maakt van leveranciers die persoonsgegevens ontvangen van de school, dan moet SOML met deze bewerkers aanvullende afspraken maken over het melden van datalekken.

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. Er is persoonlijke informatie 'gelekt'. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen. De Privacy Officer van SOML heeft het mandaat melding te maken van een datalek.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens. Die 72 uur gaat in als het formulier '[Melden datalek of incident bij SOML](#)' correct ingevuld is en ontvangen en beoordeeld is door de Privacy Officer van SOML.

Afspraken met leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. De Privacy Officer maakt schriftelijke afspraken met bewerkers over datalekken. Hiervoor wordt zoveel mogelijk gebruik gemaakt van de model bewerkersovereenkomst die hoort bij het convenant "Digitale onderwijsmiddelen en privacy" (www.privacyconvenant.nl).

Werkwijze

Uitgangssituatie

- Er is een actueel Informatiebeveiligings- en privacy beleid (bij 'Documenten' in Afas)
- Er is een actueel Gebruikersreglement ICT (op de SOML-website)

De vier rollen

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

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. Het meldpunt is de Privacy Officer van SOML.
3. **Melder (privacy officer)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (security- of privacy officer)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De zeven stappen

1. Ontdekken

De Ontdekker merkt al dan niet in overleg met een privacy functionaris (op school of van de stafdienst) een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het Meldpunt via het [Meldformulier datalekken](#)

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:

- 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 datalek):
 - 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 datalek wordt vermoed, 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:

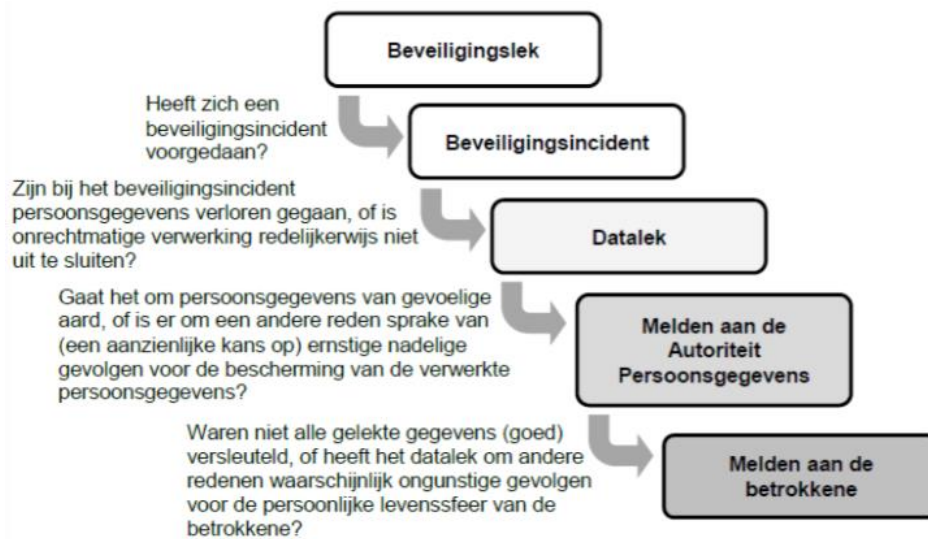
- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek' wordt er rekening gehouden met het type gegevens en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens moet 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 (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom zal 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 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 binnen 72 werkuren doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt door de Privacy Officer van SOML gemeld bij het meldloket datalekken. Een link naar het meldloket van de AP vindt u op [deze pagina](#).

6. Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten. Er zal informatie worden opgeslagen in een archiefmap en in het datalekregister. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker. Ook wordt er een rapportage opgesteld voor het bestuur en voor de Directie en de Privacy Coördinator van de betreffende school.

7. Informeren betrokkene: leerling en/of zijn ouders

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan er van worden uitgaan dat het lekken van gevoelige aard gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkenen te worden gemeld.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van SOML maakt drie keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken. Dit gebeurt via de MaRap-cyclus van SOML. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Extra informatie

Meer informatie is te vinden via de volgende links:

- [Het privacy reglement van SOML](#)
- [Meldformulier datalekken](#)
- [Gebruikersreglement ICT](#)