PROTOCOL

BEVEILIGINGSINCIDENTEN EN DATALEKKEN

28-05-2018

Inhoud

Bij dit protocol hoort ook een stappenplan (1 A4) voor medewerkers.
Dit volgt later.

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het privacy beleid van SKIPOS.

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 SKIPOS en al haar medewerkers.

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. Door deze meldplicht zijn ook scholen verplicht 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. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze verwerkers 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 is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie ‘gelekt’. Dit kan zijn een hack, het verliezen van een usb-stick of de diefstal van een laptop. Maar ook een verkeerd verzonden email of een verkeerd ingestelde autorisatie.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur.
Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

Afspraken met scholen en leveranciers

Het schoolbestuur maakt als verantwoordelijke voor de persoonsgegevens de onderstaande datalek-afspraken met de scholen en de leveranciers die persoonsgegevens ontvangen en verwerken:

- De ontdekker van een datalek meldt dit binnen 24 uur bij de directeur van de school of de zaakgelastigde of contactpersoon van een leverancier.
- De directeur of de zaakgelastigde of contactpersoon meldt binnen 24 uur het datalek bij de Functionaris Gegevensbescherming; bij voorkeur: fg@dommelgroep.nl

- De FG neemt de melding op in het Register Datalekken en doet, na een positieve weging, de melding bij de Autoriteit Persoonsgegevens. Ook informeert hij de bestuurder bij een ernstige datalek.

SKIPOS heeft schriftelijke afspraken met onze verwerker(s) over datalekken gemaakt d.m.v. de model bewerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

Werkwijze

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 of leerling)**; degene die het beveiligingsincident of datalek op het spoor komt.

2. **Meldpunt (directeur)**; een aanspreekpunt per school waar alle beveiligingsincidenten worden gemeld.

3. **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens en een incidentenregister bijhoudt.

4. **Technicus**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

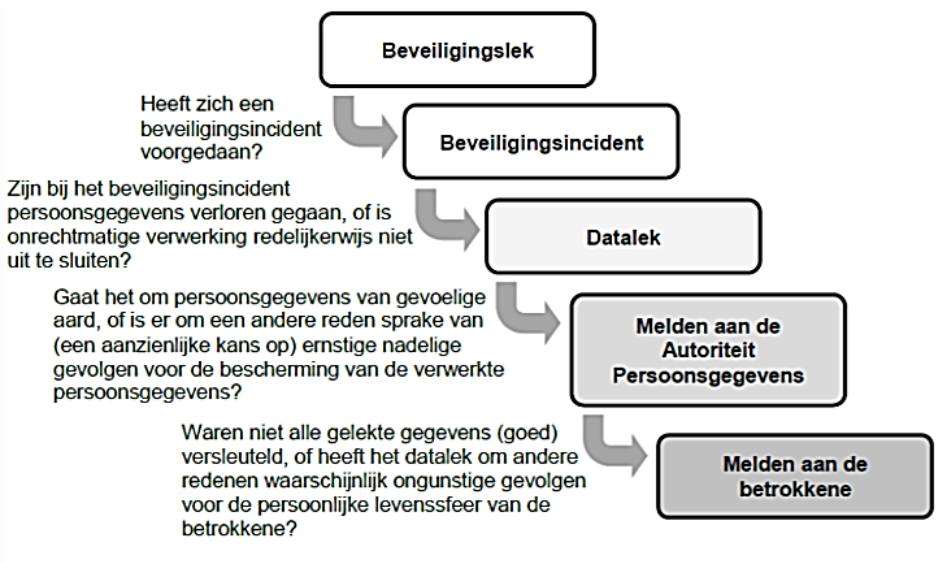
De 7 stappen

1. **Ontdekken**
   De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt dit bij de eigen directeur van de school of de zaakgelastigde of contactpersoon van een leverancier van de school.

2. **Inventariseren**
   De directeur zal samen met de melder de vragenlijst in de bijlage zo compleet mogelijk.

3. **Beoordelen**
   Wanneer de vragenlijst is ingevuld, stuurt de directeur deze binnen 24 uur naar de FG fg@dommelgroep.nl met het verzoek het datalek te beoordelen. De FG beoordeelt de informatie om te bepalen of een melding aan de Autoriteit persoonsgegevens en de bestuurder vereist is.
   De volgende informatie over het datalek wordt vastgelegd door de FG:
   - De feiten rondom het datalek en de mogelijke gevolgen van het datalek (de ingevulde vragenlijst).
   - Is het datalek gemeld aan de bestuurder? Waarom niet?
   - Is het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
   - De inhoud van de melding.
   - Is het datalek gemeld aan de betrokkenen? Waarom niet?

   Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’, houdt de FG rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen wordt er gemeld bij de Autoriteit Persoonsgegevens.
   De onderstaande beslisboom wordt gebruikt:



4. **Beperken gevolgen**
   De gevolgen worden zoveel mogelijk beperkt. Er wordt gekeken wat de oorzaak van het beveiligingsincident is. De nodige acties voor de aanpak en het verhelpen van de oorzaak worden uitgevoerd.

5. **Melden**
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens, dan zal de FG dit binnen een werkdag 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 FG waarmee het incident is afgesloten. De FG informeert de directeur van de school over de genomen (te nemen) maatregelen om herhaling te voorkomen.

7. **Informeren betrokkene: leerling en/of zijn ouders**
   Wanneer het datalekwaarschijnlijk een hoog risico inhoudt voor de betrokkene(n), dan wordt het datalek ook aan de betrokkene(n) zelf gemeld. Dat zijn medewerkers, leerlingen, of hun ouders als zij jonger zijn dan 16 jaar.
   In principe wordt ervan uitgegaan dat het lekken van persoonsgegevens van kinderen altijd van gevoelige aard is en gemeld moet worden bij de betrokkenen.
   Als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn volledig onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkenen te worden gemeld.

Monitoring beveiligingsincidenten en datalekken

De FG maakt twee keer per jaar een analyse van de meldingen van de beveiligingsincidenten en de datalekken.
In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.
De bestuurder wordt door de FG geïnformeerd over de uitkomsten van de analyse.