Protocol informatiebeveiligingsincidenten en datalekken Stichting Saenstroom

Opsteller: Jan Zonneveld
Expertise: Informatiemanagement OVO-zaanstad
Revisiedatum: 1 november 2020

Vastgesteld door het bestuur van de Stichting Saenstroom op 25 juni 2018

Inhoud

Inleiding 3
Wet- en regelgeving datalekken 3
Afspraken met leveranciers 4
Werkwijze 4
Uitgangssituatie 4
De vier rollen 4
De zeven stappen 4

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van Stichting Saenstroom

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 Stichting Saenstroom en al haar medewerkers.

Saenstroom heeft een dienstverleningsovereenkomst met OVO Zaanstad. OVO-service, het stafbureau van OVO Zaanstad, verleent de ondersteuning op het gebied van informatiemanagement, digitale zaken en digitale beveiliging.

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 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 leerlingadministratie of digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze bewerkers aanvullende afspraken 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’. 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.

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 leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Spreek af:

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatie gegevens de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Saenstroom maakt schriftelijke afspraken met bewerker(s) over datalekken. Hiervoor wordt 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;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en/of gedragscode ICT en internetgebruik.

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. **Privacy officer van de school**; Waar alle beveiligingsincidenten worden geregistreerd en volgens protocol verder worden verwerkt.
3. **Privacy officer van OVO service**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Security officer**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De zeven stappen

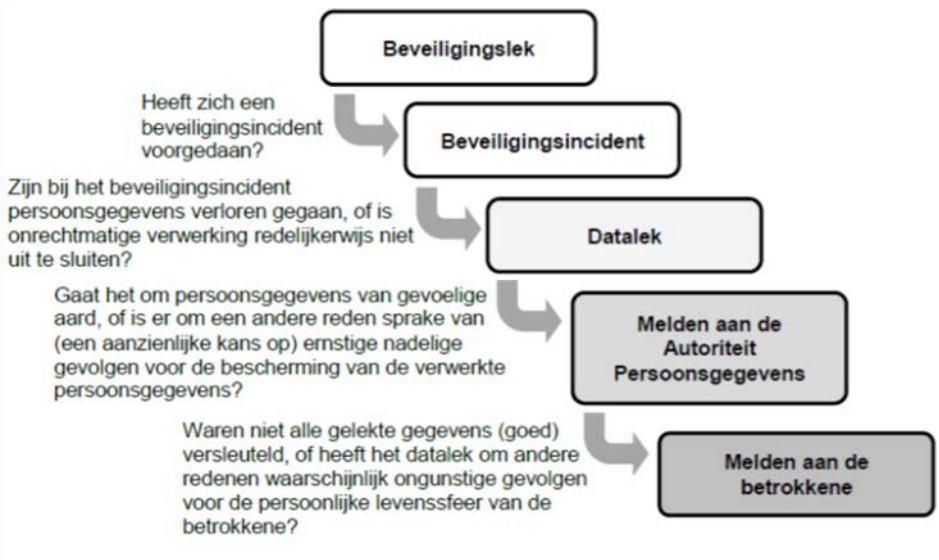
1. **Ontdekken**
   De ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde en meldt het bij de privacy officer van de school of OVO service.
   De privacy officer van de school of OVO service verzamelt zoveel mogelijk informatie over het beveiligingsincident. De privacy officer van de school geeft de melding zo spoedig mogelijk telefonisch door aan de privacy officer van OVO service. Deze heeft vervolgens de regie over de melding.

2. **Inventariseren**
De privacy officer van OVO service bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet deze aanvullende vragen uit bij de ontdekker en/of de security officer. 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 de privacy officer van OVO service voldoende informatie heeft verzameld en een datalek vermoedt, stuurt deze de ontdekker een verzoek om de verzamelde informatie te bekijken. De ontdekker beoordeelt de feiten.
De volgende informatie wordt vastgelegd door de privacy officer van OVO service. Voor vervolgstappen wordt gebruik gemaakt van de beslisboom in combinatie met pas toe en leg uit principe. De privacy officer geeft na het doorlopen van de beslisboom een advies aan het bestuur. Het bestuur beslist over de te ondernemen acties. Bij een lek door het bestuur besluit de functionaris gegevensbescherming.

Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’ wordt 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, of als het ernstige nadelige gevolgen heeft 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 wordt gebruikt:



4. **Repareren**
   De security officer wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van Stichting OVO Zaanstad 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 privacy officer van OVO service dit aan het bestuur adviseren. Wanneer het bestuur het advies overneemt zal de privacy officer de melding 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. Het meldingsformulier toegevoegd als bijlage, hierin staat wat nodig is om een datalek te melden.

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

7. **Informeren betrokkene(n): leerling en/of zijn ouders**
   Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene(n)? Dan moet het datalek ook aan de betrokkene(n) zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16

jaar). In principe kan er van worden uitgegaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkene(n). 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 toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden. Dit dient per geval beoordeeld te worden. Betrokkene(n) kunnen bij de betrokken privacy officer vragen stellen over de voortgang en zullen daarnaast ook proactief geïnformeerd worden.

8. **Monitoring en evalueren van beleid.**
   De informatiemanager van Stichting OVO Zaanstad maakt jaarlijks een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking alle privacy officers.
   In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.
   Het bestuur van Saenstroom wordt geïnformeerd over de uitkomsten van de analyse.