SAMENWERKINGSVERBAND
VO ZAANSTREEK

Protocol datalek voor het Samenwerkingsverband VO Zaanstreek

Vastgesteld door directeur-bestuurder	13 oktober 2023
Besproken in RvT	12 oktober 2023
Instemming MR-p	03 oktober 2023

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van het Samenwerkingsverband Zaanstreek.

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.

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**; Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. Waarbij de oorzaak een inbreuk op de beveiliging van deze gegevens is. Ook het ongewenst vernietigen, verliezen, wijzigen of verstrekken van persoonsgegevens door zo'n inbreuk valt onder een datalek.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving 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 een groep, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, het samenwerkingsverband. 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 samenwerkingsverband moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Spreek af:

- Hoe je elkaar informeert over datalekken, en zorgt voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Welke gegevens de verwerker 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 verwerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Het samenwerkingsverband maakt schriftelijke afspraken met verwerker(s) over datalekken. Hiervoor wordt gebruik gemaakt van de modelbewerkersovereenkomst 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 drie rollen

Er zijn tenminste drie 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. **Functionaris Gegevensbescherming**; Waar alle beveiligingsincidenten worden geregistreerd en volgens protocol verder worden verwerkt en verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
3. **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 het secretariaat op privacy@swvvozaanstreek.nl.
   De privacy-officer meldt het vermoeden bij de functionaris gegevensbescherming en verzamelt zoveel mogelijk informatie over het beveiligingsincident.

2. **Inventariseren**
   De FG 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.

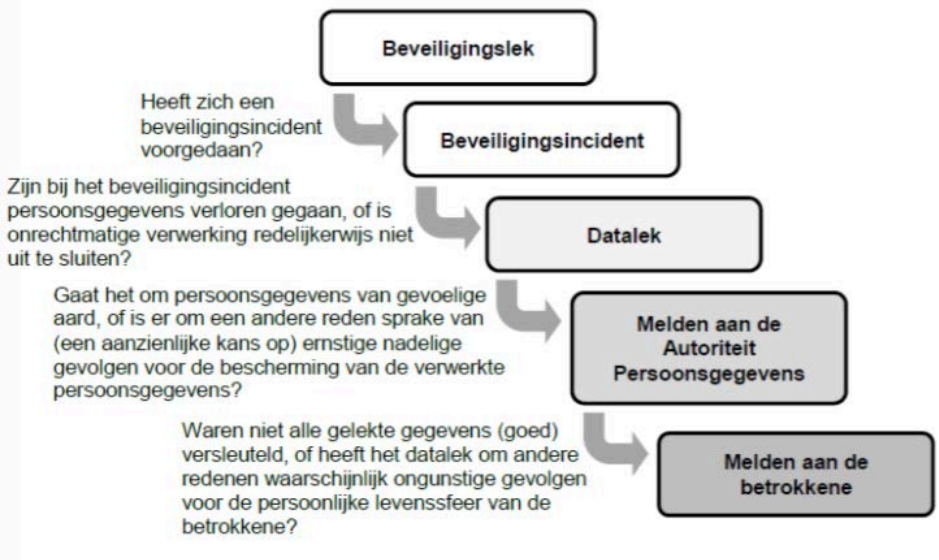
   De volgende informatie wordt daarna vastgelegd:
   - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen
     - Type persoonsgegevens in kwestie
     - Worden de gegevens binnen een keten gedeeld
   - Het al dan niet informeren van de betrokkenen en met welke boodschap
   - Genomen maatregen

3. **Beoordelen**
   Wanneer de Functionaris Gegegevensbescherming 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.
   Voor vervolgstappen wordt gebruik gemaakt van de beslisboom in combinatie met pas toe en leg uit principe. De Functionaris Gegevensbescherming geeft na het

doorlopen van de beslisboom een advies aan de bestuurder. Deze beslist over de te ondernemen acties. Bij een lek door de bestuurder besluit de Algemene Ledenvergadering of 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, en als het ongunstige gevolgen heeft voor persoonlijke levenssfeer van betrokkene dan moet er gemeld worden. Hiervan 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 Functionaris Gegevensbescherming dit aan de bestuurder adviseren. Wanneer bestuurder besluit tot melding dan draagt de Functionaris Gegevensbescherming daarvoor zorg via 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 de Functionaris Gegevensbescherming waarmee het incident is afgesloten. Een samenvatting van de genomen maatregelen wordt door de bestuurder aan de Ontdekker gezonden.

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 ervan 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 Functionaris Gegevensbescherming van het samenwerkingsverband maakt jaarlijks een analyse van de meldingen van beveiligingsincidenten en datalekken.
   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.