PRIVACY OP SCHOOL

Beveiligingsincidenten en Datalekken

Versie	Status	Datum	Auteur	Omschrijving
2.0	Definitief	Sept'26	B.Cornel	Def. versie

1. Vooraf

Dit protocol wordt gehanteerd bij het melden en afhandelen van (mogelijke) beveiligingsincidenten binnen SKOVV of (mogelijke) beveiligingsincidenten die buiten onze organisatie hebben plaatsgevonden, maar waarvoor SKOVV als verwerkingsverantwoordelijke verantwoordelijkheid draagt (bijvoorbeeld als een beveiligingsincident zich bij een verwerker van SKOVV voordoet).

In het protocol is vastgelegd hoe en naar wie de meldingen intern doorgezet dienen te worden, wie verantwoordelijk is voor welke melding en hoe de melding aan de Autoriteit Persoonsgegevens (AP) en eventueel ook aan de betrokkenen wordt gedaan.

2. Inleiding

Regelmatig lezen we in de media dat gegevens van werknemers, studenten of patiënten letterlijk op straat liggen; dossiers die worden aangeboden als oud papier, een gestolen smartphone of een verloren USB-stick. Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben spreken we van een datalek. Het risico op datalekken wordt steeds groter omdat onze persoonsgegevens in steeds meer databanken en/of op informatiedragers zijn opgeslagen. Een datalek kan nadelige gevolgen hebben voor de privacy van degene van wie de persoonsgegevens zijn gelekt. Weggelekte persoonsgegevens kunnen oneigenlijk gebruikt worden. Identiteitsfraude is hier een voorbeeld van.

We kunnen drie categorieën datalekken onderscheiden:
Inbreuk op de beschikbaarheid; Wanneer de toegang tot persoonsgegevens niet meer mogelijk is of persoonsgegevens vernietigd zijn.
Inbreuk op de integriteit; Als er sprake is van onbevoegd of onopzettelijk wijzigen van persoonsgegevens.
Inbreuk op de vertrouwelijkheid; Als er sprake is van een onbevoegde of onopzettelijke toegang tot of openbaring van persoonsgegevens.

In de AVG is de meldplicht voor datalekken opgenomen in artikel 33 en 34. Deze meldplicht verplicht organisaties, dus ook scholen, om datalekken te melden bij de toezichthouder, de Autoriteit Persoonsgegevens (AP) en, in sommige gevallen, ook bij de betrokkenen (de personen op wie de gegevens die zijn gelekt betrekking hebben).

Indien de meldplicht aan betrokkene en/of de AP niet wordt nagekomen riskeert SKOVV een hoge boete die kan oplopen tot 2% van de totale omzet (artikel 83, lid 4 AVG). Alleen die inbreuken die waarschijnlijk leiden tot een risico voor de rechten en vrijheden van de betrokkenen, moeten bij de AP worden gemeld. Door deze

clausulering worden inbreuken met geringe nadelige gevolgen voor de bescherming van persoonsgegevens uitgezonderd van de meldplicht, maar moeten wel door SKOVV geregistreerd te worden in een register voor beveiligingsincidenten.

3. Begripsbepalingen

In dit protocol worden onder meer de volgende termen gebruikt:
Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. In ons geval gaat het dan om leerlinggegevens, gegevens van ouders, leerkrachten en van de personen die voor ons werkzaam zijn;
Betrokkene: de persoon op wie de persoonsgegevens betrekking hebben;
Beveiligingsincident: een gebeurtenis (niet uitsluitend digitaal!) 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 (niet uitsluitend digitaal!) waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt (denk aan: opgeslagen, aangepast, verzonden, et cetera) of als dit niet uit te sluiten is. Of anders gezegd: een inbreuk op de informatiebeveiliging waarbij persoonsgegevens verloren gaan of in handen komen van derden die geen toegang tot die gegevens mogen hebben, of dat toegang door onbevoegden niet uitgesloten kan worden.

Alle datalekken zijn dus beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.

Bij ieder beveiligingsincident zal moeten worden vastgesteld of er sprake is van een datalek.

4. Rollen bij een (mogelijk) beveiligingsincident

SKOVV onderscheidt vier rollen om een (mogelijk) beveiligingsincident succesvol af te handelen:

1. De **Ontdekker:** degene die een (mogelijk) beveiligingsincident op het spoor komt en het proces in werking stelt. Dat kan dus iedere medewerker zijn, maar ook ouders of relaties (verwerkers). Indien een ouder, leerling, relatie of andere derde een (mogelijk) beveiligingsincident opmerkt, is het van belang dat hij/zij dit onmiddellijk meldt bij de directeur van de school.

2. Het **Meldpunt (Privacy Officer):** de centrale locatie binnen SKOVV waar alle (mogelijke) beveiligingsincidenten door de **Ontdekker** moeten worden gemeld. De gegevens over het (mogelijk) beveiligingsincident worden er geregistreerd en verder verwerkt in een register voor beveiligingsincidenten. Het meldpunt is bereikbaar via het e-mailadres privacy@skovv.nl

3. De **Melder (FG):** degene die namens de verwerkingsverantwoordelijke (bestuur van SKOVV) verantwoordelijk is voor het beoordelen van het beveiligingsincident en het eventueel melden van een datalek bij de AP en (indien van toepassing) aan de Betrokkene(n). De melder is bij SKOVV de Functionaris voor Gegevensbescherming (FG). Het melden gebeurt onder verantwoordelijkheid van de directie.

4. De **Technicus**: ICT Coördinator of de externe ICT -Dienstverlener: deze kan de oorzaak van het beveiligingsincident vinden en (laten) repareren en de gevolgen mitigeren. Deze genomen maatregel moet worden vastgelegd in het register bij betreffende incident.

5. Stappenplan bij een (mogelijk) beveiligingsincident

8 –Ontdekken} door alle medewerkers en externen

- De ontdekker merkt een (mogelijk) beveiligingsincident op. Dit kan via eigen waarneming of via waarneming van een derde. De ontdekker kan een medewerker, maar ook een ouder, leerling of relatie (verwerker) zijn.
- De ontdekker meldt het door hem of haar opgemerkte (mogelijke) beveiligingsincident direct bij het meldpunt via privacy@skovv.nl of bij de directeur van de school. In het geval van mailen wordt in het onderwerp van de e-mail “(mogelijk) Beveiligingsincident” en de naam van de school worden vermeld, zodat voor het meldpunt direct duidelijk is waar het om gaat. Bovendien moet de e-mail als “urgent” worden verzonden.

9 –Inventariseren en vastleggen} door het meldpunt

Het meldpunt (de Privacy Officer, als IBP-verantwoordelijke van SKOVV) verzamelt zo spoedig mogelijk alle relevante informatie met betrekking tot het (mogelijke) beveiligingsincident en legt e.e.a. vast. Het meldpunt kan daarvoor aanvullende vragen uitzetten bij de ontdekker en /of de technicus.

De volgende informatie wordt door het meldpunt verzameld en vastgelegd (lijst is niet uitputtend en afhankelijk van het incident):

- een samenvatting van het beveiligingsincident; waar heeft het incident plaats gevonden en wat is er met de gegevens gebeurd;
- aard van de inbreuk;
- datum/periode van het beveiligingsincident;
- vond het beveiligingsincident plaats in een verwerking die is uitbesteed aan een andere organisatie (een verwerker), zo ja, wat is de naam van de verwerker;
- een nadere omschrijving van:
  - de categorieën van betrokkenen (leerlingen, ouders, leerkrachten etc.);
  - (bij benadering) het aantal betrokkenen;
  - type persoonsgegevens (bijzondere gegevens of van gevoelige aard?);
- de vooralsnog bekende en/of te verwachten gevolgen die het beveiligingsincident voor de persoonlijke levenssfeer van de betrokkenen kan hebben;
- worden de gegevens binnen een keten gedeeld, en zo ja: welke keten
- de mogelijke technische beschermingsmaatregelen die zijn genomen (denk aan versleuteling, encryptie, hashing etc.);
- de technische en organisatorische maatregelen die zijn getroffen om het beveiligingsincident aan te pakken en in de toekomst te voorkomen.

Alle informatie die wordt verzameld dient schriftelijk te worden **vastgelegd**. Hiervoor wordt het register voor beveiligingsincidenten gebruikt in YourSafetyNet.
Wanneer het meldpunt voldoende informatie heeft verzameld, stuurt het meldpunt de melder (FG) een verzoek om de verzamelde informatie te bekijken.

0-Beoordelen

De FG beoordeelt de feiten en geeft advies over de te nemen stappen. Als de FG adviseert om de AP (en evt. betrokkenen) te informeren dan wordt dit advies voorgelegd aan het bestuur. Het bestuur besluit vervolgens of het datalek wel of niet gemeld wordt aan de AP en betrokkenen.

De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de AP? Of waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Of 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 rekening gehouden met:

- het type gegevens en
- met de hoeveelheid gegevens.
- Als extra verificatie, wordt het stappenplan van de AP in dit proces meegenomen. Zie: schema Autoriteit Persoonsgegevens

Als het datalek leidt tot een aanzienlijke kans op, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er een melding worden gedaan bij de Autoriteit Persoonsgegevens. Van ernstige nadelige gevolgen of de kans daarop is bijvoorbeeld sprake wanneer er veel gegevens van een betrokkene of gegevens van 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. Als de betrokkene jonger is dan 16 jaar worden de ouders ingelicht.

De melding aan betrokkene(n) mag achterwege worden gelaten als:

- er voordat het datalek plaatsvond passende maatregelen zijn getroffen waardoor de gelekte persoonsgegevens onbegrijpelijk zijn voor onbevoegden.
  Let op: deze uitzondering geldt alleen als:
  - de gegevens nog volledig intact zijn;
  - er nog steeds volledige controle is over de gegevens;
  - de sleutel die voor de encryptie of voor de hashing is gebruikt bij de inbreuk geen gevaar heeft gelopen en voor onbevoegden met de beschikbare technologische middelen niet te vinden is;
  - er onmiddellijk nadat het datalek heeft plaatsgevonden, maatregelen zijn getroffen waardoor het hoge risico voor de rechten en vrijheden van betrokkene(n) zich waarschijnlijk niet meer zal voordoen (bijvoorbeeld doordat de gelekte persoonsgegevens onmiddellijk na het datalek zijn gewist, nog voordat de onbevoegde ontvanger iets met de gegevens kon doen);
- wanneer het niet melden noodzakelijk en evenredig is ter waarborging van: a. de nationale veiligheid; b. landsverdediging; c. de openbare veiligheid; d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Bij ieder beveiligingsincident wordt beoordeeld of er aanwijzingen zijn voor of vermoedens van strafbaar handelen (zoals bijvoorbeeld hacken). Indien dit het geval is, kan aangifte worden gedaan bij de Politie.

Als een ontdekker het niet eens is met de beslissing van de melder om een (vermoedelijk) datalek wel of niet te melden aan de AP en/of de betrokkene(n), dan richt hij of zij zich tot het college van bestuur teneinde zijn of haar bedenkingen aldaar te bespreken. Het is de ontdekker (meestal medewerker) niet toegestaan om een (vermoedelijk) datalek zelf aan de AP en/of de betrokkene(n) te melden. Zie ook onder punt 5 bij “Communicatie”.

1–Maatregelen treffen

De technicus (de bovenschoolse ICT-coördinator of Privacy Officer wordt door het meldpunt en/of de melder gevraagd (voor zover dat nog niet is gebeurd en voor zover mogelijk) de oorzaak van het beveiligingsincident vast te stellen en (technische) maatregelen te treffen om het beveiligingsincident te (laten) verhelpen en de gevolgen van het beveiligingsincident te beperken. De technicus legt het volgende vast:

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

Ook wordt gevraagd om (technische) maatregelen te treffen om herhaling van het beveiligingsincident te voorkomen. Deze maatregelen worden zo spoedig mogelijk in gang gezet.

2–Melden en communicatie} door de FG ,melder«

Bij de AP

Indien de conclusie bij stap 3 is dat er sprake is van een datalek dat bij de AP gemeld dient te worden, dan zal de FG dit in overleg met het bestuur zo snel mogelijk doch liefst binnen 72 uur na het ontdekken van het datalek melden. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Als nog niet alle informatie over het datalek bekend is, zal alvast een incomplete melding worden gedaan, zodat de AP tijdig is geïnformeerd. Ontbrekende informatie kan later worden toegevoegd.
Het datalek wordt gemeld bij het Meldloket datalekken Autoriteit Persoonsgegevens: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Communicatie naar betrokkenen

Indien de conclusie bij stap 3 is dat een datalek ook moet worden gemeld aan de betrokkene(n), dan moet dit zo snel mogelijk, liefst binnen een week, plaats te vinden.

De melding aan betrokkene(n), dient in ieder geval behoorlijk en zorgvuldig uitgevoerd te worden, en de volgende informatie te bevatten:

- aard van de inbreuk, waarbij volstaan kan worden met een algemene omschrijving van wat er is gebeurd;
- waar men terecht kan met vragen, denk hierbij aan het telefoonnummer/e-mailadres van de FG of een speciaal telefoonnummer/e-mailadres voor vragen;
- aanbevolen maatregelen om negatieve gevolgen te beperken, zoals het veranderen van wachtwoorden.

De betrokkene(n) dienen in beginsel individueel te worden geïnformeerd, maar als het individueel informeren van de betrokkene(n) een onevenredige inspanning vergt, bijvoorbeeld omdat de contactgegevens van de betrokkene(n) door het datalek verloren zijn gegaan, dan mogen de betrokkene(n) ook worden geïnformeerd met een openbare mededeling of een soortgelijke maatregel, waarbij de betrokkene(n) even doeltreffend worden geïnformeerd.

Overige Communicatie

Bij het melden aan de AP en eventueel de Betrokkene(n) en/of de politie is de communicatie een belangrijk punt van aandacht. Het is van groot belang dat alle communicatie (zowel geschreven pers, sociale media platforms alsmede alle overige communicatieplatforms) uitsluitend via de melder en/of het bestuur in onderling overleg plaatsvindt. Ieder ander dient zich te allen tijde te onthouden van enig commentaar en hiervoor te verwijzen naar de melder en/of het bestuur van SKOVV.

3–Vastleggen} door het Meldpunt

Alle informatie die in de voorafgaande stappen met betrekking tot een beveiligingsincident is ingewonnen of ontstaan, wordt door het meldpunt (in samenspraak met de melder) geregistreerd in het “register voor beveiligingsincidenten" in YourSafetyNet. Met deze registratie wordt het afhandelen van het beveiligingsincident afgesloten.

6. Responsible Disclosure

Het kan zijn dat ondanks de genomen maatregelen om onze ict systemen te beschermen er toch een kwetsbaarheid ontdekt wordt. SKOVV vraagt in die gevallen de ontdekker hiervan een bijdrage te leveren aan de veiligheid van ict-systemen en het beheersen van de kwetsbaarheid van ict-systemen. Dat kan gedaan worden door de ontdekte kwetsbaarheden op verantwoorde wijze bij SKOVV te melden, zodat zo snel mogelijk aanvullende (beveiligings)-maatregelen getroffen kunnen worden.

7. Beheer beveiligingsincidenten

Het meldpunt maakt in samenwerking met de FG twee keer per jaar een analyse van alle meldingen van de beveiligingsincidenten die zij heeft ontvangen. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om extra maatregelen te nemen om herhaling te voorkomen. De (G)MR wordt geïnformeerd over de uitkomsten van de analyse.

8. 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 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.

Maak schriftelijke afspraken met uw verwerker(s) over datalekken. Hiervoor kan gebruik worden gemaakt van de meest recent versie van model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).