Procedure datalekken

Waarom deze procedure?

Beveiligingsincidenten kunnen leiden tot informatie/gegevens die verloren gaan of onbedoeld gewijzigd worden. Dit kan gevolgen hebben voor de kwaliteit en continuïteit van het onderwijs. Daarnaast kunnen vertrouwelijke gegevens door beveiligingsincidenten op straat komen te liggen of in verkeerde handen vallen. Voor de verwerking van persoonsgegevens zijn regels vastgelegd Algemene Verordening Persoonsgegevens (AVG). Het niet zorgvuldig omgaan met vertrouwelijke gegevens kan leiden tot boetes en imagoschade. Als een beveiligingsincident betrekking heeft op persoonsgegevens, moet er mogelijk binnen 72 uur melding worden gemaakt aan de Autoriteit Persoonsgegevens.

Wat is een beveiligingsincident?

Een beveiligingsincident is een gebeurtenis waarbij gegevens:
1. verloren zijn geraakt
2. gestolen zijn
3. beschadigd zijn
4. onbedoeld gewijzigd zijn
5. onrechtmatig toegankelijk zijn voor derden

Wat is een datalek?

Er is sprake van een datalek als er bij een opgetreden beveiligingsincident persoonsgegevens betrokken zijn.

Wat zijn persoonsgegevens?

Alle gegevens die (evt. gecombineerd met andere gegevens) tot een persoon herleid kunnen worden. Voorbeelden persoonsgegevens: naam / BSN / pasfoto / geboortedatum / adres / IP-adres / etc.

Stap 1: zorg voor overzicht

Analyseer onmiddellijk de situatie. Zorg dat u weet wat er is gebeurd en wat de omvang van het lek is. Gaat het om een inbreuk door gelekte, vernietigde of gewijzigde gegevens? Indien gegevens zijn gelekt, onderzoek dan wie er (mogelijk) toegang hebben (gehad) tot welke persoonsgegevens. Deze informatie heeft u nodig voor de vervolgstappen.

Heeft de melding betrekking op persoonsgegevens? Meld dit direct bij de privacy officer privacy@hannahscholen.nl of bij de FG lars@privacyopschool.nl / 06-48080297.
Is er sprake van opzettelijk misbruik of strafbare feiten, zoals diefstal, hacken of DDOS? Neem (ook) contact op met de schooldirecteur in verband met te nemen sancties en/of het doen van aangifte.

Indien er een melding wordt gedaan van een beveiligingsincident, dan worden de volgende gegevens geregistreerd:

- Ontdekker incident:

- Datum:
- Tijdstip:
- Omschrijving incident:
- Getroffen maatregelen:

Aanvullende gegevens:
- Betrokkenen:
- Omvang gegevens: (aantal personen)
- Locatie:
- Type hardware (tagcode):
- Naam software:
- Back-up aanwezig?: ja/nee
- Zijn de gegevens geëncrypt?: ja/nee

De privacy officer controleert of alle gegevens zijn geregistreerd over het beveiligingsincident. Deze registratie wordt aangevuld met eventuele informatie die uit de volgende stappen naar voren komt.

Stap 2: Beperk de schade!

Bepaal op basis van stap 1 of er maatregelen zijn die u meteen kunt nemen om het datalek te beëindigen en de schade te beperken. En zo ja, neem deze maatregelen onmiddellijk. Bijvoorbeeld door een gestolen laptop op afstand te wissen. Maak tegelijkertijd een inschatting van het (mogelijke) risico dat het datalek oplevert (stap 3).

Aan de hand van de verzamelde gegevens wordt de prioriteit bepaald en herstelmaatregelen uitgevoerd.

Is er sprake van diefstal, verlies of beschadiging?
Dan moet het systeem vervangen worden en/of de back-up teruggeplaatst worden (indien aanwezig). De systeembeheerder wordt ingeschakeld.

Is er sprake van onrechtmatige toegang?
Dan dient de toegang afgesloten te worden door fysieke beveiliging, een wijziging in de configuratie van het netwerk of in de accounts (door de accountbeheerders).

Is er sprake van DDOS aanval op servers die in beheer zijn van de school?
Dan dient relevante netwerkapparatuur afgesloten of opnieuw geconfigureerd te worden, eventueel in overleg met leveranciers of externe beheerders. De systeembeheerder wordt ingeschakeld.

Is er sprake van malware of anti-virus aanvallen?
Dan dient de computer of apparatuur uit het netwerk genomen, opgeschoond en hersteld te worden. Indien nodig dienen back-ups teruggeplaatst te worden. De systeembeheerder wordt ingeschakeld.
Zijn er persoonsgegevens van gevoelige aard gelekt of leidt de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Indien Ja → Ga naar stap 3
Indien Nee → Er is geen sprake van meldplicht, overleg met systeembeheer over preventieve maatregelen. Ga naar stap 4

Gegevens van gevoelige aard:
Godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakvereniging, strafrechtelijke gegevens of over onrechtmatig of hinderlijk gedrag, financiële gegevens of over de economische situatie, gegevens die kunnen leiden tot stigmatisering (schoolprestaties, relatieproblemen), gebruikersnamen en wachtwoorden, gegevens die kunnen worden gebruikt bij identiteitsfraude (BSN)

Nadelige gevolgen:
Misbruik in het criminele circuit van grote databestanden, ingrijpende beslissingen die op basis van (gewijzigde) gegevens worden genomen, gevolgen die binnen ketens van gegevensverwerking kunnen optreden.

Stap 3: Wel/niet melden bij de AP

Bepaal of u het datalek verplicht moet melden bij de Autoriteit Persoonsgegevens (AP). Zo ja, zorg dat u dit ***binnen 72 uur*** nadat u het lek heeft ontdekt doet. U moet een datalek melden bij de AP tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen.

Heeft u bij de eerste melding nog niet alle informatie over het datalek?
Doe dan een eerste melding binnen 72 uur en doe later een vervolgmelding.

Naar het meldloket datalekken
Zie ook: voorbeeldlijst 'datalek wel/niet melden bij AP en betrokkenen'

Zijn er bij het incident persoonsgegevens verloren gegaan?
Er is geen kopie of back-up aanwezig van de persoonsgegevens

Is er bij het incident sprake van onrechtmatige verwerking van persoonsgegevens? En kan dit niet uitgesloten worden?
Onbevoegden hebben onrechtmatig toegang kunnen krijgen tot de persoonsgegevens

Indien Ja op één van beide → schakel de FG'er in. De FG'er bepaalt of het datalek gemeld moet worden bij de AP. De bestuurder is betrokken bij een melding aan de AP.

Indien Nee op beide → er is geen sprake van een datalek, overleg met systeembeheer over preventieve maatregelen

Melding bij AP
-De FG'er verzamelt alle benodigde informatie
-Na toestemming van het college van bestuur wordt door de FG'er een melding gedaan via https://datalekken.autoriteitpersoonsgegevens.nl/

De melding wordt minimaal 3 jaar bewaard. Informeer indien nodig de leverancier over de melding.

Stap 4: Wel/niet melden aan de betrokken personen

Bepaal of u het datalek verplicht moet melden aan de betrokken personen. Zo ja, zorg dat u dit zo snel mogelijk doet. U moet een datalek melden aan de betrokken personen wanneer er sprake is van een *hoog* risico voor de rechten en vrijheden van de betrokken personen.

In de kennisgeving aan de betrokkene wordt in ieder geval vermeld:
Een algemene omschrijving van de aard van het incident, de contactgegevens om meer informatie over de inbreuk te verkrijgen en de maatregelen die genomen zijn en/of door betrokkene genomen moeten worden om negatieve gevolgen te beperken. Bij grootschalige datalekken dient er ook een persbericht in overleg met de bestuurder opgesteld te worden.

Stap 5: Registreer het datalek

Registreer het datalek in uw verplichte datalekregister. Ook wanneer u het datalek niet meldt aan de AP.

Zie ook: 10 praktische tips voor betere datalekregistratie

De melding kan pas afgesloten worden als de herstelmaatregelen zijn uitgevoerd en er preventieve maatregelen zijn genomen en beschreven om het risico op toekomstige incidenten te vermijden of te verkleinen. De herstelmaatregelen en preventieve maatregelen worden geregistreerd bij de melding.

N.B. De registratie van meldingen wordt meegenomen in de periodieke evaluatie van het privacybeleid van ons bestuur. In de evaluatie wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.