Kwaliteitskaart Wijs! – H&F – Meldplicht datalekken

Kaart	**Kwaliteitskaart Wijs! – H&F – Meldplicht datalekken**
Eigenaar	**Staffunctionaris facilitair**
Versie	**Februari 2023**

Doel

Via deze kwaliteitskaart wordt uitgelegd wat een datalek is, waar dit gemeld moet worden en welke stappen we zetten om de melding te behandelen.

Aanleiding

Binnen Wijs! verwerken we informatie over onze organisatie en persoonsgegevens van onder andere onze leerlingen, ouders en medewerkers. Wanneer informatie of persoonsgegevens worden gelekt, kan dit schade opleveren voor de betrokken personen. In geval van een dergelijk incident moeten we daarom zo snel mogelijk hiervan op de hoogte zijn, zodat we de impact kunnen beperken. Daarnaast zijn we in bepaalde gevallen wettelijk verplicht om datalekken binnen 72 uur te melden.

Wat is nu een datalek?

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens en om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgevens, zonder dat dit wettelijk is toegestaan. Hierdoor kunnen de betrokken personen mogelijk schade leiden.

Denk bijvoorbeeld aan:
- Het versturen van een e-mail met persoonsgegevens naar de verkeerde ontvanger;
- Een gestolen of gehackte laptop;
- Het klikken op een phishing e-mail;
- Het verstrekken van teveel persoonsgegevens;
- Meekijkers op je scherm.

Voorbeelden:
Top 10 datalekken - En tips om deze te voorkomen!

Datalek melden

Alle (mogelijke) datalekken moeten gemeld worden. Degene die dit constateert meldt het onmiddellijk uiterlijk binnen 24 uur bij de directie. Ook bij twijfel! Een datalek wordt altijd gemeld bij de interne privacy officer (Staffunctionaris H&F) via bestuur@wijs-utrecht.nl door middel van het “melden datalekformulier” te vinden in kwaliteitsbieb.

De directeur:

- zorgt voor overzicht;
- beperkt de schade;
- meldt bij de privacy contactpersoon van Wijs!.

De privacy contactpersoon van Wijs!:

- beoordeelt de binnengekomen melding,
- verzamelt zo snel mogelijk alle relevante informatie en zet zo nodig een aantal acties uit (in samenspraak met de betrokken schooldirecteur/bestuurder).
- De melding wordt geregistreerd in het incidentenregister van Wijs!.

In geval van een mogelijk datalek neemt de privacy contactpersoon van Wijs! binnen 72 uur contact op met de bestuurder van Wijs! en de externe Functionaris Gegevensbescherming voor verdere beoordeling.
Beoordeeld wordt:

- Of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens;
- Of de betrokken personen geïnformeerd moeten worden;
- Welke maatregelen genomen moeten worden om negatieve effecten te verminderen.

Het advies van de externe Functionaris Gegevensbescherming wordt door de privacy contactpersoon gedeeld met de betrokken schooldirecteur en de bestuurder. Op basis van het advies kunnen verdere stappenondernomen worden.

- Er wordt bepaald hoe verdere communicatie verloopt;
- De Externe Funtionaris Gegevensbescherming draagt zorg voor registratie van het datalek in het (verplichte) datalekregister.

Stappenplan

AUTORITEIT
PERSOONSGEGEVENS

Stappenplan: kom in actie bij een datalek

Heeft uw organisatie te maken met een datalek? Dan is het belangrijk dat u als privacycontactpersoon snel in actie komt. Met dit stappenplan helpen we u op weg.

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.

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).

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'

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.

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

Heeft u bovenstaande stappen doorlopen? En alles gedaan om de schade te beperken?
Start dan een evaluatie om een herhaling van het datalek te voorkomen.

Literatuur of verder lezen?

Wil je meer weten over privacy en de meldplicht datalekken? Kijk dan eens op

Meldplicht datalekken

informatie over datalek