PROTOCOL

Naam: Format Rapportage datalek / beveiligingsincident
(na invulling: VERTROUWELIJK)

Vastgesteld door DO: 29 maart 2021
Vastgesteld door bestuur: 15 februari 2021
Vastgesteld door GMR: 28 januari 2021
Update vastgesteld door GMR: januari 2024

Melding datalekken
Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht 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. Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of waarbij het niet valt uit te sluiten dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie 'gelekt'. Als er een Datalek is, moet daar binnen 72 uur na ontdekking van het lek melding worden gedaan bij de Autoriteit Persoonsgegevens.
Dit protocol handelt over het format datalekken met daarbij genoemd de procedures die belangrijk zijn vanuit de veschillende functies en is een bijlage van het protocol datalekken en informatiebeveiligingsincidenten.

Procedure voor ontdekker
De ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De ontdekker mailt direct naar datalek@hsn-scholen.nl. De ontdekker ontvangt een automatisch antwoord waarop de stappen staan die ondernomen moeten worden:

1. de directeur wordt in kennis gesteld;
2. de betrokkenen en de ontvangers van het lek worden in kennis gesteld van het lek en er worden excuses aangeboden door de ontdekker, zowel mondeling als schriftelijk. Tevens worden de betrokkenen en ontvangers in kennis gesteld dat de ontdekker het beveiligingsincident bespreekt met de privacy officer;
3. de ontdekker mailt het beveiligingsincident naar de directeur en CC naar de privacy officer en de functionaris gegevensbescherming en voegt daarbij de rapportage datalek en beveiligingsincident en de schriftelijke communicatie met betrokkenen;
4. de ontdekker krijgt reactie van de privacy officer of er voldoende informatie gegeven is of dat er aanvullende informatie wordt verwacht;
5. de ontdekker houdt contact met de directeur totdat het beveiligingsincident is afgerond.

Procedure voor directeur

1. de directeur wordt op de hoogte gebracht van een beveiligingsincident door de ontdekker;
2. de directeur spreekt met de ontdekker af wie er contact houdt met de betrokkenen en de ontvangers;
3. de directeur neemt contact op met de privacy officer. Tijdens dit gesprek wordt een eerste inschatting gemaakt of het een beveiligingsincident betreft of dat er sprake is van een datalek wat gemeld moet worden bij de Autoriteit Persoonsgegevens;
4. de directeur hoort definitief van de privacy officer of er sprake is van een beveiligingsincident of van een datalek wat gemeld moet worden bij de Autoriteit Persoonsgegevens;
5. bij melding bij de Autoriteit Persoonsgegevens, is de directeur verantwoordelijk voor de melding. Deze vindt binnen 72 uur plaats nadat de directeur op de hoogte is gebracht van een beveiligingsincident door de ontdekker via https://datalekken.autoriteitpersoonsgegevens.nl/;
6. bij melding bij de Autoriteit Persoonsgegevens stelt de directeur, de algemeen directeur op de hoogte.
7. als de directeur de rapportage datalek en beveiligingsincident heeft ontvangen, verwerkt de directeur het rapport in PCC met daarbij alle schriftelijke communicatie die er is geweest zodat het proces achteraf gereproduceerd kan worden;
8. na afronding van het incident vindt er via Teams een evaluatie plaats met de directeur, privacy officer en functionaris gegevensbescherming en bij melding bij de Autoriteit Persoonsgegevens ook met de algemeen directeur.

Procedure voor de algemeen directeur

1. als de privacy officer en de functionaris gegevensbescherming adviseren om het datalek te melden bij de Autoriteit Persoonsgegevens stelt de privacy officer de algemeen directeur op de hoogte van het advies;
2. de algemeen directeur beslist op grond van alle beschikbare gegevens of er gemeld wordt bij de Autoriteit persoonsgegevens;
3. de algemeen directeur stelt de directeur van de betreffende school en de privacy officer op de hoogte van zijn beslissing;
4. mocht het datalek zodanig zijn dat de pers erbij komt, is de algemeen directeur degene die de communicatie verzorgd;
5. bij melding vindt er na afronding van het incident een evaluatie plaats met de algemeen directeur, directeur, privacy officer en functionaris gegevensbescherming.

Procedure voor privacy officer

1. de privacy officer wordt op de hoogte gebracht van een beveiligingsincident door de directeur en via de mail door de ontdekker;
2. de privacy officer bespreekt met de directeur de aard van het incident en maakt een voorlopige inschatting van de ernst van het lek;
3. de privacy officer neemt contact op met de functionaris gegevensbescherming en bespreekt de melding;
4. de privacy officer stelt de directeur op de hoogte van de beoordeling van de functionaris gegevensbescherming en stelt ook de ontdekker op de hoogte via de mail. In deze mail komt ter sprake wat de beoordeling is en ook of er nog aanvullende informatie nodig is voor een juiste beoordeling;
5. de privacy officer meldt het beveiligingsincident aan de algemeen directeur en stelt hem op de hoogte van het advies;
6. na afronding van het incident vindt er via Teams een evaluatie plaats met de directeur, privacy officer en functionaris gegevensbescherming en bij melding bij de Autoriteit Persoonsgegevens ook met de algemeen directeur;
7. de privacy officer checkt na afloop of de directeur de rapportage datalek en beveiligingsincident heeft geüpload in PCC;
8. de privacy officer sluit het datalek uiteindelijk af in PCC.

Procedure voor functionaris gegevensbescherming

1. de functionaris gegevensbescherming wordt op de hoogte gebracht van een beveiligingsincident door de privacy officer;
2. de functionaris gegevensbescherming bepaalt of het incident gemeld moet worden bij de Autoriteit Persoonsgegevens. Bij de beoordeling wordt er 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 betrokkenen moet er gemeld worden;
3. de functionaris gegevensbescherming initieert na afloop van het incident een evaluatie via Teams met de directeur, privacy officer en functionaris gegevensbescherming en bij melding bij de Autoriteit Persoonsgegevens ook met de algemeen directeur;
4. De functionaris gegevensbescherming checkt bij de privacy officer of de rapportage datalek en beveiligingsincident is geüpload in PCC.

Gegevens privacy officer en functionaris gegevensbescherming:

1. Privacy officer: Erna Luiten; e.luiten@hsn-scholen.nl; 06-33779566
2. Functionaris gegevensbescherming; Rob van Son; r.vanson@privaty.nl; 06-18719908

Bijlage 1 – Rapportage beveiligingsincident en datalek

Datum	**Actie**
	Datalekmelding binnengekomen Contact met: Verzoek om meer informatie Voorzitter of lid College van Bestuur geïnformeerd Ja / Nee

Ontdekker/melder

Naam	
School	
E-mail	
Telefoonnummer	

Omschrijving
Korte omschrijving:

Uitgebreide omschrijving: (wordt eventueel per datum aangevuld om ontwikkelingen te volgen en te kunnen reproduceren – logboek)

Beoordelen ernst datalek

Wat was de oorzaak? *(Menselijke fout; verkeerde inrichting systeem; fout in software; hacken?)*	
Wie en hoeveel zijn er bij betrokken, van wie zijn gegevens gelekt? Zijn de betrokkenen in groepen in te delen en om hoeveel aantallen betrokkenen gaat het? Welke categorie persoonsgegevens zijn betrokken bij het incident?	
Zijn er minderjarigen betrokken?	Ja/ Nee
Zijn er personen uit kwetsbare groepen betrokken?	Ja/ Nee
Waren de persoonsgegevens versleuteld op het moment van het datalek?	Ja/ Nee
Welke gevolgen voor de persoonlijke levenssfeer van de betrokkenen kunnen er ontstaan?	
- Discriminatie?	0
- Identiteitsdiefstal?	0
- Reputatieschade?	0
- Verlies van vertrouwen van door het beroepsgeheim beschermde persoonsgegevens?	0
Hoe lang heeft het datalek bestaan?	
Welke maatregelen zijn genomen om het datalek te dichten?	

Zijn de betrokkenen geïnformeerd?	Ja/Nee
Hoe zijn de betrokkenen geïnformeerd? (Noteer datum + actie)	
Datum: Actie:	
Datum: Actie:	
Datum: Actie:	
Welke corrigerende maatregelen zijn genomen om de gevolgen voor de betrokkenen de beperken?	
Datum: Actie:	
Datum: Actie:	
Welke preventieve maatregelen worden genomen om in de toekomst dergelijke beveiligingsincidenten c.q. datalekken te voorkomen?	
Datum: Actie:	
Datum: Actie:	
Verstuur deze rapportage naar e.luiten@hsn-scholen.nl en naar fg@hsn-scholen.nl en naar je directeur.	

Advies Privacy Officer (PO)
Melden bij AP? J/N
Motivatie:

Advies Functionaris Gegevensbescherming (FG)
Melden bij AP? J/N
Motivatie:

Besluitvorming door bestuurder
Melden bij AP? J/N
Motivatie:

Melding bij AP
Melding bij AP? J/N
Dossiernummer bevestiging AP:

Bijlage 2 – automatisch antwoord bij mailen naar datalek@hsn-scholen.nl

Oei, een beveiligingsincident of datalek? Goed dat je mailt. Een snelle reactie is belangrijk bij zoiets, want als het echt een datalek is, moet het binnen 72 uur gemeld zijn bij de Autoriteit Persoonsgegevens.

Hieronder vind je het stappenplan wat je moet volgen:

1. Stel de directeur van je school in kennis.
2. Stel de betrokkenen en de ontvangers van het lek kennis en bied excuses aan voor het datalek en de ontstane situatie. Geef in dat gesprek aan dat je het beveiligingsincident of datalek bespreekt met de functionaris gegevensbescherming en de privacy officer en daarna weer contact met hen opneemt.
3. Mail je directeur en in de CC de Functionaris Gegevensbescherming (Rob van Son) en de Privacy Officer (Erna Luiten) op de volgende mailadressen:
    a. r.vanson@privaty.nl
    b. fg@hsn-scholen.nl
    c. e.luiten@hsn-scholen.nl

    Heb je voldoende tijd? Ga direct naar punt 4.

    Heb je onvoldoende tijd? Gebruik in deze mail de volgende gegevens:

    1. Over het datalek of beveiligingsincident: datum/tijd/periode
    2. Over jou: gegevens van de melder (naam, functie) en hoe kan ik je (snel) bereiken?
    3. Heeft het datalek/incident binnen de school plaatsgevonden? Indien niet binnen de school, waar dan wel? Toedracht van het incident
    4. Wat is er gebeurd: korte beschrijving (tijden, plaatsen, wat is er met gegevens gebeurd, verlies, diefstal, ...)
    5. Gaat het om persoonsgegevens? Om welke / wat voor soort gegevens gaat het?
    6. Wie zijn er betrokken, over wie / wiens gegevens gaat het?
    7. Welke actie is al ondernomen?

    Naar aanleiding van de antwoorden beslist de functionaris gegevensbescherming of de melding als Datalek naar de autoriteit gegevensbescherming moet.
4. Download en vul in het "P AVG Datalek Rapport HSN". Deze is te vinden op:
    - https://hsn-scholen.nl/privacyverkaring/ > Format Datalek Rapport
    - SharePoint > HSN Medewerkers > Documenten > Org&Comm > Protocollen (P AVG Format datalek rapport HSN)
5. Stuur dit rapport ingevuld naar de directeur van je school (CC naar de FG en Erna). Het overlapt 1–7 wel, maar dit Rapport is wat bewaard wordt.
6. Je directeur verwerkt alles in PCC in het Incidentregister en voegt dit rapport bij.

Succes hiermee en hartelijke groet,

Erna Luiten.