Procedure datalekken Rehoboth Scholenvereniging (Vastgesteld, 14-04-2025)

Inleiding
Een schoolbestuur moet elk datalek registreren en in veel gevallen ook melden bij de Autoriteit Persoonsgegevens (AP) en betrokkenen (lees slachtoffers van het datalek) informeren.

AP raadt aan om ook beveiligingsincidenten die geen datalekken zijn te registreren.

Een beveiligingsincident is een fout of lek in de informatiebeveiliging. Een datalek is een beveiligingsincident dat (mogelijk) gevolgen heeft voor de privacy van leerlingen, ouders of medewerkers. Een datalek is altijd een beveiligingsincident maar een beveiligingsincident is niet altijd een datalek.

De volgende datalekken komen het meest voor:

- een mail met persoonsgegevens naar de verkeerde ontvanger
- diefstal van een laptop of het verlies van een USB-stick met niet-versleutelde persoonsgegevens
- hacking van een computer of onbevoegde toegang tot een server.

Een datalek leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van persoonsgegevens of tot ongeoorloofde toegang tot die gegevens. Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’). Er bestaat een onderscheid tussen direct en indirect identificerende gegevens. Direct identificerende gegevens zijn gegevens die betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen, zoals een naam eventueel in combinatie met het adres en de geboortedatum. Van indirect identificerende gegevens is sprake wanneer gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon (bijv. postcode/huisnummer of een leerlingennummer).

Een schoolbestuur is zelf verantwoordelijk om de oorzaak van het datalek te achterhalen en maatregelen te treffen om herhaling te voorkomen.

Procedure
De volgende procedure is gebaseerd op het stappenplan van AP en het protocol informatiebeveiligingsincidenten en datalekken van Kennisnet.

	Stap	Wat moet je doen?	Toelichting
1.	**Herken beveiligings-incident**	Iedereen in de school die werkt met persoonsgegevens moet weten dat de school een registratieplicht en een meldplicht datalekken heeft en dat hij of zij een beveiligings-incident of datalek direct moet melden.	Als er **geen** sprake is van verwerking van persoonsgegevens dan zijn de AVG en deze procedure **niet** van toepassing. Bijv. indien de school per ongeluk een e-mail in BCC verstuurt aan verkeerde personen over een schoolfeest dat binnenkort plaatsvindt.
2.	**Informeer directeur over beveiligings-incident**	Degene die een beveiligings-incident veroorzaakt of constateert meldt dit onmiddellijk aan zijn of haar directeur.	De melder gaat onmiddellijk naar de directeur of belt op. Als dit niet mogelijk is dan mailt melder beveiligingsincident naar de directeur.

3.	**Analyseer de situatie en bepaal aanpak**	De directeur analyseert zo snel mogelijk samen met de melder en de ICT'er van de school de situatie. Betrek indien nodig ook de stafmedewerker ICT die tevens privacy officer is, de systeembeheerder Cloudwise en/of de Functionaris Gegevensbescherming (FG) bij dit overleg. De volgende vragen moeten worden beantwoord: 1. Is er een fout of lek in de informatiebeveiliging? Zo ja, dan is er een beveiligingsincident. 2. Zijn er persoons-gegevens openbaar gemaakt of is er onbevoegd toegang geweest tot persoons-gegevens? 3. Of zijn persoons-gegevens gewijzigd door iemand die daartoe niet bevoegd is? 4. Of kan organisatie niet meer bij de persoons-gegevens komen of zijn die vernietigd? Zo ja, dan is het beveiligings-incident een datalek. De directeur informeert de algemeen directeur. De algemeen directeur spreekt in overleg met de stafmedewerker ICT en de FG af wie wat gaat doen en bevestigt dit per e-mail. Is beveiligingsincident géén datalek? Ga dan naar stap 9.	Als de school **geen** verantwoordingsverantwoordelijke is dan is deze procedure **niet** van toepassing. Bijv. een leerkracht verliest een USB-stick met de contactgegevens van zijn tennis teamgenoten. Contactpersoon Cloudwise: Marjolein ten Dam 06-55182698 m.tendam@cloudwise.nl FG van Rehoboth Scholenvereniging: Clemens Geenen van PEP Onderwijsadvies 06-21210234 info@peponderwijsadvies.nl Indien nodig wordt een crisisteam ingesteld.
4.	**Beperk de schade en leg genomen maatregelen vast**	De stafmedewerker ICT zorgt samen met de systeem-beheerder dat de oorzaak van het beveiligingsincident zo snel mogelijk wordt achterhaald en verholpen.	Bepaal op basis van stap 3 of er maatregelen zijn die u meteen kunt nemen om het beveiligingsincident te beëindigen en de schade te beperken. En zo ja, neem deze maatregelen onmiddellijk. Denk aan blokkeren accounts of op afstand wissen van een gestolen laptop (remote wipe).

			De stafmedewerker ICT legt in het datalekregister 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? Zo ja, hoe?
5.	**Informeer school-bestuur over datalek**	De algemeen directeur informeert schoolbestuur over datalek.	
6.	**Overleg met FG of datalek bij AP en aan betrokkenen gemeld moet worden**	De algemeen directeur overlegt met de FG en de staf-medewerker ICT. Indien nodig wordt de systeembeheerder bij dit overleg betrokken. De volgende vragen moeten worden beantwoord: 1. Houdt datalek risico in voor rechten en vrijheden van betrokkenen? Zo ja, dan moet datalek bij AP worden gemeld. 2. Houdt datalek een hoog risico in voor rechten en vrijheden van betrokkenen? Zo ja, dan moeten betrokkenen worden geïnformeerd. Hoeft datalek niet gemeld te worden bij AP en aan betrokkenen? Ga dan naar stap 9.	AP geeft handvatten om te bepalen of een datalek bij AP moet worden gemeld, zie hieronder bij[1]. Er is geen risico als vooraf passende maatregelen zijn genomen (bijv. versleuteling) waardoor gelekte persoons-gegevens onbegrijpelijk zijn voor onbevoegden. Er is geen hoog risico als: • Er vooraf passende maatregelen zijn genomen waardoor gelekte persoons-gegevens onbegrijpelijk zijn voor onbevoegden. • Er achteraf maatregelen zijn genomen (bijv. remote wipe) waardoor datalek is beëindigd en hoge risico zich waarschijnlijk niet (meer) voordoet. • Een zwaarwegend belang moet worden gewaarborgd zoals bescherming van privacy van anderen.
7.	**Meld datalek bij AP**	De algemeen directeur of de FG meldt het datalek binnen 72 uur bij AP na het ontdekken van het datalek. Bij twijfel wordt een proforma melding gedaan en later een vervolgmelding. Rehoboth Scholenvereniging kan een proforma melding later altijd weer intrekken.	De algemeen directeur meldt het datalek bij AP via het Meldloket Datalekken: zie hieronder bij[2]. Ten onrechte niet melden kan leiden tot boetes van AP. Als Rehoboth Scholenvereniging het datalek wel meldt bij AP maar betrokkenen niet informeert dan

			moet Rehoboth Scholenvereniging in de melding bij AP aangeven dat betrokkenen niet worden geïnformeerd inclusief de redenen waarom niet.
8.	**Informeer betrokken over datalek**	De algemeen directeur zorgt dat betrokkenen geïnformeerd worden over het datalek.	Betrokkenen moeten ook informatie krijgen over mogelijke maatregelen ter beperking van de gevolgen van het datalek. Als persoonlijk informeren een onevenredige inspanning van Rehoboth Scholenvereniging vraagt dan volstaat een openbare mededeling (bijv. via website).
9.	**Vul het register aan en bewaar alle informatie**	De algemeen directeur zorgt samen met de stafmedewerker ICT dat het datalekregister wordt aangevuld.	Alle informatie en correspondentie worden tenminste 2 jaar bewaard.
10.	**Evalueer elk jaar**	De algemeen directeur evalueert jaarlijks in het directieberaad alle datalekken van het afgelopen jaar en rapporteert hierover aan het schoolbestuur.	Bij de evaluatie wordt in ieder geval gekeken of de school datalekken tijdig en correct heeft afgehandeld en of de genomen maatregelen effectief zijn.

[1] Datalek: wel of niet melden | Autoriteit Persoonsgegevens
[2] datalekken.autoriteitpersoonsgegevens.nl