AVG Procedure datalekken

Betreft: **Procedure datalekken Edese Schoolvereniging**
Datum team: **7 mei 2024 - memo intern**
Datum bestuur: **18 maart 2024**
Datum mr: **4 april 2024**

Procedure datalekken Edese Schoolvereniging

Inleiding
Het bestuur heeft op grond van de AVG een registratieplicht en een meldplicht voor datalekken.

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

Beveiligingsincident en datalek

Een school moet onderscheid maken tussen een beveiligingsincident en een datalek. Een *beveiligingsincident* is een inbreuk op de informatiebeveiliging. Een *datalek* is een beveiligingsincident dat (mogelijk) gevolgen heeft voor de privacy van leerlingen, ouders en/of medewerkers. Een datalek is altijd een beveiligingsincident maar een beveiligingsincident is niet altijd een datalek. De volgende datalekken komen het meest voor:

- een e-mail met persoonsgegevens naar de verkeerde ontvanger
- verlies/diefstal van een laptop of het verlies/diefstal 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, e-mailadres, kenteken van een auto of een leerlingnummer).

Registratieplicht datalek

Een school moet alle datalekken documenteren, inclusief de feiten over het datalek, de gevolgen daarvan en de genomen corrigerende maatregelen. Dat geldt ook voor datalekken die een school niet hoeft te melden bij de Autoriteit Persoonsgegevens (AP).

Meldingsplicht datalek

AP

Een school moet een datalek binnen 72 uur na ontdekking bij AP melden, tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van betrokkene(n). Een school moet een datalek ook melden als deze zich voordoet bij een partij die namens de school persoonsgegevens verwerkt (bijvoorbeeld de uitgever van digitale leermiddelen, de leverancier van het leerlingvolgsysteem of het administratiekantoor).

AVG Procedure datalekken

Betrokkene

Een school moet een datalek ook melden aan betrokkene(n) als het lek waarschijnlijk een hoog risico met zich meebrengt voor zijn rechten en vrijheden (bijvoorbeeld ingeval van fraude of identiteitsfraude). De school moet betrokkene(n) in dat geval tevens informeren over mogelijke maatregelen ter beperking van de gevolgen van het datalek. Op basis van het volgende schema kan de school bepalen of betrokkene(n) geïnformeerd moeten worden:

Hoe groot is de impact van het datalek?	Geen gevoelige gegevens gelekt		Wel gevoelige gegevens gelekt	
	Beperkte nadelige gevolgen	Grote nadelige gevolgen	Beperkte nadelige gevolgen	Grote nadelige gevolgen
Kleine kans op nadelige gevolgen	Laag	Gemiddeld	Gemiddeld	Hoog
Grote kans op nadelige gevolgen	Gemiddeld	Hoog	Hoog	Hoog

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 persoons-gegevens 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.	**Meld beveiligings-incident**	Degene die een beveiligings-incident veroorzaakt of constateert meldt dit onmiddellijk aan de directeur.	De melder gaat onmiddellijk naar de directeur of belt op. Als dit niet mogelijk is dan mailt melder beveiligingsincident naar de directeur: directie@esvede.nl of bestuur@esvede.nl
3.	**Analyseer de situatie en vul intake-formulier in**	De directeur analyseert zo snel mogelijk samen met de melder en de ICT'er de situatie. Overleg indien nodig ook met de externe ICT-beheerder.	Als de school **geen** verantwoording verantwoordelijke is dan is deze procedure **niet** van toepassing. Bijv. een leerkracht verliest een USB-stick met de contactgegevens van zijn tennis teamgenoten. Zorg dat u weet wat er is gebeurd en wat de omvang van het lek is. Vul intakeformulier in (zie bijlage 1) en plaats dat in het register beveiligingsincidenten en datalekken (zie bijlage 2). Register staat in Sharepoint.
4.	**Bepaal aanpak**	De directeur bepaalt met met het bestuur wie wat wanneer	Is beveiligingsincident géén datalek? Ga dan naar stap 11.

		gaat doen. Indien nodig overlegt hij met de FG over de aanpak.	Indien nodig wordt een crisisteam ingesteld.
5.	**Beperk de schade en leg genomen maatregelen vast**	De directeur zorgt dat de oorzaak van het beveiligingsincident zo snel mogelijk wordt achterhaald en verholpen.	Bepaal op basis van stappen 3 en 4 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. Denk aan blokkeren accounts of op afstand wissen van een gestolen laptop. De ICT'er legt in 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? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?
6.	**Informeer FG en (indien nodig) systeembeheerder**	De directeur informeert onmiddellijk alle betrokken partijen. Zie ook hierboven bij 4.	Stuur een mail met intakeformulier of met een link naar het datalekregister en bel indien nodig direct na.
7.	**Overleg met FG of beveiligingsincident een datalek is en zo ja, of dit datalek bij AP en aan betrokkenen moet worden gemeld**	De directeur overlegt zo snel mogelijk met de FG. De volgende 4 vragen moeten worden beantwoord: 1. Heeft zich een beveiligingsincident voorgedaan? 2. Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten? Zo ja, dan is het beveiligingsincident een datalek. 3. Zijn er persoons-gegevens van	De FG van de school is Clemens Geenen van PEP Onderwijsadvies: info@peponderwijsadvies.nl 06-21210234 De Guidelines meldplicht datalekken (in het bijzonder hoofdstuk 4) van AP geeft handvatten om te bepalen of een datalek bij AP moet worden gemeld, zie URL hieronder bij[1]. In principe kan er van worden uitgaan dat het lekken van gevoelige gegevens gemeld moet worden bij betrokkene(n). Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld en de gelekte data zijn

		gevoelige aard gelekt of is het waarschijnlijk dat het datalek risico's met zich meebrengt voor de rechten en vrijheden van betrokkene(n)? Zo ja, dan moet datalek bij AP gemeld worden. 4. Bieden de genomen technische beschermings-maatregelen (bijv. cryptografie of remote wipe) voldoende bescherming om te kunnen uitsluiten dat het datalek een hoog risico voor betrokkene(n) inhoudt? Of vergt de mededeling onevenredige inspanningen of zou de melding een onderzoek naar de omstandigheden van een datalek nodeloos hinderen? Zo ja, dan hoeft datalek **niet** aan betrokkene(n) te worden gemeld.	onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkene(n) te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.
8.	**Overleg met schoolbestuur over advies FG**	De directeur overlegt met het bestuur over advies van FG en spreekt af wie wat wanneer gaat doen.	
9.	**Meld datalek bij AP**	Het bestuur, de directeur of de FG meldt het datalek binnen 72 uur bij AP na het ontdekken van het datalek. Bij twijfel doet het bestuur een proforma melding en later een vervolgmelding. Het bestuur kan een melding later altijd weer intrekken.	Het bestuur meldt het datalek via het Meldloket Datalekken van AP: zie hieronder bij[2]. Ten onrechte niet melden kan leiden tot boetes van AP. Als het bestuur het datalek wel meldt bij AP maar betrokkenen niet informeert dan moet het schoolbestuur in de melding bij AP aangeven dat betrokkenen niet worden geïnformeerd inclusief de redenen waarom niet.
10.	**Meld datalek aan betrokkenen**	De directeur zorgt in overleg met het bestuur dat indien nodig betrokkenen geïnformeerd worden over het datalek.	Gebruik voorbeeldbrief (zie bijlage 3). Betrokkenen moeten ook informatie krijgen over mogelijke maatregelen ter beperking van de gevolgen van het datalek.

11.	**Vul het register aan en bewaar alle informatie**	De directeur zorgt dat het register wordt aangevuld en bewaart alle informatie en correspondentie tenminste 2 jaar.	
12.	**Evalueer elk jaar**	De AVG-werkgroep evalueert jaarlijks alle datalekken van het afgelopen jaar. De ICT-coördinator kan hierbij aanwezig zijn. De directeur rapporteert de uitkomsten aan het intern toezicht.	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] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-guidelines
[2] https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?1

Bijlagen:
1. Intakeformulier beveiligingsincident of datalek
2. Format register beveiligingsincidenten en datalekken
3. Voorbeeldbrief aan betrokkenen