Protocol Informatiebeveiligingsincidenten en datalekken
Conform de Algemene Verordening Gegevensbescherming

Inhoud

1. Inleiding

In dit Protocol informatiebeveiligingsincidenten en datalekken wordt aangesloten bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van het Stichting Openbaar Onderwijs Emmen.

Dit protocol biedt een handleiding voor de melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van het Stichting Openbaar Onderwijs Emmen en al haar medewerkers.

Toelichting gebruikte termen:

- **Beveiligingsincident:** een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening:** het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek:** een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene:** de persoon van wie de persoonsgegevens zijn gelekt.

2. Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Dit houdt in dat de onderwijsinstelling verplicht is om (potentiële) datalekken te melden aan de toezichthouder, de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene van wie de gegevens zijn gelekt. Als blijkt dat niet of onvoldoende is voldaan aan deze meldplicht kan de toezichthouder een boete opleggen tot € 20 miljoen of 4% van de jaarlijkse wereldwijde omzet per overtreding.

Voor alle verwerkingen waar Stichting OOE de verwerkingsverantwoordelijke is, is Stichting OOE verantwoordelijk voor de meldingsplicht datalekken vanuit de AVG.

Zo is Stichting OOE verantwoordelijke voor het melden van datalekken van bijvoorbeeld het leerling administratie of digitale leermiddelen. De school maakt gebruik van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school. Met deze verwerkers maakt Stichting OOE aanvullende afspraken over het melden van datalekken in het verwerkersovereenkomsten.

Volgens de AVG is er sprake van een datalek als zich een inbreuk voordoet op de beveiligingsmaatregelen, wat leidt tot het per ongeluk, opzettelijk of onrechtmatig vernietigen, verliezen, aanpassen, ongeautoriseerde openbaring van, of toegang tot, persoonsgegevens die overgedragen, bewaard of op een andere manier verwerkt zijn. Voorbeelden van een datalek zijn het verlies van een mobiel apparaat waarop gevoelige persoonsgegevens staan. Maar ook computer hacking, besmetting met ransomware, of het technische falen van apparatuur, stroomuitval, wateroverlast kunnen leiden tot een datalek. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

Niet ieder datalek-incident valt onder de meldplicht. Er is sprake van een zogeheten geclausuleerde meldplicht voor datalekken.

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de Autoriteit persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de Autoriteit Persoonsgegevens niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

3. Afspraken met leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Spreek af:

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatiegegevens de verwerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de verwerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

4. Procedure Datalekken

4.1 De vier rollen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt (functionaris gegevensbescherming)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming)**; Na akkoord van verwerkingsverantwoordelijke doet de functionaris gegevensbescherming de melding van de datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (security officer/ICT-coördinator)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

4.2 De zeven stappen

1. Ontdekken

De Ontdekker merkt een beveiligingsincident op, via eigen waarneming of via waarneming van een derde. De ontdekker meldt het beveiligingsincident bij de directe leidinggevende (de schoolleider). De Ontdekker samen met de leidinggevende verzamelen zoveel mogelijk informatie (zie hieronder) en meldt het door een e-mail te sturen naar het meldpunt (de Functionaris Gegevensbesherming) via mailadres a.sueters@oo-emmen.nl.

Melding via de e-mail van een beveiligingsincident/ datalek moet onderstaande informatie bevatten:

- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident en wanneer het ontdekt is

- Aard van het beveiligingsincident (inbreuk op vertrouwelijkheid, integriteit of beschikbaarheid van gegevens)
- Welke groep betrokkenen het betreft (leerlingen, ouders, medewerkers)
- Aantal betrokkenen
- Type persoonsgegevens in kwestie en hoeveel
- Zijn er ook andere organisaties betrokken bij het beveiligingsincident/ datalek; worden de gegevens binnen een keten gedeeld
- Zijn er voor het incident maatregelen genomen voor de beveiliging van de persoonsgegevens (zoals bijvoorbeeld het versleutelen van gegevens of ontoegankelijk maken voor onbevoegde)

2. Inventariseren

Het meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus.

3. Beoordelen

Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten en aan de hand van de geldende richtsnoeren van de AP om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.
De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’, hou je rekening mee met de risico van de inbreuk in verband met persoonsgegevens op de rechten en vrijheid van de betrokkenen.

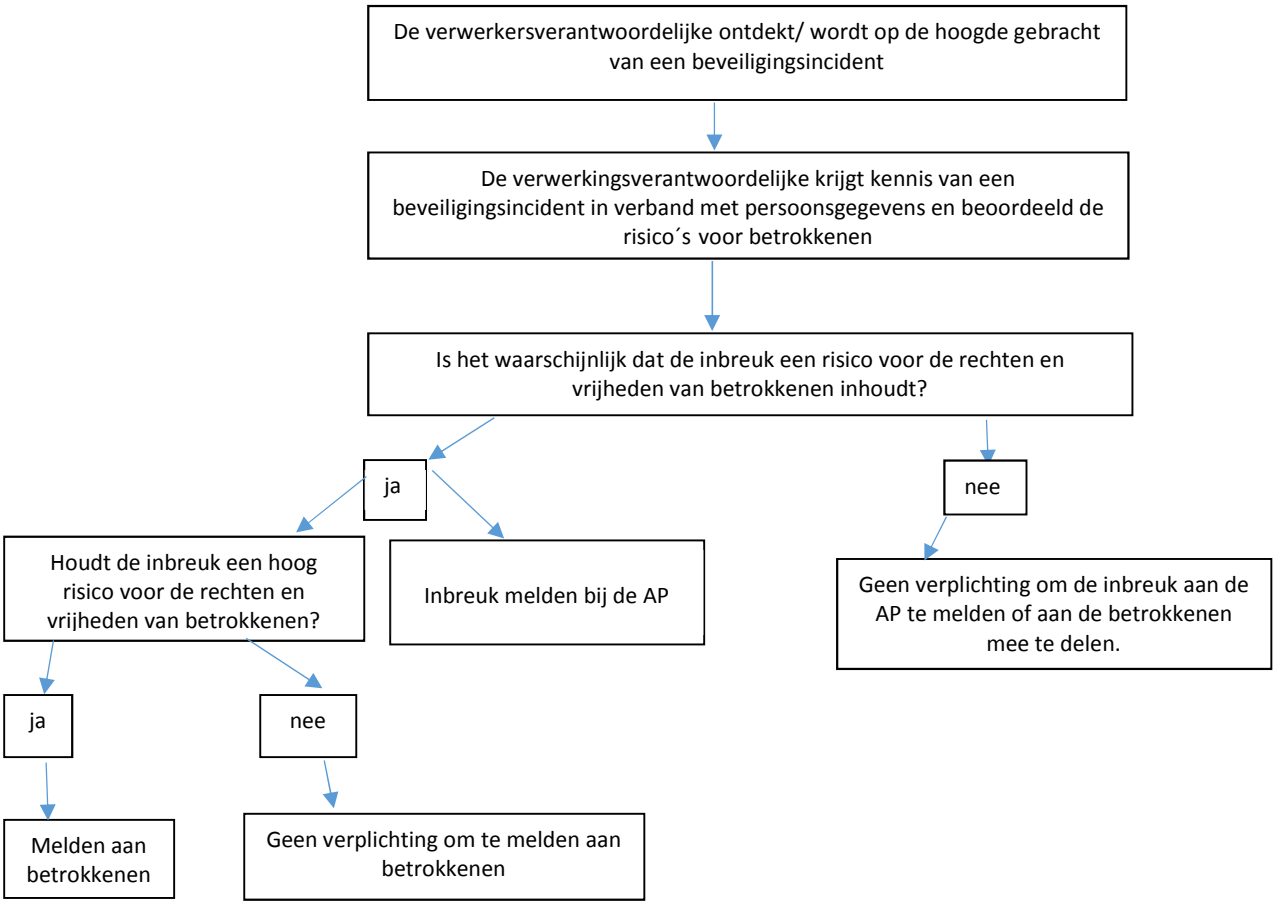
Hoewel de AVG de verplichting invoert om een inbreuk te melden, is dit niet in alle omstandigheden verplicht:
• Een inbreuk moet aan de bevoegde toezichthoudende autoriteit worden gemeld, tenzij het
onwaarschijnlijk is dat ze een risico voor de rechten en vrijheden van natuurlijke personen
inhoudt.
• Een inbreuk wordt alleen aan de persoon meegedeeld als het waarschijnlijk is dat ze een hoog risico voor de rechten en vrijheden inhoudt.

Dit betekent dat het van essentieel belang is dat de verwerkingsverantwoordelijke onmiddellijk nadat hij kennis heeft gekregen van een inbreuk niet alleen tracht het incident onder controle te krijgen, maar ook het risico inschat dat eruit kan voortvloeien. Daar zijn twee belangrijke redenen voor: in de eerste plaats zal kennis van de waarschijnlijkheid en de potentiële ernst van het effect op de persoon de verwerkingsverantwoordelijke helpen om doeltreffende maatregelen te nemen teneinde de inbreuk in te dammen en aan te pakken; in de tweede plaats zal het de verwerkingsverantwoordelijke helpen bepalen of een melding aan de toezichthoudende autoriteit en, indien nodig, een mededeling aan de betrokken personen vereist is.

De belangrijkste aanleiding op grond waarvan een inbreuk aan betrokkenen moet worden meegedeeld, is als het waarschijnlijk is dat de inbreuk een hoog risico voor de rechten en vrijheden van natuurlijke personen met zich meebrengt. Dit risico bestaat

als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen wier gegevens het voorwerp van de inbreuk zijn.

De onderstaande beslisboom kan hiervoor gebruikt worden:



4. Repareren

De **ICT-afdeling,** in geval van een incident op IT gebied, zal worden gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen.
De **ICT-afdeling** legt 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)?

Als het beveiligingsincident resulteert door het niet naleven van de privacy gerelateerde werkprocessen, dan is de schoolleider verantwoordelijk voor het achterhalen van de oorzaak van het beveiligingsincident en daarop actie te ondernemen.

5. Melden bij de Autoriteit Persoonsgegevens

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de melder dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken. https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1 Het lege meldingsformulier is openbaar. Neem eens een kijkje welke informatie er eigenlijk nodig is om een datalek te melden. Dan ben je voorbereid als dat ooit nodig mocht zijn.

Afhankelijk van de aard van de inbreuk kan nader onderzoek door de verwerkingsverantwoordelijke nodig zijn om alle relevante feiten met betrekking tot het incident vast te stellen. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

Artikel 34(3) van de AVG stelt drie voorwaarden waaronder geen melding aan betrokkenen vereist is. Dit geldt in de volgende situaties:

1. Er zijn passende technische en organisatorische maatregelen getroffen ter bescherming van de persoonsgegevens en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk betrekking heeft. Met name maatregelen die ervoor zorgen dat de data niet toegankelijk is voor ongeautoriseerde personen. Bijvoorbeeld door encryptie of anonimiseren.
2. Direct na een datalek zijn er acties ondernomen om ervoor te zorgen dat er geen hoog risico meer is op schade aan de persoonlijke levenssfeer van betrokkenen.
3. Het zou onevenredige inspanningen vergen om contact op te nemen met de betrokken individuen, bijvoorbeeld wanneer de contactgegevens van betrokkenen verloren zijn. In dit geval zal er gekozen moeten worden voor een openbare communicatie uiting of een vergelijkbare maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd .

Termijn van melden

Voor het melden van een datalek aan betrokkenen geldt dat dit ‘onverwijld’ moet gebeuren. Uitgangspunt is dat onnodige vertraging wordt voorkomen, zodat de betrokkene de nodige maatregelen kan treffen. Gelet hierop dient een datalek binnen 72 uur te worden gemeld aan de toezichthouder. De wijze waarop betrokkenen worden geïnformeerd, bepaalt de verantwoordelijke zelf.

6. Informeren betrokkene:

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

De verwerkingsverantwoordelijke ten minste de volgende informatie te verstrekken aan de betrokkene:

• een beschrijving van de aard van de inbreuk;

• de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander
contactpunt;
• een beschrijving van de waarschijnlijke gevolgen van de inbreuk;
• een beschrijving van de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk aan te pakken, met inbegrip van, in voorkomend geval, maatregelen om de mogelijke nadelige gevolgen ervan te beperken.

De verwerkingsverantwoordelijke dient indien passend ook specifiek advies te geven aan personen om zich te beschermen tegen mogelijke negatieve gevolgen van de inbreuk, zoals het wijzigen van wachtwoorden indien hun toegangsgegevens in het bezit zijn gekomen van derden.

7. Vastleggen

Alle informatie en documenten, die in de voorafgaande stappen is ingewonnen of ontstaan (inclusief het digitale formulier van de Autoriteit Persoonsgegevens), wordt gearchiveerd door het meldpunt waarmee het incident is afgesloten. Het meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

Alle beveiligingsincidenten en datalekken (ook datalekken die niet leiden tot een melding bij de Autoriteit persoonsgegevens), dienen vastgelegd te worden in een incidentenregister.

5. Monitoring beveiligingsincidenten en datalekken

Het meldpunt van het Stichting Openbaar Onderwijs Emmen maakt twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de functionaris gegevensbescherming.

In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen. Er wordt per oorzaak van elk incident bepaald of op de korte of langere termijn maatregelen nodig zijn (op moment dat de datalek zich voordoet).

Het schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.