PROTOCOL meldplicht datalekken

OPENBAAR VOORTGEZET ONDERWIJS ZAANSTAD

Datum:	13 mei 2022
Opsteller:	Jan Zonneveld (versie 2017), Rob Binda (versie 2022)
Expertise:	Informatiemanagement
Besluitvorming:	Vastgesteld door College van Bestuur op 24 mei 2022
Revisiedatum:	13 mei 2024

Inhoud

1. Inleiding

Het Protocol meldplicht datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van Stichting OVO Zaanstad. Het protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken.

Iedere medewerker die direct of indirect kennis draagt of krijgt van een incident inzake het lekken van privacygegevens, is verplicht dit direct te melden aan de privacy-medewerker op school en/of aan de FG. Het Formulier melding beveiligingsincident is bijgevoegd.

Dit protocol is van toepassing op de gehele organisatie van Stichting **OVO Zaanstad.**

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die er voor 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.
- **Privacy medewerker**: de medewerker op school dan wel bij OVO Service die eerste aanspreekpunt is voor en toezicht houdt op naleving en implementatie van het IBP-beleid van OVO Zaanstad
- **Functionaris Gegevensbescherming**: Iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG). En beoordeelt of een beveiligingsincident een datalek is en gemeld dient te worden bij de Autoriteit Persoonsgegevens. .

2. Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplichting 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. Bijvoorbeeld in de leerling administratie of digitale leermiddelen van de scholen van OVO Zaanstad. Als een school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan worden met deze verwerkers aanvullende afspraken over het melden van datalekken gemaakt. Binnen OVO Zaanstad is afgesproken dat alle contracten op het gebied van ICT-hardware, ICT-contracten en –licenties, (beheer van) technologische infrastructuur en digitale middelen in brede zin die het onderwijs op een school ondersteunen worden getekend door het CvB en worden voorbereid door OVO Service.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie 'gelekt'. 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.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.
De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een verwerker voor de school. Er kan worden afgesproken dat een verwerker **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

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. De afspraken betreffen:

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

OVO Zaanstad maakt schriftelijke afspraken met verwerker(s) over datalekken. Hiervoor wordt gebruik gemaakt van de model verwerkersovereenkomst die hoort bij het convenant "Digitale onderwijsmiddelen en privacy" (www.privacyconvenant.nl).

4. Werkwijze

a. Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een gedragscode gebruik internet, intranet, email en sociale media.

b. 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 (privacy medewerker van een school en/of OVO Service);** waar alle beveiligingsincidenten van de school naar toegestuurd worden, geregistreerd worden en volgens protocol verder worden verwerkt.
3. **Melder (Functionaris Gegevensbescherming OVO Zaanstad)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (netwerkbeheerder/ICT medewerker)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

c. De zeven stappen

1. **Ontdekken**

   De ontdekker merkt een beveiligingsincident op via eigen waarneming of via waarneming van een derde en meldt het bij de privacy medewerker, de bovenschools privacy-officer of rechtstreeks aan de Functionaris Gegevensbescherming.

   De privacy medewerker verzamelt zoveel mogelijk informatie over het beveiligingsincident. De privacy medewerker geeft de melding per ommegaande, en uiterlijk binnen 24 uur telefonisch door aan de Functionaris Gegevensbescherming van OVO Service, vult het Formulier melding beveiligingsincidenten OVO Zaanstad in en stuurt dit formulier inclusief alle verzamelde informatie naar de Functionaris Gegevensbescherming. Deze heeft vervolgens de regie over de melding.

2. **Inventariseren**

   De Functionaris Gegevensbescherming bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij/zij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt vastgelegd:

   - 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);
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen (leerlingen, ouders, medewerkers);
     - Aantal betrokkenen;
     - Type persoonsgegevens in kwestie
     - Hoeveel persoonsgegevens in kwestie;
     - Worden de gegevens binnen een keten gedeeld (zijn er ook andere organisaties betrokken bij het beveiligingsincident/datalek) en zo ja met welke partijen;
     - Zijn er na ontdekking van het incident maatregelen genomen voor de beveiliging van de persoonsgegevens (zoals bijvoorbeeld het versleutelen ontoegankelijk maken voor onbevoegde)

3. **Beoordelen**

   Wanneer de Functionaris Gegevensbescherming voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Ontdekker een verzoek om de verzamelde informatie te bekijken. De Ontdekker beoordeelt de feiten en geeft de Functionaris Gegevensbescherming een terugkoppeling.

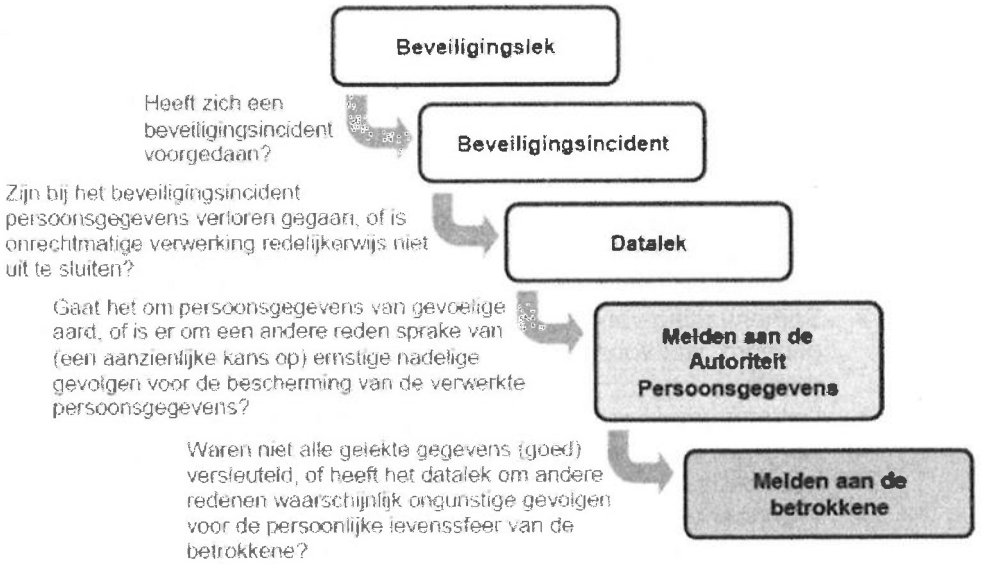
   Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek' aan de Autoriteit Persoonsgegevens houdt de Functionaris Gegevensbescherming rekening met het type gegevens en met de hoeveelheid gegevens.

   Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden.

   Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens "gevoelig" zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid,

over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak andere kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom kan gebruikt worden als leidraad:



De volgende informatie wordt vastgelegd door de Functionaris Gegevensbescherming:

- 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?

4. Repareren

De Technicus (netwerkbeheerder/ICT medewerker); wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De Technicus legt onderstaande vast:

- Technische, organisatorische en juridische maatregelen[1] die genomen zijn (door hem of anderen) 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)?

5. Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Functionaris Gegevensbescherming dit binnen 72 uur doen. Bij deze afweging wordt het College van Bestuur van OVO Zaanstad betrokken.

[1] Een overzicht van technische, organisatorische en juridische maatregelen zijn in de bijlage opgenomen.

De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek dient gemeld te worden bij het meldloket datalekken:
https://datalekken.autoriteitpersoonsgegevens.nl/

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de Functionaris Gegevensbescherming waarmee het incident is afgesloten.

   Het datalek wordt geregistreerd in het Datalekregister van OVO Zaanstad door de Functionaris Gegevensbescherming.

   De Functionaris Gegevensbescherming verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

7. **Informeren betrokkene: leerling en/of zijn ouders**
   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 er van worden uitgaan dat het lekken van persoonsgegevens van gevoelige aard 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 toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden. Dit dient per geval beoordeeld te worden. Betrokkene(n) kunnen bij de betrokken privacy medewerker/officer vragen stellen over de voortgang en zullen daarnaast ook proactief geïnformeerd worden.

5. Monitoring beveiligingsincidenten en datalekken

De Functionaris Gegevensbescherming van OVO Zaanstad maakt jaarlijks een analyse van de meldingen van beveiligingsincidenten en datalekken; de privacy medewerkers en de bovenschools privacy-officer kunnen geconsulteerd worden.

In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Het CvB wordt geïnformeerd over de uitkomsten van de analyse.

Bijlage 1 Persoonsgegevens

Een school verwerkt persoonsgegevens van leerlingen, ouders, medewerkers, leveranciers en andere relaties. De volgende categorieën persoonsgegevens worden door de Autoriteit Persoonsgegevens onderscheiden:

1. **Persoonsgegevens:**
   - NAW-gegevens;
   - Mailadres en IP adres;
   - Telefoonnummer;
   - BSN-nummer;
   - geboortedatum.

2. **Bijzondere persoonsgegevens:**
   De school mag deze niet gebruiken, tenzij daarvoor in de wet een uitzondering is vastgelegd of één van de zes grondslagen in de AVG van toepassing is
   - raciale of etnische afkomst;
   - politieke opvattingen;
   - religieuze of levensbeschouwelijke overtuiging;
   - lidmaatschap van een vakvereniging;
   - iemands gezondheid;
   - iemands seksuele gedrag of seksuele gerichtheid;
   - genetische gegevens;
   - biometrische gegevens met het oog op de unieke identificatie van een persoon.

3. **Strafrechtelijke gegevens:**
   De school mag deze niet gebruiken.

4. **Persoonsgegevens van gevoelige aard:**
   De school mag deze gebruiken, maar moet deze extra goed beveiligen gezien het risico en de impact van het verliezen van dit soort gegevens voor de personen in kwestie:
   - Financiële situatie, bijvoorbeeld:
     - (problematische) schulden;
     - salarisgegevens (ook loonschaal);
     - betalingsgegevens.
   - Economische situatie, bijvoorbeeld:
     - Werkeloosheid.
   - Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, bijvoorbeeld:
     - (gok)verslaving;
     - prestaties op school;
     - prestaties op het werk;
     - relatieproblemen.
   - Sociale problematiek, bijvoorbeeld:
     - armoede;
     - huiselijk geweld;
     - betrokkenheid van jeugdzorg of maatschappelijk werk.
   - Inloggegevens, bijvoorbeeld:
     - gebruikersnamen en wachtwoorden.
   - Kopie identificatiebewijs, bijvoorbeeld :
     - paspoort;
     - ID-bewijs.