



**onderwijs**professionals

---

## Procedure datalek

---

Naam auteur : Daniel Hoopman  
Versie datum : 21 september 2018

---

**Onderwijs Professionals BV**

Nicolaes Maesstraat 2 - 216, 1506 LB Zaandam  
075-6143561

info@onderwijs-professionals.nl  
www.onderwijs-professionals.nl

NL68 INGB 0005706664, BIC INGBNL2A  
KvK Amsterdam 34309851, BTW NL8198.27.721.B01



*Onderwijs Professionals respecteert uw privacy en al uw gegevens worden vertrouwelijk behandeld. De verwerking van persoonsgegevens geschiedt altijd op een manier die in overeenstemming is met de eisen die de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679, hierna AVG) en eventuele andere wet- en regelgeving daaraan stelt. In deze Procedure Datalek wordt in meer detail uiteengezet hoe Onderwijs Professionals in onverhoopt geval met het verlies van dergelijke gegevens omgaat.*

Dit document beschrijft de verschillende stappen die binnen OP genomen worden bij een datalek, die valt onder de Meldplicht Datalekken. De Meldplicht Datalekken is een wijziging van de Wet Bescherming Persoonsgegevens en is met ingang van 1 januari 2016 in werking getreden. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 13 van WBP). De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking. Een datalek moet - onder bepaalde voorwaarden - onverwijld (binnen 2 dagen) nadat de verantwoordelijke persoon binnen OP er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens (voorheen CBP) gemeld worden en - onder diezelfde voorwaarden - ook door de verwerkingsverantwoordelijke worden gemeld bij de betrokkenen. In het geval van OP zijn dit over het algemeen klanten (ouders, kinderen, gemeente en/of scholen) of medewerkers. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer.

1. **Verwerkingsverantwoordelijke (Onderwijs Professionals)**- De Verwerkingsverantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk (functioneel) degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft en verantwoordelijk is over doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De Verwerkingsverantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten), zoals staat beschreven in de Algemene Verordening Gegevensbescherming (Verordening EU 2016/679) (hierna: "AVG"). Onderwijs Professionals is verwerkingsverantwoordelijke voor de verslagen van onderzoek en behandeling die zij zelf opstelt en bewaard.
2. **Verwerker (leveranciers)** - De organisatie die de gegevens ten behoeve van de Verwerkingsverantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen. De Verwerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de Verwerkingsverantwoordelijke. De Verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens, zoals tevens staat beschreven in de tussen Verwerkingsverantwoordelijke en Verwerker overeengekomen Bewerkerovereenkomst. De organisaties die software aan Onderwijs Professionals leveren waarmee Onderwijs Professionals haar diensten kan verlenen zijn verwerker in de zin van de wet.



Mogelijke oorzaken van een datalek:

- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, malware);
- technisch falen (fouten of bugs in software, verlate updates, storingen);
- menselijk falen (onzorgvuldige omgang gebruikersnaam of wachtwoord, nalatigheid);
- verloren of gestolen hardware (externe harde schijf, USB stick, server-apparatuur of laptop);
- verzenden e-mail naar meerdere gebruikers met openbaring van e-mailadressen;
- calamiteit (brand datacentrum, wateroverlast).

## Melding

Alle datalekken van persoonsgegevens moeten intern worden gemeld en worden gedocumenteerd door de Functionaris Gegevensbescherming (FG). De melding kan door iedere gebruiker en iedere medewerker of derde partij worden gedaan. De melding kan ook door een externe persoon worden gedaan bij een medewerker van OP. De melding moet direct en telefonisch worden gedaan bij de FG en schriftelijk worden vastgelegd. Deze meldt het datalek zo nodig bij de Autoriteit Persoonsgegevens.

De Functionaris Gegevensbescherming legt vast:

- naam van de melder;
- de contactpersoon voor de melding;
- datum en tijd van de melding;
- aard van de inbreuk en risico op verlies of onrechtmatig gebruik gegevens;
- welke persoonsgegevens vallen onder de melding;
- om welk aantal gegevensrecords gaat het;
- welke (groepen) personen zijn betrokken bij de melding;
- welke maatregelen zijn of worden door de melder getroffen;
- welke gevolgen zijn er volgens de melder voor de betrokkenen.

## Escalatie bij afwezigheid

Bij afwezigheid van de Functionaris Gegevensbescherming wordt diens rol ingevuld door de backoffice van OP. Buiten kantoor tijden en in het weekend wordt de melding gedaan bij de FG.

## Analyse

De Functionaris Gegevensbescherming beoordeelt of van de inbreuk 'redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden'. Is dit niet het geval, dan vindt alleen registratie van de melding plaats door de FG en hoeven geen meldingen gedaan te worden aan de autoriteit persoonsgegevens en de betrokkenen.



Is dit aanmerkelijke risico wel aanwezig, dan voert de FG de acties uit zoals beschreven in het Calamiteitenplan van OP:

1. Telefonisch informeren teamleden OP Diagnostiek;
2. Tijdens kantooruren onmiddellijk bijeenroepen van het Responseteam Datalek, bestaande uit:
  - a. **Functionaris Gegevensbescherming (FG)** - Daniel Hoopman
  - b. **Teamleden Onderwijs Professionals Diagnostiek;** Laura Voetman en Rinske Hoopman

Als het mogelijk is, wordt een eventueel benodigd overleg uitgesteld tot tijdens kantooruren. Als dit niet mogelijk is, wordt zoveel als mogelijk telefonisch en elektronisch overleg gevoerd.

## Responseteam Datalek

Het Responseteam Datalek wordt met hoge prioriteit bijeengeroepen door de FG. De bijeenkomst wordt voorgezeten door de FG. Het responseteam communiceert en neemt besluiten over de volgende zaken;

- De gegevens die door de FG zijn vastgelegd bij het aannemen van de melding;
- De noodzakelijke vervolgacties met betrekking tot het datalek (lek dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer);
- De melding die opgesteld moet worden voor de Autoriteit Persoonsgegevens door de FG. Naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records:
  - o De mogelijke gevolgen voor de betrokkenen;
  - o De maatregelen die OP neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
  - o De maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;
  - o Contactgegevens voor betrokkenen.
- De wijze van afhandeling intern, inclusief communicatie naar melder, betreffende afdeling(-en) en manager(s);
- Of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd), of een onrechtmatige daad;
- Of het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit OP zelf, een klant, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregelheden te voorkomen. Indien gewenst vindt overleg plaats met de Privacy Officer;
- Wat er intern wordt gecommuniceerd over het incident;
- Wat er extern wordt gecommuniceerd over het incident en vaststellen of de pers geïnformeerd moet worden;
- Of naast de Autoriteit Persoonsgegevens ook andere stakeholders geïnformeerd moeten worden;
- Of er individuen, klanten, leveranciers geïnformeerd moeten worden;
- Op welke wijze er intern wordt gerapporteerd;
- Of eventuele schade is gedekt door de verzekeringspolis.

## **Melding bij de Autoriteit Persoonsgegevens**

De FG meldt binnen 2 dagen volgens de aangewezen methode het datalek via het Meldpunt Datalek van de Autoriteit Persoonsgegevens (<https://datalekken.autoriteitpersoonsgegevens.nl/>). In ieder geval zal gemeld moeten worden:

- Aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, beschrijving gegevens;
- Beschrijving van de te verwachten gevolgen;
- Getroffen en/of voorgestelde maatregelen;
- Informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- Contactgegevens voor betrokkene;

## **Ontvangstbevestiging Autoriteit Persoonsgegevens**

Is er een melding gedaan, dan ontvangt OP een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door de Autoriteit Persoonsgegevens, zal de Autoriteit Persoonsgegevens contact opnemen met OP om de herkomst van de melding te verifiëren.

## **Terugkoppeling betrokken**

Na de melding bij de Autoriteit Persoonsgegevens en eventuele getroffen maatregelen zal terugkoppeling plaatsvinden bij de betrokkenen. Hierna zal het incident worden afgesloten en zullen de getroffen maatregelen worden geëvalueerd binnen de PDCA-cyclus van het Risico Management Programma.