Protocol informatiebeveiligingsincidenten en datalekken

PROOLeiden/OBSG Leiderdorp

Bewerkt door:

Versie	Status	Datum	Auteur	Omschrijving
1.0	concept	Mei 2018	M. van Velsen	Ter bespreking in BOD

Vastgesteld door:

Versie	Datum	Naam	Functie
		M. de Pinth	Directeur-bestuurder

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van PROOLeiden/OBSG Leiderdorp

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

Dit protocol is van toepassing op de gehele organisatie van PROOLeiden/OBSG Leiderdorp, zoals vermeld in het IBP beleid.

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. Onder de AVG blijft de meldplicht bestaan, echter wel met strengere eisen aan de registratie van datalekken.

Bij een datalek gaat het om toegang tot of vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens, en verlies van (toegang tot) persoonsgegevens. 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.

De term ‘datalek’ komt niet voor in de wet. In de plaats daarvan heeft de AVG het over een ‘inbreuk in verband met persoonsgegevens’. Hiervan is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (Artikel 4, punt 12, AVG).

Er zijn drie categorieën datalekken te onderscheiden:

1. Inbreuk op de vertrouwelijkheid Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
2. Inbreuk op de integriteit Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
3. Inbreuk op de beschikbaarheid Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

Een datalek kan, afhankelijk van de omstandigheden, in meer dan één van de bovenstaande categorieën vallen.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het bestuur van PROOLeiden/OBSG Leiderdorp. Een leverancier is een verwerker van persoonsgegevens voor de school. Er kan worden afgesproken dat een vewerker **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur.

Als er een datalek is, moet daar **binnen 72 uur** na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

Een datalek hoeft alleen te worden gemeld als dit leidt tot een risico voor de rechten en vrijheden van betrokkenen.

Guidelines
De Guidelines on Personal data breach notification under Regulation 2016/679 van de Europese privacytoezichthouders, en dan met name hoofdstuk IV, geven richtlijnen of het datalek moet worden gemeld.

Werkwijze

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 (meldpuntdatalekken@prooleiden.nl)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. Bestuurssecretaris en/of hoofd ICT beheren het meldpunt.
3. **Melder (bestuurssecretaris, hoofd ICT)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (hoofd ICT, ict-dcoördinator, applicatiebeheerder)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De zeven stappen

1. **Ontdekken**
   De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt via **meldpuntdatalekken@prooleiden.nl**

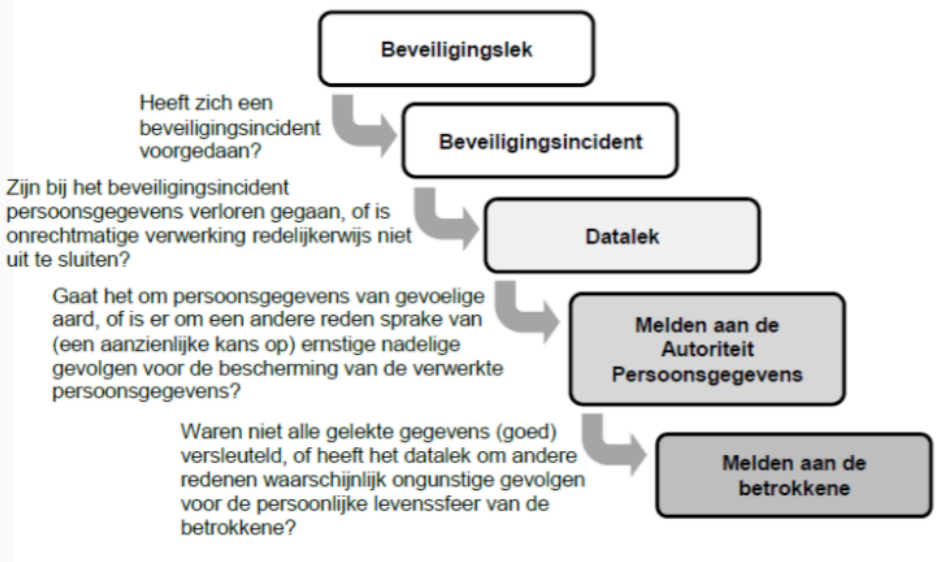
2. **Inventariseren**
   Het Meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:
   - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen
     - Type persoonsgegevens in kwestie
     - Worden de gegevens binnen een keten gedeeld

3. **Beoordelen**
   Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoedt, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten 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', houd je 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 kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom kan gebruikt worden



4. Repareren

De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus 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)?

5. Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij het meldloket datalekken van 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/actionpage?0.

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd in Sharepoint in het **register beveiligingsincidenten** door het Meldpunt waarmee het incident is afgesloten. Het Meldpunt 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 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 toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van PROOLeiden/OBSG Leiderdorp 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.

De directeur-bestuurder wordt geïnformeerd over de uitkomsten van de analyse.

Communicatie

De bestuurssecretaris coördineert eventuele communicatie, intern en extern bij beveiligingsincidenten en datalekken, in afstemming met schooldirecteur en direur-bestuurder. Indien nodig zal de externe woordvoerder van PROOLeiden/OBSG Leiderdorp worden ingeschakeld.