Protocol informatiebeveiligingsincidenten en datalekken

Vereniging Christelijk Voortgezet Onderwijs te Rotterdam en omgeving (CVO)

Bewerkt door:
De Vereniging Christelijk Voortgezet Onderwijs te Rotterdam en omgeving, projectgroep IBP

Versie	Status	Datum	Auteur	Omschrijving
1.0	Definitief	25-05-2018	T. Mout	

Vastgesteld door CVO:

Versie	Datum	Naam	Functie
1.0	25-05-2018	dhr. drs. H.H. Post	Voorzitter raad van bestuur

Inhoud

1. Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het privacy beleid van CVO. Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken. Dit protocol is van toepassing op de gehele organisatie van CVO en al haar medewerkers.

Het protocol bestaat uit vijf onderdelen. Het eerste deel geeft uitleg over de wet- en regelgeving bij datalekken. Het tweede deel gaat over de afspraken met leveranciers m.b.t. persoonsgegevens. Het derde deel geeft de werkwijze aan bij een datalek. Het vierde deel gaat over het analyseren en monitoring van beveiligingsincidenten en datalekken. Het vijfde en laatste deel gaat over de communicatie bij een datalek.

Gebruikte termen:

- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.
- **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.
- **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. Hierbij moet niet alleen gedacht worden aan digitale dragers, maar ook aan andere dragers van persoonsgegevens.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Meldplicht datalekken;** De meldplicht datalekken houdt in dat CVO direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

2. Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht 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 leerlingenadministratie of digitale leermiddelen. Als de school gebruik maakt van leveranciers die persoonsgegevens ontvangen van de school (zoals uitgevers of distributeurs), dan moet de school met deze bewerkers aanvullende afspraken maken over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf wanneer het niet uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is dan 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.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is binnen CVO de raad van bestuur. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker namens de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van de raad van bestuur. Wanneer geen afspraken zijn vastgelegd, moet de verantwoordelijke zelf de melding doen.

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

3. Afspraken met leveranciers

De raad van bestuur van CVO moet als eindverantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers wanneer deze persoonsgegevens van CVO ontvangen. Afspraken over hoe te handelen in geval van datalekken vallen daar ook onder. Voor het schriftelijk vastleggen van afspraken kan gebruik worden gemaakt van de model bewerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (http://www.privacyconvenant.nl/).
Hierbij moeten de volgende zaken worden vastgelegd:

- De wijze waarop je elkaar informeert over datalekken en hoe je de bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties hebt georganiseerd.
- Wie de melding doet bij de Autoriteit Persoonsgegevens.
- Welke informatiegegevens de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding en de wijze waarop je elkaar hiervan op de hoogte houdt (maak bv afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de bewerkers de gegevens i.v.m. een datalek moeten aanleveren.
- Wie verantwoordelijk is voor de communicatie met de gebruikers als dat nodig is.

4. Werkwijze

a. Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en/of gedragscode ICT en internetgebruik.

b. De vier rollen

Er zijn in het algemeen vier rollen te onderscheiden bij de afhandeling van een beveiligingsincident en/of datalek. Het gaat hierbij om de volgende rollen:

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (functioneel-/technisch beheerder)**; 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. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt via: datalek@cvo.nl

2. **Inventariseren**
   Het Meldpunt bepaalt vervolgens 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
    - Of de gegevens binnen een keten gedeeld worden

3. Beoordelen

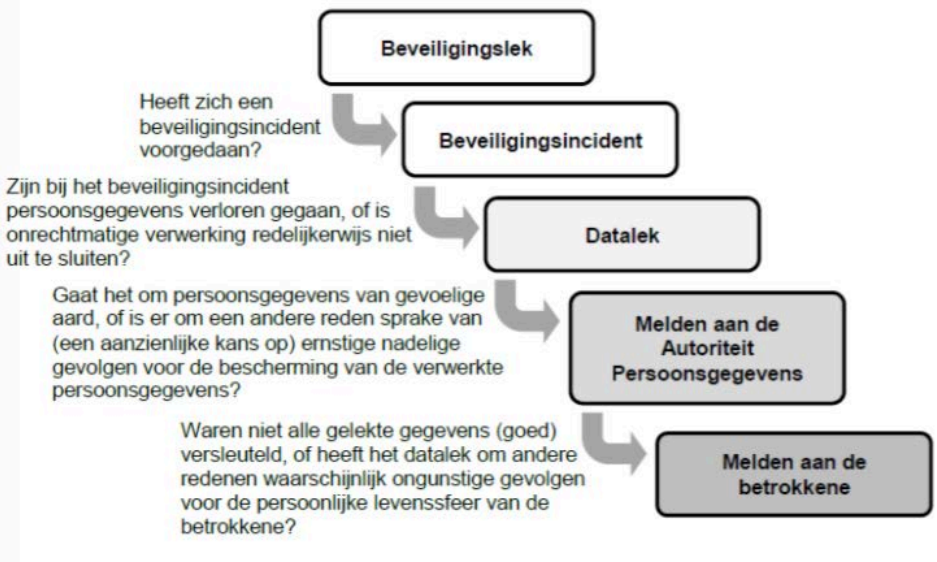
Wanneer het Meldpunt voldoende informatie heeft verzameld en een datalek vermoedt, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkenen vereist is.
De volgende informatie 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', wordt rekening gehouden 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 een melding gedaan worden.

Van ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn. Dit geldt 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 hierbij worden gebruikt.



4. **Repareren**
   Bij een ICT gerelateerd datalek wordt aan De Technicus gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is. Hij moet vervolgens de oorzaak (laten) verhelpen. De technicus van CVO legt onderstaande vast:
   - Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voor zover de oorzaak bekend is. Indien dit niet direct is vast te stellen volgt nader onderzoek.
   - Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen.

5. **Melden**
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkene(n)), dan moet 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 van de Autoriteit Persoonsgegevens.

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

7. **Informeren betrokkenen: medewerkers, leerling en/of ouders.**
   Indien het datalek waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n), dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders/verzorgers als zij jonger zijn dan 16 jaar). In principe kan er van worden uitgaan dat het lekken van gevoelige ‘aard’ gemeld moet worden bij de betrokkenen.

   Let op: als er persoonsgegevens zijn gelekt 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.

5. Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van CVO 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 raad van bestuur wordt geïnformeerd over de uitkomsten van de analyse.

6. Communicatie

Communicatie bij een mogelijk datalek zal verlopen volgens het CVO persprotocol. Dit protocol is te vinden op het CVO intranet. Indien de aard van het datalek risico geeft op imagoschade voor CVO, kan ervoor worden gekozen een externe expert in te huren.