Protocol informatiebeveiligingsincidenten en datalekken

Stichting Scala College en Coenecoop College

Versie Scala College

Na instemming van de GMR vastgesteld door het college van bestuur op 6 juni 2019

F.J. de Wit

Instemming GMR 05-06-2019
Revisie 02-02-2022

Inhoud

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van Stichting Scala College en Coenecoop College.
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.

Deze versie van het protocol is van toepassing op het Scala College.

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 (mogelijk) zijn gelekt.

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. Bovendien is sinds 25 mei 2018 de Algemene Verordening Gegevensbescherming van kracht, waarin de meldplicht onverkort is gehandhaafd. Het niet voldoen aan de meldingsplicht kan leiden tot een fikse boete, maar ook tot schade aan de reputatie van de school.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Persoonsgegevens worden onder meer verwerkt in de leerlingadministratie, in de personeelsadministratie of bij het gebruik van digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school of persoonsgegevens verwerken namens de school, dan zijn deze leveranciers zogeheten “verwerkers”. Stichting Scala College en Coenecoop College maakt met deze verwerkers aanvullende afspraken in verwerkersovereenkomsten; ook over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten dat derden ongeoorloofd toegang hebben gekregen tot de persoonsgegevens. M.a.w.: 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 leerlingen is bijvoorbeeld ook een datalek.

De meldplicht geldt voor de verwerkingsverantwoordelijke voor de persoonsgegevens, dat is namens Stichting Scala College en Coenecoop College het college van bestuur (als bevoegd gezag). Er kan worden afgesproken dat een verwerker **namens** Stichting Scala College en Coenecoop College de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het college van bestuur van Stichting Scala College en Coenecoop College. Zie ook hierna.

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

Afspraken met leveranciers (verwerkers)

Het college van bestuur maakt als verwerkingsverantwoordelijke voor de persoonsgegevens afspraken maken met verwerkers. (Zie hiervoor). Afspraken over datalekken horen daar ook bij en met deze afspraken worden in elk geval de volgende vragen beantwoord:

- 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 informatie/gegevens moet de verwerker geven bij een datalek.
- Welke informatie is nodig 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.

De afspraken die Stichting Scala College en Coenecoop College met een verwerker maakt worden vastgelegd in een verwerkersovereenkomst. Daarbij wordt zoveel mogelijk gebruik worden gemaakt van de model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

Werkwijze

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.

De vier rollen binnen het Scala College

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 (Servicedesk ICT)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. Bij het Scala College is dat de Servicedesk ICT.
3. **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Medewerker Servicedesk ICT (systeem- of netwerkbeheerder);** degene die de oorzaak van het datalek kan vinden en kan (laten) verhelpen.

De acht stappen bij het Scala College

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 incident direct, ook buiten schooltijd:

A) Telefonisch aan de vestigingsdirecteur of een van de andere leden van het managementteam. En **tevens**:
B) Per e-mail: datalekken@scalacollege.nl
De melding wordt gedaan via telefoon en e-mail, om er zeker van te zijn dat de melding z.s.m. op de juiste plaats belandt. De ontvanger van de melding overlegt direct met het hoofd Systeembeheer, Gerben Westerveld, bereikbaar op 06 477 63 684.

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 relevante andere partijen, zoals een leverancier (verwerker). 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.

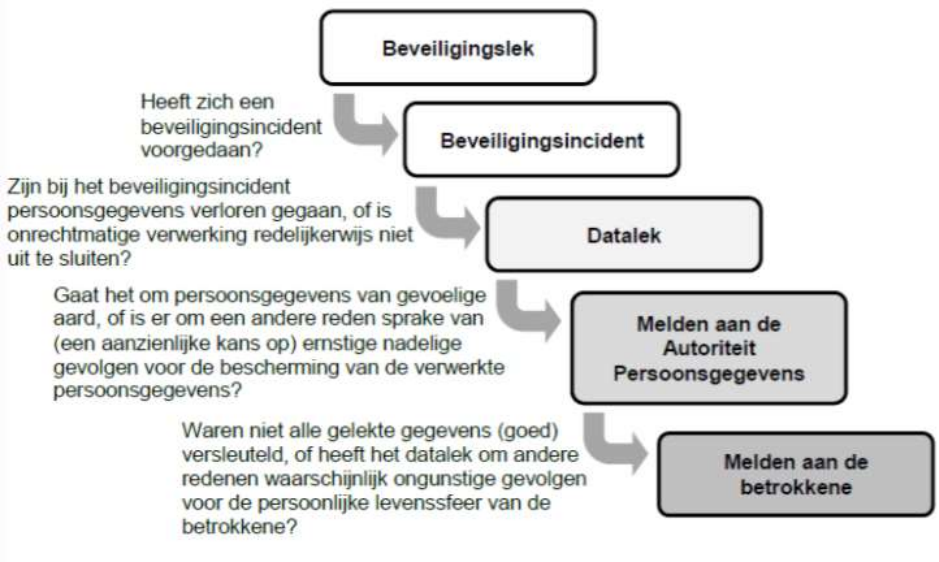
3. Beoordelen

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? (Zie ook onder 7.)
- 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, dan moet er gemeld worden aan de Autoriteit Persoonsgegevens.
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.

De onderstaande beslisboom kan gebruikt worden:



4. **Oorzaak verhelpen**
   De Medewerker Servicedesk ICT van het Scala College wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De Medewerker ICT van het Scala College 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 de Autoriteit Persoonsgegevens (en eventueel ook bij betrokkenen; zie onder 7.), 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 door het Meldpunt in een incidentenregister (zie hierna onder 8.). 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 persoonsgegevens 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 daardoor 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.

8. **Opslag in Register beveiligingsincidenten en datalekken**
   Alle beveiligingsincidenten en datalekken worden opgeslagen in het Register beveiligingsincidenten en datalekken. Dit wordt beheerd door het Meldpunt (de Servicedesk ICT), in een incidentenregister. Alle in het register opgeslagen beveiligingsincidenten en datalekken worden minimaal 3 jaar bewaard.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van het Scala College maakt jaarlijks in januari een analyse van de meldingen van beveiligingsincidenten en datalekken in het achterliggende kalenderjaar, 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.

Het college van bestuur wordt geïnformeerd over de uitkomsten van de analyse.