# Protocol Informatie-beveiligingsincidenten en datalekken

## Lauwers College

Buitenpost, november 2020
Vastgesteld door de bestuurder op 1-12-2020

# Inleiding

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

Dit protocol biedt een handleiding voor de melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligings-incidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van het Lauwers College en haar medewerkers.

**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.

# 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 boete.

De meldplicht is van toepassing wanneer persoonsgegevens worden verwerkt, bijvoorbeeld in de leerlingenadministratie. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze verwerkers aanvullende afspraken maken 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 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 een klas, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Dit geldt ook als het datalek zich voordoet bij een externe verwerker van 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.

Als er een datalek is, moet de school daarvan binnen 72 uur na ontdekking van het lek, melding doen bij de Autoriteit Persoonsgegevens.

# Afspraken met leveranciers

Het schoolbestuur maakt als verantwoordelijke voor de persoonsgegevens afspraken met leveranciers als die persoonsgegevens ontvangen en verwerken. Afspraken over datalekken vallen daar ook onder. Deze afspraken gaan over:

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

Voor de schriftelijke afspraken met de verwerker(s) wordt gebruik gemaakt van de model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl). De school beheert alle afgesloten verwerkingsovereenkomsten in een verwerkingsregister en ziet toe op de naleving.

# Werkwijze datalekken

Er worden vijf rollen onderscheiden om een incident en/of datalek succesvol af te handelen:

1. **Ontdekker**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt. Alle medewerkers van het Lauwers College kunnen in de situatie verkeren dat zij deze rol op zich nemen.
2. **Meldpunt;** de centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. Het Lauwers College heeft deze rol belegd bij het servicedesk ICT; ict@lauwerscollege.nl .
3. **Melder**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens (AP). De directeur Stafbureau is verantwoordelijk voor de melding van het datalek aan de AP. De melding aan de AP vindt plaats na overleg met de FG van de school.
4. **De privacy-coördinator**; degene die de oorzaak van het datalek kan vaststellen en opdracht geeft om het te (laten) repareren. Deze rol ligt bij de directeur Stafbureau.
5. **De Functionaris Gegevensbescherming (FG)**; de FG begeleidt en adviseert de school in dit proces.

## *De werkwijze bestaat uit 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 ict@lauwerscollege.nl

   De Privacy-coördinator kan ook uit eigen beweging onveilige situaties opmerken – reactief en preventief -en daarmee in afstemming met betreffende medewerker en/of leidinggevende, het meldproces in gang zetten.

**2. Inventariseren**

Het Meldpunt bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan wordt technisch onderzoek uitgevoerd of worden aanvullende vragen uitgezet bij de Ontdekker.
De volgende informatie wordt daarna vastgelegd:

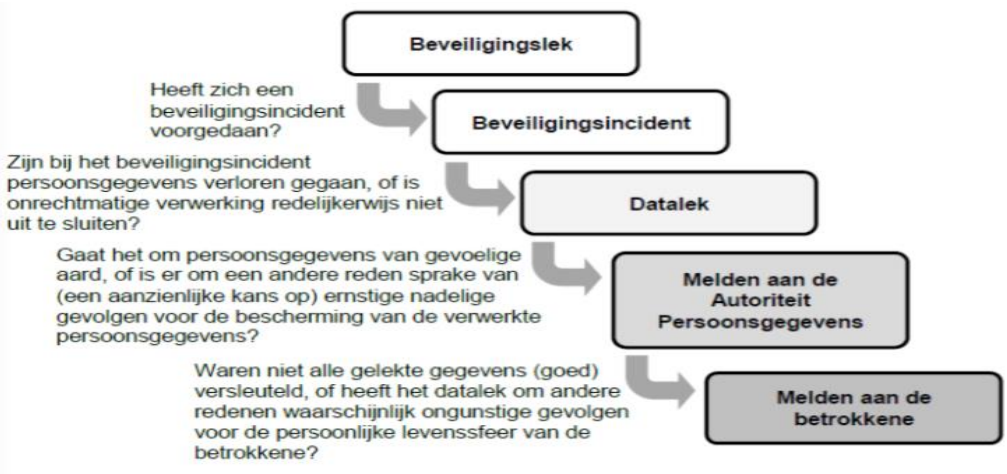
- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum en tijdstip van constatering van een vermeend datalek
- De periode waarin het beveiligingsincident of datalek zich heeft voorgedaan
- Aard van 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

De gegevens over gemelde incidenten en datalekken worden door het Meldpunt vastgelegd in een datalekkenregister. Per geval wordt de hiervoor vermelde informatie geregistreerd. Belangrijk is dat het register inzage biedt in het toepassen van de meldtermijn van 72 uren.

**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?

De onderstaande beslisboom kan gebruikt worden.



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 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 informatie over een leerling die vaak leerlingen pest en daarmee gezien kan worden als notoire pester).

**4. Repareren**

De Privacy-coördinator zal parallel aan het meldingsproces opdracht verstrekken om de oorzaak van het beveiligingsincident te achterhalen en maatregelen nemen om de oorzaak te (laten) verhelpen. Deze functionaris 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 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 door het Meldpunt in het datalek-register waarmee het incident kan worden afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

**7. Informeren betrokkene: leerling en/of ouders/verzorgers**

Heeft het datalek (naar verwachting) ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene dan wordt het datalek ook aan de betrokkenen zelf gemeld. Dat kunnen medewerkers, leerlingen of ouders zijn in geval de leerling jonger is dan 16 jaar. In principe kan er van worden uitgaan dat het lekken van gevoelige aard door de school gemeld moet worden bij de betrokkenen.
Let op: als er persoonsgegevens gelekt zijn die beveiligd of versleuteld zijn, 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.

# Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van de school 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 gerapporteerd over de uitkomsten van deze analyses.

De privacy-coördinator van het Lauwers College heeft een eigen mandaat m.b.t. de uitvoering van zijn verantwoordelijkheid. Dit houdt in dat hij van de bestuurder het mandaat heeft alle maatregelen te treffen die noodzakelijk zijn voor de gegevensbescherming. Dit mandaat is mede geborgd door de informatiefunctie van de functionaris gegevensbescherming jegens de Raad van Toezicht; in de RvT-auditcommissie wordt de kaderstelling en rapportages gegevensbescherming besproken.

# Communicatie

Wanneer het Lauwers College in een situatie geraakt met aanzienlijke schadeberokkening van persoonsgegevens – er is dan sprake van een melding datalek - treedt de volgende procedure in werking.

Communicatieprocedure.

1. De directeur stafbureau roept het OVERLEG-DATALEK bijeen. Dit bestaat uit de bestuurder, de directeur stafbureau en de FG. Indien nodig wordt de ICT-expert en de betrokken locatiedirecteur uitgenodigd.
2. De beoordeling (Stap 3) van het datalek wordt besproken.
3. Op basis van het overleg formuleert de bestuurder conclusies m.b.t. de aspecten:
    a. Persoonlijke schade van leerlingen, ouders en personeel
    b. Gebreken in de organisatie: techniek, organisatie en gedrag
    c. Imago-effecten voor de school
4. Naar bevind van zaken wordt gecommuniceerd met:
    a. Betrokkenen, door locatiedirecteur
    b. Media, door bestuurder
    c. Leveranciers, door directeur stafbureau
    d. AP, door de FG.
5. Twee maanden na de melding van het datalek communiceert de school de lessons learned en de getroffen maatregelen.

Het bestuur en de directie van het Lauwers College voeren een communicatiebeleid gebaseerd op volledige openheid van zaken.

<u>Contactgegevens</u>

| | | |
|---|---|---|
| Bestuurder: | R. de Wit | 06 4392 8780 |
| Directeur stafbureau: | D. Boersma | 06 5099 9378 |
| Meldpunt datalekken: | J. Kuipers | 06 2112 4929 |
| | | |
| FG/ S. Sarneel, Lumen-Group B.V. : | | 088 889 6575 |
| Autoriteit Persoonsgegevens: | | 070 8888 500 |