# Protocol Datalekken

STOVOG

Stichting Openbaar Voortgezet Onderwijs Gouda

Versie april 2019

**Inleiding**
Het Protocol Datalekken sluit aan bij de uitgangspunten in het informatiebeveiliging- en privacy (IBP) beleid van STOVOG.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen- en minimaliseren van de effecten van beveiligingsincidenten en datalekken. Het betreft het beschermen van persoonsgegevens conform de doelstelling van de AVG.

Dit protocol is van toepassing op de gehele organisatie van STOVOG, zoals vermeld in het IBP beleid, Privacy reglement en al 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 verwerkt (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**
De wet meldplicht datalekken geldt ook na de invoering van de AVG. Door deze meldplicht zijn ook scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van een datalekmelding waarbij er sprake is van een meldplicht kan leiden tot een boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in de leerlingadministratie, personele zaken of digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens verwerken 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 is 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 klas 3b, is ook een datalek. De meeste datalekken komen voort uit het menselijk handelen.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een verwerker voor de school. Het is van belang dat de verantwoordelijke altijd controle houdt over een eventuele melding aan de Autoriteit Persoonsgegevens.

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

**Afspraken met leveranciers**
Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken voor de interne organisatie en met leveranciers (verwerkers in de zin van de AVG) als die persoonsgegevens verwerken. Afspraken over datalekken vallen daar ook onder. De volgende aspecten zijn van belang:

- 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 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

Maak schriftelijke afspraken met uw verwerker(s) over datalekken. Dit is een standaard onderdeel van een verwerkersovereenkomst.

**Werkwijze**
Dit protocol kan niet bestaan zonder een Informatiebeveiligingsplan en een gedragsprotocol betreffende de omgang met persoonsgegeven door de werknemers van STOVOG. Deze documenten beschrijven de genomen maatregelen die beveiligingsincidenten en datalekken moeten voorkomen. Tijdens het afhandelen van de melding is het schoolbestuur verantwoordelijk voor de interne en externe communicatie over de ontwikkelingen. Het staat het schoolbestuur te allen tijde vrij om experts van buitenaf in te huren indien dit naar haar mening nodig is. Hieronder volgen een aantal definities en een stappenplan.

*Ontdekker (medewerker)*; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
*Meldpunt (servicedesk)*; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt ( de FG).
*Melder (privacy officer/coördinator of functionaris gegevensbescherming)*; degene die verantwoordelijk is (naast het bestuur) voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
*Technicus (security officer/ICT coördinator)*; degene die de (technische) oorzaak van het datalek kan vinden en kan (laten) repareren, en mogelijke vervolg schade kan beperken.

Wanneer een datalek ontdekt wordt treedt het volgende stappenplan in werking:

*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 de leidinggevende en de FG.

*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 (gevoelige en of bijzondere gegevens);
- 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 vermoed, 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’, hou 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 betrokkene(n), moet het datalek gemeld worden bij de Autoriteit Persoonsgegevens.

Van mogelijke (ernstige) nadelige gevolgen is bijvoorbeeld sprake wanneer er (veel) gegevens van betrokkene(n) gelekt zijn maar met name wanneer de gelekte gegevens “gevoelig” zijn zoals

bijvoorbeeld financiële gegevens. Of erger als het “bijzondere persoonsgegevens” betreft. Bijzondere gegevens betreffen de volgende onderwerpen: gezondheid, geloofsovertuiging, economische situatie van de betrokkene, seksuele geaardheid, politieke opvatting, verwerking van genetische gegevens, biometrische gegevens 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 ICT coördinator (intern of extern) eventueel samen met de Privacy coördinator wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident/datalek is en moet de oorzaak (laten) verhelpen. De ICT coördinator (technicus) en eventueel de Privacy coördinator (melder) van STOVOG leggen 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 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 betrokkene(n) worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan er van worden uitgegaan dat het lekken van gevoelige aard gemeld moet worden bij de betrokkene(n).

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 betrokkene(n) te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

**Monitoring beveiligingsincidenten en datalekken**

Het Meldpunt van STOVOG maakt minimaal een 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.

Het schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.