Protocol datalekken Stichting Archipel

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

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 Stichting Archipel, zoals vermeld in het IBP beleid, 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 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 fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in je leerlingenadministratie of digitale leermiddelen. 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 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 groep 3, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een verwerker voor 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 daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

Afspraken met leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder.

Met alle leveranciers die gebruik maken van persoonsgegevens worden schriftelijke afspraken gemaakt. Hiervoor wordt gebruik gemaakt van de model verwerkersovereenkomst die hoort bij het convenant “Digitale Onderwijsmiddelen en Privacy 3.0” (www.privacyconvenant.nl).

Werkwijze

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document betreffende de gedragscode ict en internetgebruik.

De vier rollen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

- **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
- **Meldpunt (datalek@archipelprimair.nl)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
- **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
- **Technicus (security officer/ICT medewerker)**; 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 (de manager IBP) via datalek@archipelprimair.nl.

2. Inventariseren

Het Meldpunt (de manager IBP) 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

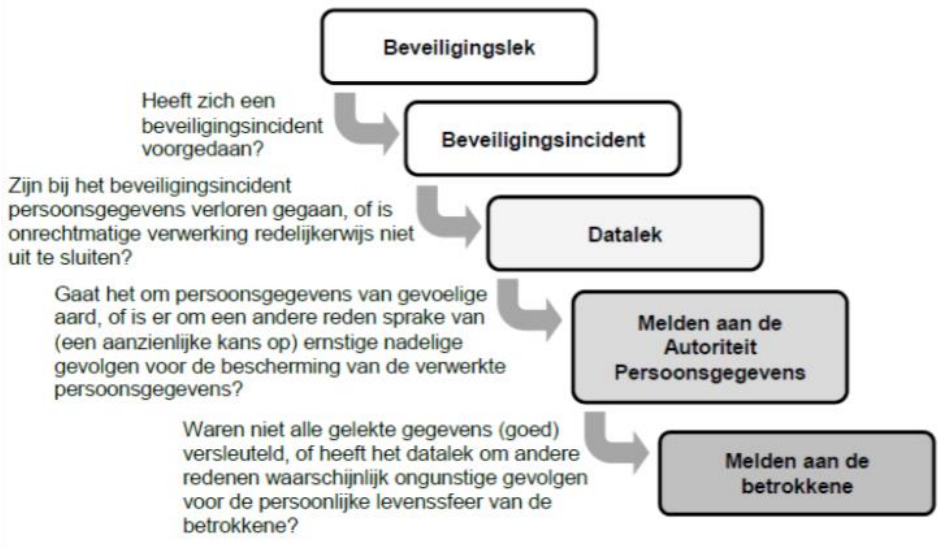
3. Beoordelen

Wanneer het Meldpunt (de manager IBP) 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', 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 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.

De onderstaande beslisboom wordt gebruikt:



4. Repareren

De Technicus (medewerker ICT) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus legt het volgende vast:

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen, 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. Het meldingsformulier is openbaar.

6. Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt (Manager IBP), 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 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 gemeld moet worden bij de betrokkene. 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 te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van Stichting Archipel 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.
Het college van bestuur wordt geïnformeerd over de uitkomsten van de analyse.

Communicatie

Eventueel noodzakelijke communicatie, anders dan in dit protocol vermeld, bijvoorbeeld naar de pers, loopt altijd via het college van bestuur.
Mocht het noodzakelijk zijn bij het optreden van een datalek externe deskundigheid in te huren dan wordt dit door het college van bestuur bepaald.
Dit protocol wordt aan alle medewerkers van Stichting Archipel bekend gemaakt en gepubliceerd op het intranet en internet.