Protocol informatiebeveiligingsincidenten en datalekken.

Versie geschiedenis:

Versie	Status	Datum	Auteur	Omschrijving
001	Ontwerp	07-06-2022	BRR	Conceptversie
002	Controle	29-06-2022	BRR	Goedgekeurd door Hoofd ICT.
003	Controle FG	30-06-2022	BRR	Goedgekeurd door de Lumen Group.
004	Aanbieden GMR	24-11-2022	BRR	Aangeboden voor goedkeuring GMR.
005	Goedgekeurd	24-11-2022	BRR	Goedgekeurd GMR.

Vastgesteld door OGMF:

Versie	Datum	Naam	Functie
001	09-02-2023	Merijn Sprenger	Voorzitter College van Bestuur (CvB).

Looptijd en reikwijdte:

Dit *Protocol informatiebeveiligingsincidenten en datalekken* is vastgesteld op 1 januari 2023 en treedt in werking op na goedkeuring door de GMR, en wordt per twee jaar geëvalueerd (voorjaar 2025). Het protocol geldt voor alle vestigingen van OGMF.

INHOUDSOPGAVE

Inhoud

INLEIDING

Het *Protocol informatiebeveiligingsincidenten en datalekken* sluit aan bij de uitgangspunten in het *Informatiebeveiligings- en privacy beleid* van OGMF. Dit protocol biedt een handleiding voor de professionele melding, boordeling en afhandeling van beveiligingsincidenten en datalekken.

Het protocol is van toepassing op de gehele organisatie van OGMF en al zijn medewerkers, zoals vermeld in het IBP-beleid.

1 GEBRUIKTE BEGRIPPEN

In dit protocol wordt een aantal begrippen gebruikt, die hieronder worden gedefinieerd:

beveiligingsincident	een gebeurtenis die ervoor zorgt of ervoor zou kunnen zorgen dan de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast
betrokkene	de persoon van wie de persoonsgegevens zijn gelekt; dit kunnen een of meer leerlingen of medewerkers zijn
bevoegd gezag	het College van Bestuur (CvB)
datalek	een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, etc.); alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken
informatievoorziening	het geheel van mensen, middelen en maatregelen gericht op de informatiebehoefte van de organisatie
verantwoordelijke	het bevoegd gezag, CvB
verwerker van gegevens	de persoon of organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed

2 WET- EN REGELGEVING DATALEKKEN

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht bij de Autoriteit Persoonsgegevens (AP) melding te maken van ernstige datalekken. Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt, zoals in de leerling administratie of in digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan maakt de school met deze verwerkers in verwerkersovereenkomsten aanvullende afspraken over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren, een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot

doorgezonden, opgeslagen of anderszins verwerkte gegevens heeft geleid. Of als het niet valt uit te sluiten dat daarbij 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 laptop met daarop de adresgegevens van bijvoorbeeld klas 3b is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het bevoegd gezag. Een bewerker van gegevens kan namens de verantwoordelijke de melding doen, maar dat gebeurt dan onder verantwoordelijkheid van het bevoegd gezag. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.
Als er een datalek is, dan moet - indien het nodig is de Autoriteit Persoonsgegevens hiervan op de hoogte te brengen - dit binnen 72 uur na ontdekking gemeld worden.

3 AFSPRAKEN MET LEVERANCIERS

Het CvB is verantwoordelijk voor de persoonsgegevens en moet daarom afspraken maken met leveranciers als die persoonsgegevens ontvangen. De Privacy Officer handelt dit in de praktijk af namens, in opdracht en met goedkeuring van, het CvB. Afspraken over datalekken vallen daar ook onder. Afgesproken moet worden:

- hoe men elkaar over en weer informeert over datalekken; hierbij moet ervoor worden gezorgd dat er ook afspraken gemaakt worden over bereikbaarheid tijdens bijvoorbeeld het weekend en de vakanties;
- wie de melding doet bij de Autoriteit Persoonsgegevens;
- welke informatiegegevens de verwerker moet geven bij een datalek;
- welke informatie nodig is voor het doen van een melding, dat men elkaar informeert over de melding en hoe dat dan gebeurt (bijvoorbeeld door een kopie van de melding door te sturen of te ontvangen);
- binnen welk tijdsbestek de bewerkers de gegevens moeten aanleveren;
- wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

De school maakt schriftelijke afspraken over datalekken met de verwerker(s). OGMF maakt hiervoor gebruik van de modelovereenkomst die hoort bij het convenant *Digitale onderwijsmiddelen en privacy* (www.privacyconvenant.nl).

4 WERKWIJZE

In het proces van melden en afhandelen van een datalek worden verschillende rollen onderscheiden en moet een aantal stappen gezet worden. Deze worden in het vervolg van deze paragraaf besproken.

Rollen

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

1. **Ontdekker** (bijvoorbeeld een medewerker) - degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt** (Privacy Officer) - een centrale persoon die alle beveiligingsincidenten registreert en het proces monitort.
3. **Melder** (Privacy Officer) - degene die verantwoordelijk is voor het melden van een datalek bij de

Autoriteit Persoonsgegevens.

4. **FG** (De Lumen Group) Functionaris gegevensbescherming van OGMF. Deze wordt door de PO ten alle tijden geïnformeerd over gemelde of geconstateerde datalekken.
5. **Technicus** (ICT-medewerker of applicatiebeheerder) - degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

Proces

In het proces van het ontdekken en afhandelen van een datalek worden zeven fasen onderscheiden. Deze fasen kunnen ook gelijktijdig plaatsvinden.

1. **Ontdekken**

De ontdekker merkt een beveilingsincident op via eigen waarneming of via de waarneming van een derde. De ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het incident zo snel mogelijk via Privacy@Sevenwolden.nl.
Signalen van buitenaf over een mogelijk datalek worden serieus genomen. De Privacy Officer zal onderzoek doen naar de bron van de signalen en indien nodig deze vragen een officiële melding te doen, waarna de benodigde procedurele stappen genomen zullen worden.

2. **Inventariseren**

Het meldpunt bepaalt 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:

- Een samenvatting van het beveiligingsincident: wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of gegevens van gevoelige aard).
- De datum/periode van het beveiligingsincident.
- De aard van het beveiligingsincident.
- Wanneer van toepassing (als het inderdaad om een datalek gaat):
    - een omschrijving van de groep betrokkenen;
    - het aantal betrokkenen;
    - om welk type persoonsgegevens het gaat;
    - of de gegevens binnen een keten gedeeld worden.

De Privacy Officer overlegt, indien nodig, met de voorzitter van het College van Bestuur (CvB) over de communicatie richting medewerker(s) en/of leerlingen of hun ouder(s)/verzorger(s) indien de leerlingen jonger zijn dan 16 jaar.

3. **Beoordelen**

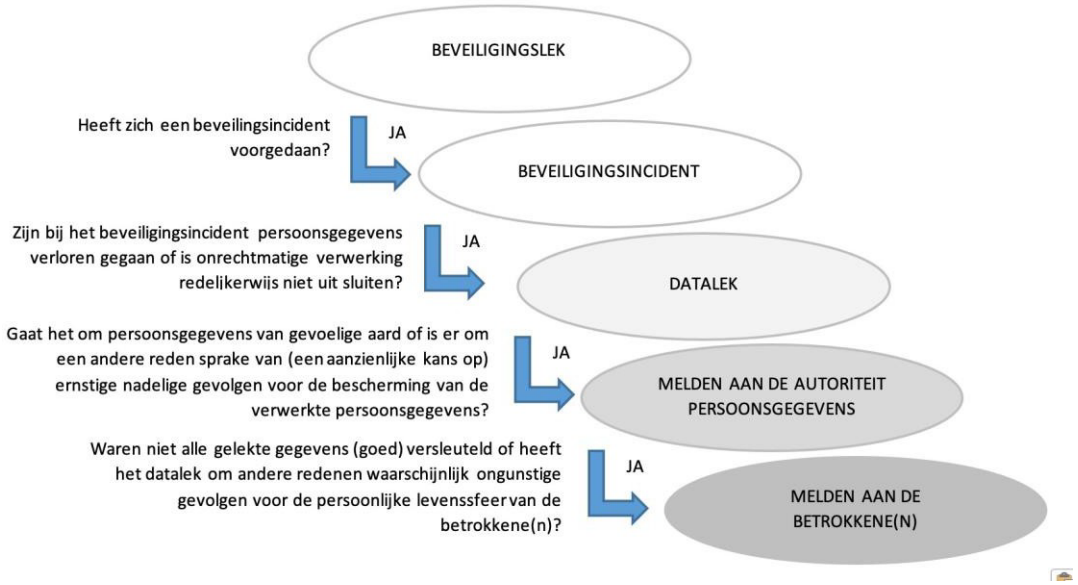
Als de Privacy Officer voldoende informatie verzameld heeft en een datalek vermoedt, moet beoordeeld worden of het lek aan de Autoriteit Persoonsgegevens gemeld moet worden. Omdat deze rol bij de Privacy Officer ligt, maar de CvB de verantwoording hiervoor draagt, betrekt de Privacy Officer deze bij de beoordeling hiervan.

De Privacy Officer beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkene(n) vereist is.
De volgende informatie wordt vastgelegd door de melder:

- Wat zijn de mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene(n)?
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom (niet)?
- Wordt het datalek gemeld aan de betrokkene(n)? Waarom (niet)?
- Hoe worden de meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’ houdt de melder rekening met het type gegevens en met de hoeveelheid gegevens. Als een datalek leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens of op een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, dan moet er gemeld worden. Van ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake als er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn, of als de gelekte gegevens ‘gevoelig’ zijn zoals bijvoorbeeld bijzondere persoonsgegevens over de gezondheid, de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene(n) (denk aan het lekken van gegevens over een leerling die vaak medeleerlingen pest en daarmee gezien kan worden als een notoire pester).

Bij OGMF gebruiken we de volgende beslisboom:



4. **Melden**

   Als de Privacy Officer bij stap 3 concludeert dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en dat de betrokkene(n) geïnformeerd moeten worden), dan doet hij deze melding na overleg met het CvB en eventueel met de Functionaris gegevensbescherming. De melding wordt binnen twee werkdagen gedaan bij de Autoriteit Persoonsgegevens via het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?

   De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. (Zie bijlage 1.)
   Het CvB en de Functionaris gegevensbescherming worden op de hoogte gebracht van de melding.

5. **Repareren**

   De technicus (intern of zo-nodig extern) wordt indien het datalek het gevolg is van een technisch beveiligingsincident gevraagd te achterhalen wat de oorzaak van het incident is. Hij moet de oorzaak (laten) verhelpen.

Of het gewenst is dat externe deskundigen worden ingeschakeld is afhankelijk van de situatie en ter beoordeling van de Privacy Officer, zo nodig in overleg met het hoofd ICT en/of het CvB.

De (ingehuurde) technicus van OGMF legt het onderstaande vast:

- welke technische en organisatorische maatregelen genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen;
- in hoeverre de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen en hoe de gegevens onbegrijpelijk zijn gemaakt (versleuteld)?

6. **Vastleggen**
   Alle informatie die in de voorafgaande stappen is ingewonnen of ontstaan, wordt vastgelegd in het document *Incidentenmelding en -verwerking* en gearchiveerd door het meldpunt, waarmee het incident is afgesloten. Het meldpunt verstuurt een samenvatting van de genomen maatregelen aan de ontdekker.

7. **Informeren**
   Een datalek kan mogelijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene(n). In dat geval meldt de Privacy Officer het lek - na overleg met de stafmedewerker communicatie - ook aan de betrokkene(n) zelf. De betrokkene(n) kunnen medewerker(s) of leerling(en) (of hun ouder(s)/verzorger(s) als de leerlingen jonger zijn dan 16 jaar) zijn.
   Als er persoonsgegevens zijn gelekt die beveiligd of versleuteld waren, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft het datalek niet aan de betrokkene(n) te worden gemeld. Zie ook de beslisboom bij stap 3.

5 MONITORING BEVEILINGSINCIDENTEN EN DATALEKKEN

De Privacy Officer van OGMF maakt één keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen en wordt aangegeven of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen. Het CvB wordt geïnformeerd over de uitkomsten van de analyse.

6 COMMUNICATIE

Als bij de Autoriteit Persoonsgegevens een melding is gedaan van een datalek, en het datalek betreft gegevens die niet (goed) versleuteld zijn of die om andere redenen ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene(n), dan wordt/worden de betrokkene(n) hiervan op de hoogte gesteld. Afhankelijk van de situatie en de ernst van het datalek zal het CvB indien nodig de media via een persbericht op de hoogte stellen.

BIJLAGE 1

MELDINGSFORMULIER DATALEK van de Autoriteit Persoonsgegevens

AUTORITEIT PERSOONSGEGEVENS

Meldloket

Een nieuwe melding doen

- Voor het melden van een datalek vult u onderstaand formulier in.
- Lees ook onze informatie over meldplicht datalekken en raadpleeg de Richtsnoeren voor de melding van datalekken van de Europese privacytoezichthouders.
- Nadat u een melding heeft gedaan, krijgt u een meldingsnummer te zien ter bevestiging. Registreer dit nummer voor verdere communicatie met de Autoriteit Persoonsgegevens.

0. Over deze melding

Gaat het om een nieuwe of bestaande melding? Nieuwe melding

Op grond van welke wettelijke bepaling doet u deze melding? Kies er een

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Registratienummer bij de Kamer van Koophandel

Naam van het bedrijf of de organisatie

Adres

Postcode

Plaats

In welke sector is de organisatie of het bedrijf actief? Kies er een

Overige sector, te weten:

Wie meldt het datalek?

Naam

Functie

E-mailadres

Telefoonnummer

Tweede telefoonnummer

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon Kies er een

Naam contactpersoon

Functie contactpersoon

E-mailadres contactpersoon

Telefoonnummer contactpersoon

Tweede telefoonnummer contactpersoon

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk? Kies er een

Naam van de andere organisatie die betrokken was bij de inbreuk

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend

Startdatum van de periode waarbinnen de inbreuk was

Einddatum van de periode waarbinnen de inbreuk was

Duurt de inbreuk op dit moment nog voort? Kies er een

Wanneer werd de inbreuk ontdekt?

Als u de inbreuk later meldt dan 72 uur na de ontdekking, wat is daarvan dan de reden?

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens Kies er een

Inbreuk op de integriteit van de gegevens Kies er een

Inbreuk op de beschikbaarheid van de gegevens Kies er een

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest? Kies er een

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Kies er een
Geslacht, geboortedatum en/of leeftijd	Kies er een
Burgerservicenummer (BSN)	Kies er een
Contactgegevens	Kies er een
Toegangs- of identificatiegegevens	Kies er een
Financiële gegevens	Kies er een
(Kopieën van) paspoorten of andere legitimatiebewijzen	Kies er een
Locatiegegevens	Kies er een
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	Kies er een
Onbekend / anders, namelijk:	

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Kies er een
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Kies er een
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Kies er een
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Kies er een
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Kies er een
Gegevens over iemands gezondheid	Kies er een
Genetische gegevens	Kies er een
Biometrische gegevens	Kies er een

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Kies er een
Klanten (huidig en potentieel)	Kies er een
Leerlingen of studenten	Kies er een
Patiënten	Kies er een
Minderjarigen	Kies er een
Personen uit kwetsbare groepen	Kies er een

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Kies er een
Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om welk deel gaat dat dan?	

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens — Kies er een

De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt — Kies er een

Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt — Kies er een

Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties — Kies er een

Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen — Kies er een

Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen — Kies er een

Anders, namelijk

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie — Kies er een

Identiteitsdiefstal of -fraude — Kies er een

Financiële verliezen — Kies er een

Reputatieschade — Kies er een

Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens — Kies er een

Ongeoorloofde ongedaanmaking van pseudonimisering — Kies er een

Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen — Kies er een

Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen — Kies er een

Andere gevolgen, namelijk:

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen — Kies er een

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? — Kies er een

Wanneer heeft u het datalek gemeld aan de betrokkenen?

Wanneer gaat u het datalek melden aan de betrokkenen?

Wat is de inhoud van de melding aan de betrokkenen?

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?

Waarom ziet u af van het melden van het datalek aan de betrokkenen? — Kies er een

Als het informeren van alle betrokkenen een onevenredige inspanning zou vergen, licht dan toe hoe u door een openbare mededeling of een soortgelijke maatregel de betrokkenen gaat informeren.

Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?

Welke andere redenen heeft u om de betrokkenen niet te informeren?

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder? Kies er een

Als er sprake is van een grensoverschrijdende gegevensverwerking, om welke EU-landen gaat het dan?

Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen? Kies er een

Ja, namelijk

Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen? Kies er een

Ja, namelijk

9. Overig

Is naar uw mening deze melding compleet? Kies er een