OSZG | ONDERWIJSSTICHTING ZELFSTANDIGE GYMNASIA

Protocol beveiligingsincidenten en datalekken

Vastgesteld in de bestuursvergadering van: 23-6-2018 (B2018-33)

Inhoud

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken zal worden opgenomen in het informatiebeveiligings- en privacybeleid van OSZG.

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 OSZG 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 verplichting 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 de leerlingadministratie 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 bewerkers aanvullende afspraken 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 meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker **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. Spreek af:

- 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 bewerker 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 bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Maak schriftelijke afspraken met uw bewerker(s) over datalekken. Hiervoor kan gebruik worden gemaakt van de model bewerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl).

Werkwijze

Uitgangssituatie

- Er is wordt naar aanleiding van een PIA een actueel informatiebeveiligings- en privacybeleid opgesteld. Tot die tijd gelden de huidige privacyreglementen voor leerlingen en medewerkers.
- De notitie informatiebeveiliging- en privacybeleid wordt in september door het bestuur vastgesteld.

De vier rollen

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)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming** of **privacy officer)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (security officer/ict-coördinator)**; 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 via **gegevensbescherming@oszg.nl.**

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 (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

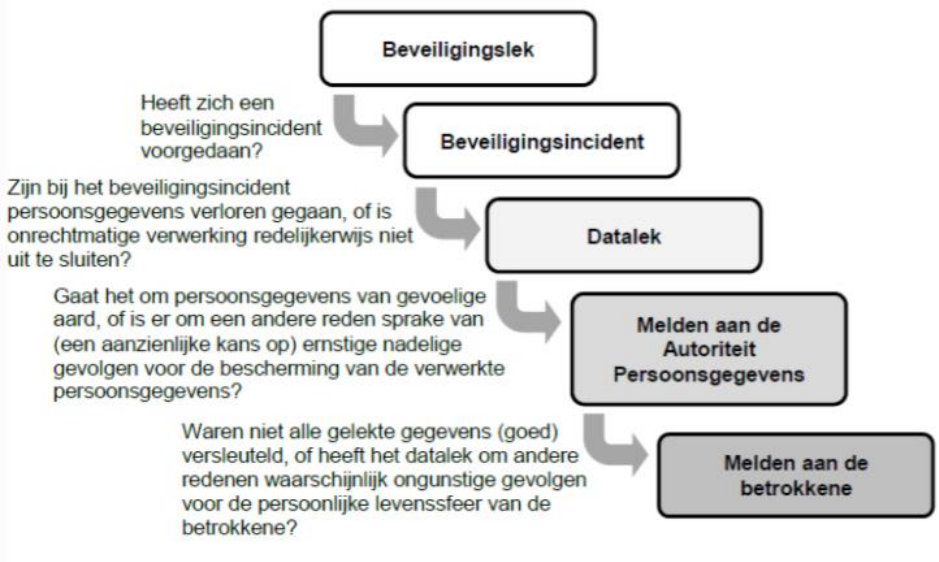
3. Beoordelen

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?
- 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 (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 Technicus (intern of extern) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus 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 (zie bijlage). Het meldingsformulier is openbaar.

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 en/of medewerkers**
   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 gevoelige aard gelekt gemeld moet worden bij de betrokkenen. 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 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 OSZG 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 schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.

Meldpunt datalekken OSZG

Yvonne Brandenburg (ad interim) : gegevensbescherming@oszg.nl
(y.brandenburg@oszg.nl)

Overzicht Technici (verantwoordelijke ICT-medewerkers per school)

Barlaeus Gymnasium	: Evan van Hooren (evanhooren@barlaeus.nl)
Gymnasium Bernrode	: Marc Brok (MBR@bernrode.nl)
Gymnasium Felisenum	: Jordi van Ditmar (j.ditmar@felisenum.nl) en Marcel Kemper (m. kemper@felisenum.nl)
Stedelijk Gymnasium Haarlem	: Jelle Snoeks (j.snoeks@sghaarlem.nl)
Stedelijk Gymnasium ’s Hertogenbosch	: Wim Heijzelaar (hr@stedgymdenbosch.nl)
Vossius Gymnasium	: Paulo Ramos (ramos@vossius.nl)
Bestuursbureau	: Winsys (bo@winsys.nl)

Communicatie

Denk hier na over:
- ✓ De manier van communiceren met betrokkenen en de pers.
- ✓ Hoe kan worden omgegaan met signalen van buitenaf over een mogelijk datalek.
- ✓ Is het inschakelen van externe deskundigen gewenst?

Een nieuwe melding doen bij de Autoriteit Persoonsgegevens

Voor het melden van een datalek vult u onderstaand formulier in.

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?

Op grond van welke wettelijke bepaling doet u deze melding?

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?

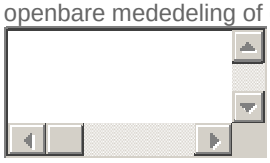
Wat is de inhoud van de melding aan de betrokkenen?

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?

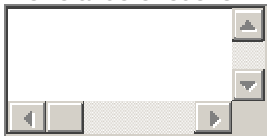
Waarom ziet u af van het melden van het datalek aan de betrokkenen?

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.



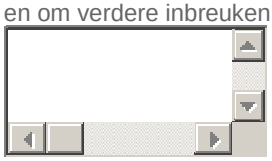
Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?

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?

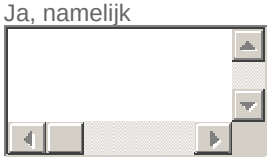
Kies er een

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