Protocol informatiebeveiligingsincidenten en datalekken

Scholengroep Katholiek Onderwijs
Flevoland Veluwe

SCHOLENGROEP KATHOLIEK ONDERWIJS

Flevoland en Veluwe

Protocol informatiebeveiligingsincidenten en datalekken SKO 2018

Deze regeling is vastgesteld door het College van Bestuur op 27 juni 2018.
Deze regeling is ter instemming voorgelegd aan de GMR op 25 juni 2018.
Deze regeling is besproken door het Directieberaad op 17 april 2018.

Inhoud

Documentbeheer
De stuurgroep IBP is de eigenaar van dit document. De originele en geaccordeerde versie is in beheer van en kan worden verkregen via het emailadres: datalekken@skofv.nl. Een elektronische of papieren kopie is verkrijgbaar op aanvraag.

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van Scholengroep Katholiek Onderwijs Flevoland Veluwe, hierna te noemen 'SKO'.

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 SKO, zoals vermeld in het IBP-beleid en al haar medewerkers.

Dit protocol is gebaseerd op het model 'protocol informatiebeveiligingsincidenten en datalekken' d.d. 6 oktober 2016 van Kennisnet.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die ervoor 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 je leerling administratie 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 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 College van Bestuur. Een leverancier is een verwerker voor de school. Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan door het College van Bestuur bij de Autoriteit Persoonsgegevens.

Afspraken met leveranciers

Het College van Bestuur maakt als verantwoordelijke voor de persoonsgegevens afspraken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Wij maken met iedere verwerker de volgende afspraken :

- Informeren over datalekken (bereikbaarheid weekend en vakanties).
- Meldingsplicht Autoriteit Persoonsgegevens.
- Welke informatiegegevens de verwerker verstrekt 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 verwerker de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Bovenstaande afspraken worden vastgelegd in de individuele verwerkersovereenkomsten.

Werkwijze

Uitgangssituatie

- Er is een informatiebeveiligings- en privacy beleid SKO 2018
- Er is een EIC-regeling SKO.

De vier rollen

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

1. **Individuele medewerker**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Stuurgroep IBP (via datalekken@skofv.nl)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Het College van Bestuur:** degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Comlog & ICT-coördinator:** degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De zeven stappen

1. **Ontdekken**
   De medewerker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De medewerker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt via datalekken@skofv.nl,

2. **Inventariseren**
   De stuurgroep IBP bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de betreffende medewerker en/of ICT-coordinator / Comlog. 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

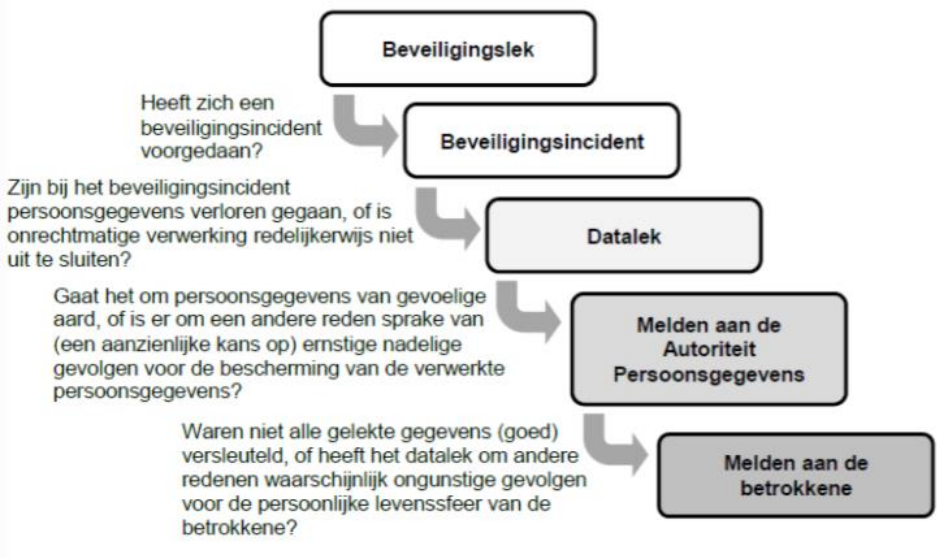
3. Beoordelen

Wanneer CvB voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de medewerker een verzoek om de verzamelde informatie te bekijken. Het CvB beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.
De volgende informatie wordt vastgelegd door het CvB:

- 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', wordt rekening gehouden met 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 wordt gebruikt.



4. Repareren

Comlog en / of de ICT-coördinator wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. Onderstaande wordt vastgelegd.

- 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 het CvB dit binnen twee werkdagen doen. Het CvB 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 de stuurgroep IBP waarmee het incident is afgesloten. De stuurgroep IBP verstuurt een samenvatting van de genomen maatregelen aan de medewerker / directeur.

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 betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgaan dat het lekken van persoonsgegevens van gevoelige aard 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

De stuurgroep IBP 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 CvB wordt geïnformeerd over de uitkomsten van de analyse.