PROTOCOL IBP INCIDENTEN EN DATALEKKEN

REHOBOTH

VERENIGING VOOR SCHOLEN MET DE BIJBEL

Protocol IBP Incidenten en Datalekken

Bron: Kennisnet

Bewerkt: Schoolvereniging Rehoboth

Versie	Status	Datum	Auteur	Omschrijving
0.1	concept	14-3-2018	Catharinus Doornbos	

Vastgesteld door Schoolvereniging Rehoboth

Versie	Datum	Naam	Functie	Paraaf
1.0	10-04-2018	Wilma Dorleijn	Algemeen Directeur a.i.	
1.0	09-04-2018	Frits Cleveringa	Voorzitter GMR	

Inhoudsopgave

Protocol IBP Incidenten en Datalekken

1 Inleiding

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

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 Schoolvereniging Rehoboth en al haar medewerkers, zoals vermeld in het IBP Beleid.

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, etc.). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.

Betrokkene
De persoon van wie de persoonsgegevens zijn gelekt.

2 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, de personeelsadministratie, de schoolgids of digitale leermiddelen. Als de stichting en/of de scholen gebruik maken van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de stichting en/of de scholen, dan moeten de stichting en/of de scholen met deze bewerkers schriftelijk 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 of in verkeerde handen zijn gekomen. 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 uitgeprint leerlingendossier of een usb-stick met daarop de adresgegevens van een klas, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, bij Schoolvereniging Rehoboth dus de Algemeen Directeur. Een leverancier is een bewerker voor stichting en/of de scholen. Er kan worden afgesproken dat een bewerker namens de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van de Algemeen Directeur. 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.

3 Afspraken met leveranciers

De Algemeen Directeur maakt als verantwoordelijke voor de persoonsgegevens afspraken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Er worden afspraken gemaakt over:

- Het informeren van elkaar over datalekken.
- Wederzijdse bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie melding doet bij de Autoriteit Persoonsgegevens.
- Welke informatiegegevens de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding.
- Het elkaar informeren over de melding en elkaar (door-)sturen van een kopie van de melding.
- De tijd waarbinnen de bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers en/of betrokkenen voor haar rekening neemt als dat nodig is.

De afspraken met bewerker(s) over datalekken worden schriftelijk vastgelegd. Wanneer de bewerker zelf geen bewerkingsovereenkomst aanlevert, maken we gebruik van de model bewerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (www.privacyconvenant.nl). Wanneer bewerker zelf een bewerkingsovereenkomst aanlevert, verwachten we dat deze voldoet aan de eisen zoals afgesproken in genoemd convenant.

4 Werkwijze

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en een Gedragscode ICT en internetgebruik.

De vier rollen

Er zijn tenminste vier rollen die we onderscheiden 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 (Manager IBP)**
De centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.

*Melder (Functionaris voor Gegevensbescherming)**
Degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.

Technicus (Bovenschools ICT-coördinator en/of externe beheerder)
Degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

**Deze twee rollen worden binnen Schoolvereniging Rehoboth door één persoon ingevuld.*

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 (meldpunt-ibp@rehoboth.nu). Voor het melden kan gebruik worden gemaakt van het 'Meldingsformulier IBP Incidenten en datalekken' (Bijlage 1). Deze is via de website van Schoolvereniging Rehoboth beschikbaar als download en als digitaal formulier.

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 er met de gegevens is 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
    - Het al dan niet gedeeld worden van de gegevens binnen een keten; zo ja beschrijving van de keten en betrokkenen

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.

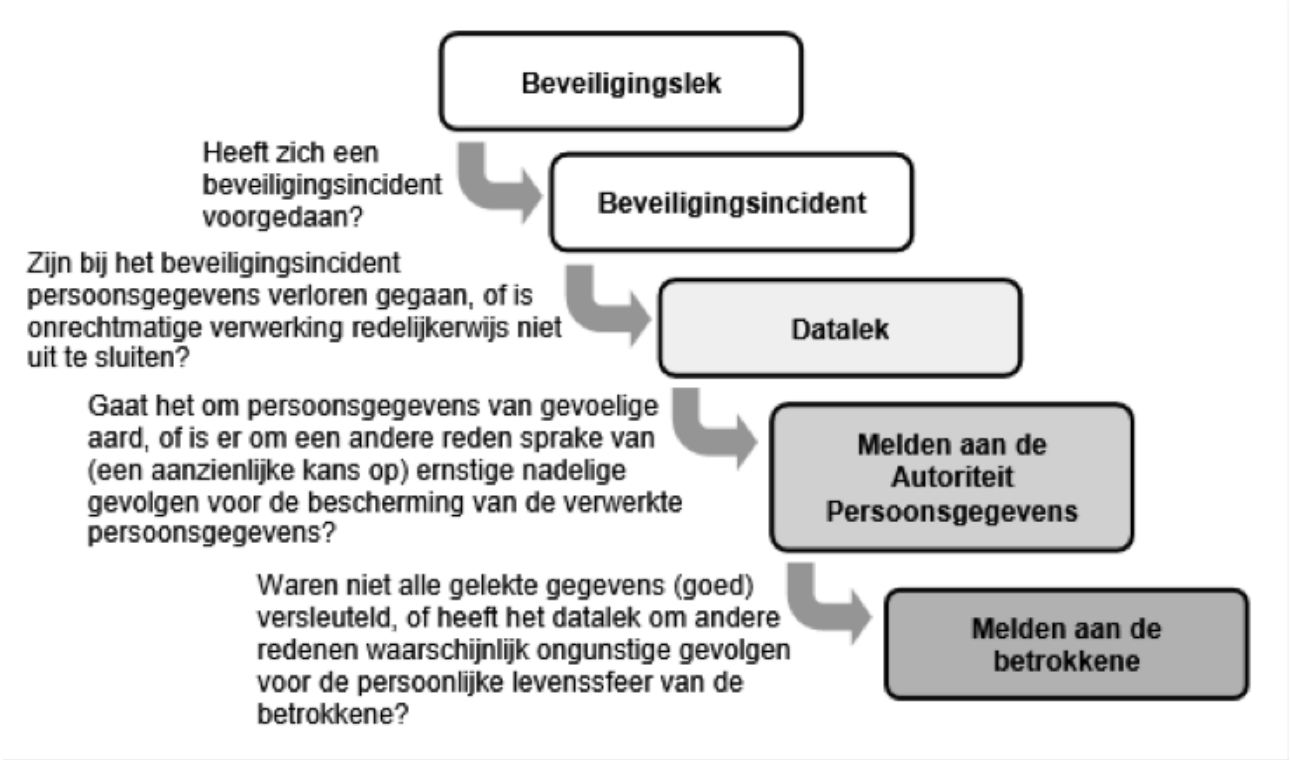
De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen.
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom wel/niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom wel/niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', houden we 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 wordt hierbij gebruikt:



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 van Schoolvereniging Rehoboth 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 degene 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
Het incident en/of datalek wordt vastgelegd in het 'Logboek IBP Incidenten en Datalekken' (Bijlage 2). 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 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 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.

5 Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van Schoolvereniging Rehoboth maakt twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de Functionaris voor Gegevensbescherming. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen. De Algemeen Directeur wordt geïnformeerd over de uitkomsten van de analyse.

6 Communicatie

Indien er contact moet worden gelegd met Betrokkenen of als contact met de pers noodzakelijk is, dan wordt dit gedaan door de Algemeen Directeur. Dit gebeurt na inhoudelijke afstemming met de Functionaris voor Gegevensbescherming, de Manager IBP en het Meldpunt. Indien de Algemeen Directeur niet beschikbaar is, bijvoorbeeld tijdens een vakantie, dan wordt deze taak opgepakt door een hiervoor door Algemeen Directeur gemachtigde Directeur.

Indien er van buiten de organisatie signalen over een mogelijk datalek vernomen worden, dan wordt dit gemeld bij het Meldpunt. De Algemeen Directeur zoekt contact met de bron van deze signalen om het verzoek te doen de relevante informatie kenbaar te maken aan Algemeen Directeur dan wel het Meldpunt.

In geval van strafbare feiten zal Algemeen Directeur daarvan aangifte doen.

Algemeen Directeur kan beslissen in voorkomende gevallen advies of hulp in te winnen van externe deskundigen. Hierbij kan gedacht worden aan een persvoorlichter, een jurist, een internet- en (sociale) media-expert, etc.

7 Bijlagen

Bijlage 1 – Meldingsformulier IBP Incidenten en Datalekken

Bijlage 2 – Logboek IBP Incidenten en Datalekken

Bijlage 3 – Procedure Melding Kwetsbaarheden – Medewerkers

Bijlage 4 – Procedure Melding Kwetsbaarheden – Leerlingen