Protocol informatiebeveiligingsincidenten en datalekken

Stichting Onderwijsgroep Amersfoort

Versie: 0.6
Datum: 8 oktober 2019

	STATUS			
Van toepassing op:	Concept/Definitief	Bespreken	Vastgesteld	Versienummer
Intern	C	5 mei 2018		0.1
Projectgroep	C	15 mei 2018		0.2
Werkgroep AVG	C	11 september 2019		0.3
Stuurgroep AVG	C	27 september 2019		0.4
Directieraad	C	3 oktober 2019		0.5
CvB	D	8 oktober 2019		0.6

Inhoud

Inleiding

Op basis van de Algemene Verordening Gegevensbescherming (hierna: AVG) zijn scholen verplicht melding te maken van datalekken bij de Autoriteit Persoonsgegevens (hierna: AP). Het nalaten van een dergelijke melding kan leiden tot een fikse boete.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is te voldoen aan wet- en regelgeving en de informatiebeveiliging te verbeteren.

Dit protocol is van toepassing op de gehele organisatie van de Stichting Onderwijsgroep Amersfoort (hierna: OGA).

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. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Ook het verliezen van een usb-stick met bijvoorbeeld daarop de adresgegevens van klas 3b, is een datalek.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Te hanteren werkwijze

De drie rollen

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

1. **Ontdekker:** degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt. In de praktijk is dit een medewerker die zelf een beveiligingsincident of datalek opmerkt of hierop wordt gewezen door een leerling of ouder.
2. **Privacy Coördinator:** het directielid binnen de school die verantwoordelijk is voor de implementatie en toezicht op naleving van de AVG. De Privacy Coördinator is ook verantwoordelijk voor het schakelen met de technicus binnen de school die mogelijk de oorzaak van het datalek kan vinden en kan (laten) repareren. Tevens is hij/zij verantwoordelijk voor het melden van een datalek bij de Functionaris Gegevensbescherming.
3. **Functionaris Gegevensbescherming (hierna: FG):** De door het CvB aangestelde functionaris die toezicht houdt binnen de OGA op de toepassing en naleving van de AVG. Tevens is de FG de centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.

De elf stappen

Er zijn elf stappen voor de afhandeling van een beveiligingsincident c.q. datalek:

1. **Constatering beveiligingsincident**
   De Ontdekker merkt een beveiligingsincident / datalek op, via eigen waarneming of via waarneming van een derde. Hierbij kan bijvoorbeeld gedacht worden aan een melding van een ouder of externe partij die een beveiligingslek of datalek vermoed. Denk hierbij niet alleen aan bijvoorbeeld een vermoedelijke hack of een USB-stick die kwijt is, maar ook aan een telefoonlijst op papier welke kwijt is of een tas met papieren dossiers welke gestolen is.

2. **Verzamelen van informatie**

De Ontdekker verzamelt zoveel mogelijk informatie over het (online of offline) beveiligingsincident / datalek en meldt het per omgaande bij de Privacy Coördinator en bij de directie van de desbetreffende locatie.
De volgende informatie wordt minimaal aangedragen:

- Datum/periode van het beveiligingsincident.
- Aard van het beveiligingsincident.
- Wanneer van toepassing bij een datalek (zie het meldformulier Datalekken) o.a.:
    - Omschrijving van de groep betrokkenen.
    - Aantal betrokkenen.
    - Type persoonsgegevens in kwestie.

De Privacy Coördinator meldt het beveiligingsincident / datalek per ommegaande bij de Functionaris Gegevensbescherming via privacy@onderwijsgroepamersfoort.nl

3. Beoordeling van aangedragen informatie

De Privacy Coördinator en de Functionaris Gegevensbescherming bepalen of er voldoende informatie omtrent het beveiligingsincident / datalek bekend is. Zo niet, dan zeten zij aanvullende vragen uit bij de Ontdekker en/of de Technicus.

4. Opnemen incident in register beveiligingsincidenten en datalekken

De Functionaris Gegevensbescherming neemt het beveiligingsincident / datalek op in het register Beveiligingsincidenten en Datalekken en registreert hierbij in ieder geval:

- Datum van (constatering) beveiligingsincident / datalek.
- Naam van de Privacy Coördinator en de Ontdekker.
- Waar het incident heeft plaatsgevonden.
- Toedracht van het incident.
- Type persoonsgegevens
- Oorzaak van het incident (zie stap 5).
- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen (zie stap 5).
- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen.
- Wordt het datalek aan betrokkenen gemeld? Waarom niet? (Zie stap 7, 8)
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet? (zie stap 9)

5. Overleg met Technicus

De Privacy Coördinator zal in overleg met de Technicus nagaan wat de oorzaak van het incident is en welke maatregelen genomen kunnen worden om een beveiligingsincident / datalek in de toekomst te voorkomen.

6. Beoordeling van beveiligingsincident / datalek

De Functionaris Gegevensbescherming beoordeelt samen met de Privacy Coördinator de feiten (aan de hand van het datalek-formulier) om te bepalen of het beveiligingsincident aangemerkt kan worden als een datalek en of een melding aan de Autoriteit Persoonsgegevens (AP) vereist is.

Bij de beoordeling of er sprake is van een ‘meldingsplichtig datalek’ wordt rekening gehouden 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).

7. **Beoordeling meldplicht Betrokkenen**
   Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene zoals beschreven in stap zes? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers en leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgegaan dat het lekken van informatie 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 niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

8. **Informatieverstrekking Betrokkenen bepalen**
   Indien het datalek aan Betrokkenen gemeld wordt, bepaalt de Functionaris Gegevensbescherming in overleg met de Directie van de betreffende school hoe deze melding gedaan zal worden en wat de inhoud van de melding zal zijn. De CvB wordt parallel geïnformeerd.

9. **Melden**
   Indien de conclusie bij stap zes is dat er melding gedaan moet worden bij de AP (en eventueel betrokkenen), dan wordt deze melding z.s.m. gedaan. 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.

   Indien van toepassing worden de Betrokkenen geïnformeerd volgens de besluiten die in stap acht hierover zijn genomen.

10. **Toezicht maatregelen**
    Om toekomstige beveiligingsincidenten / datalekken te voorkomen, zullen de benodigde maatregelen worden genomen en uitgevoerd. De Privacy Coördinator zal de vorderingen van deze maatregelen nauwgezet volgen en de Betrokkenen opnieuw informeren wanneer de maatregelen volledig zijn genomen.

11. **Vastleggen**
    Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd in het register beveiligingsincidenten / datalekken door de Functionaris Gegevensbescherming waarmee het incident is afgesloten. De Functionaris Gegevensbescherming en Privacy Coördinator versturen een samenvatting van de genomen maatregelen aan het CvB en de directie van de desbetreffende locatie.

NB **Tussen stap 1 en stap 9 mag nooit meer dan 72 uur zitten.**

Monitoring beveiligingsincidenten en datalekken

De Functionaris Gegevensbescherming van de OGA maakt ten minste twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Het CvB, directies en de Privacy Coördinatoren van de scholen worden geïnformeerd over de uitkomsten van de analyse.

Communicatie

Elke terugkoppeling naar de Ontdekker rondom de afhandeling van een melding wordt door de directie van de school uitgevoerd. De Privacy Coördinator zal alle benodigde informatie aan de directie van de school verstrekken.
Elke vraag van de pers rondom beveiligingsincidenten / datalekken dient te worden doorgezet naar de directie van de school. De directie stemt met het CvB af wie de pers te woord staat.