Protocol beveiligingsincidenten en datalekken

Instemming door GMR:

Datum	Naam	Functie
10-12-2018	R. Kwerreveld	Voorzitter GMR

Vastgesteld door BEVOEGD GEZAG:

Datum	Naam	Functie
11-12-2018	Thea Janson	Voorzitter College van Bestuur

Inhoud

Inleiding

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

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 WIJ de Venen, zoals vermeld in het IBP–beleid, en al haar medewerkers.

Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken!

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.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt.

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’.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het bevoegd gezag.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

Werkwijze

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid (beleidsplan IBP).
- Er is een actueel reglement internet en sociale media.

De vier rollen

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt:** een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. Dit meldpunt wordt beheerd door de Privacy Officer, Astrid Kalmeijer.
3. **Melder (functionaris gegevensbescherming, afgekort FG)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens. Deze rol wordt ingevuld door Bert Dasselaar van Groenendijk Onderwijs consultancy.
4. **Technicus:** degene die de oorzaak van het datalek kan vinden en kan (laten) repareren. Deze rol wordt ingevuld door de externe systeembeheerder.

De zeven stappen

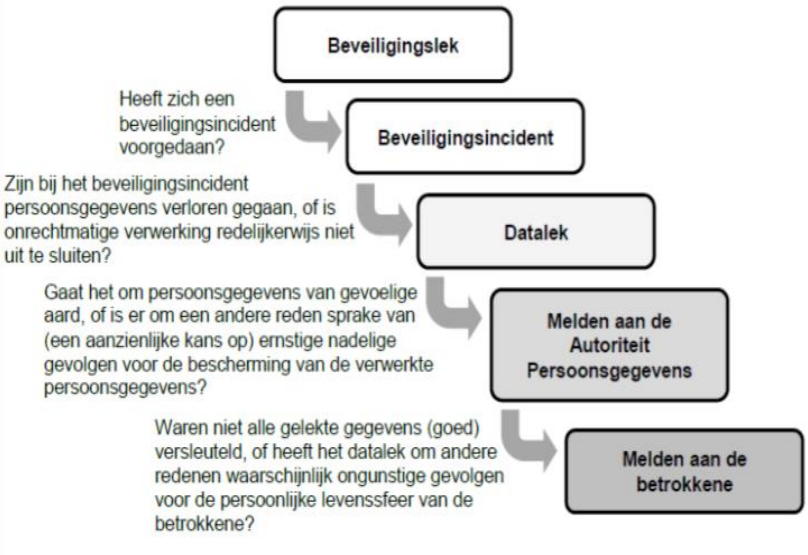
1. **Ontdekken**
   De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt via meldpuntprivacy@wijdevenen.nl. Hiervoor dient de ontdekker het formulier incidentenregistratie te gebruiken, dit formulier is te vinden op de website van WIJ de Venen.

2. **Inventariseren**
   De Privacy Officer bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet zij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd door de ontdekker/technicus i.s.m. de Privacy Officer.
   - 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 de Privacy Officer voldoende informatie heeft verzameld, en een datalek vermoedt, stuurt deze de FG een verzoek om de verzamelde informatie te bekijken. De FG 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 FG en teruggekoppeld naar de Privacy Officer.
   - 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’, houd de melder 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.

De onderstaande beslisboom dient gehanteerd te worden:



4. **Repareren**
   De externe systeembeheerder wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De externe systeembeheerder legt onderstaande vast en koppelt dit terug naar de Privacy Officer.
   - 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 FG i.s.m. de Privacy Officer dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt door de FG gemeld bij het meldloket datalekken.

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de FG. De Privacy Officer verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker, waarna het incident is afgesloten.

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 uitgegaan dat het lekken van informatie en/of data van gevoelige aard gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt, welke zijn beveiligd of versleuteld en de

gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat niet aan betrokkenen te worden gemeld.

Monitoring beveiligingsincidenten en datalekken

De Privacy Officer van WIJ de Venen 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 College van bestuur wordt geïnformeerd over de uitkomsten van de analyse.

Communicatie

- ✓ Als er sprake is van een datalek wordt het College van Bestuur direct op de hoogte gesteld. De FG verstrekt ook de benodigde gegevens ten behoeve van de communicatie.
- ✓ De betrokkene wordt in overleg met het College van Bestuur op de hoogte gebracht van het datalek.
- ✓ In de kennisgeving aan de betrokkene wordt in ieder geval vermeld: Een algemene omschrijving van de aard van het incident, de contactgegevens om meer informatie over de inbreuk te verkrijgen, en de maatregelen die genomen zijn en/of door betrokkene genomen moeten worden om negatieve gevolgen te beperken.
- ✓ Bij grootschalige datalekken dient er ook een persbericht te worden opgesteld in overleg met het College van bestuur.