Protocol informatiebeveiligingsincidenten en datalekken

SWV Helmond-Peelland PO

Inhoud

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het Informatiebeveiligings- en Privacy (IBP) beleid van SWV Helmond-Peelland PO. Deze zijn te vinden in het Team AVG en Privacy.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het leren van incidenten om uiteindelijk beveiligingsincidenten en datalekken te kunnen voorkomen. Melden moet dus gestimuleerd worden.

Dit protocol is van toepassing op de gehele organisatie van SWV Helmond-Peelland PO, dus niet alleen op medewerkers maar ook op (ingehuurde) externen, stagiaires, vrijwilligers zoals vermeld in het IBP-beleid.

Gebruikte termen:

- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.
- **Beveiligingsincident**; een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid (BIV) van de informatievoorziening wordt aangetast. Dus informatie of een applicatie is niet te gebruiken (beschikbaar/bereikbaar), de informatie klopt niet (gegevens zijn aangetast/ongeoorloofd aangepast), of (persoons)gegevens zijn beschikbaar geweest voor een onbevoegde (iemand die die gegevens niet nodig heeft, of een hacker).
- **BIV**; Beschikbaarheid (continuïteit), Integriteit (correctheid) en Vertrouwelijkheid (privacy);
- **Datalek**; een beveiligingsincident waarbij specifiek persoonsgegevens verloren raken of onrechtmatig worden verwerkt (beschikbaar, opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **IBP**; Informatiebeveiliging en Privacy.
- **Informatievoorziening**; het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht is ook het Samenwerkingsverband verplicht 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 kind-administratie, je personeels- en salarisadministratie of in digitale middelen. Als het samenwerkingsverband gebruik maakt van leveranciers die persoonsgegevens ontvangen van het samenwerkingsverband, dan moet het samenwerkingsverband met deze verwerkers aanvullende afspraken over het melden van datalekken.

Er is sprake van een Datalek als er bij een beveiligingsincident persoonsgegevens ‘verloren’ zijn gegaan of beschikbaar zijn (geweest) voor onbevoegden, óf waarbij dat niet valt uit te sluiten. Er is persoonlijke informatie ‘gelekt’. Een klassiek voorbeeld van een Datalek is het verliezen van een usb-stick met daarop gevoelige documenten, of wanneer een e-mail per ongeluk ook naar anderen dan de bedoelde ontvangers is gestuurd. Een hack waarbij een database met persoonsgegevens is gestolen, is uiteraard ook een Datalek.

De meldplicht geldt voor de Verwerkingsverantwoordelijke voor de persoonsgegevens, dat is de directeur-bestuurder. Een leverancier is een Verwerker voor het samenwerkingsverband. Bij uitzondering kan worden afgesproken dat een Verwerker **namens** de Verwerkingsverantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van de directeur-bestuurder. In de regel zal de verantwoordelijke zelf de melding moeten doen.

Als er een Datalek is, moet daar ‘onverwijld’ - dus zo snel mogelijk - maar in ieder geval binnen 72 uur na ontdekking en interne melding van het lek, melding gedaan kunnen worden gedaan bij de Autoriteit Persoonsgegevens. Of er een melding gedaan moet worden is afhankelijk van de impact. De impact dient beoordeeld en van een advies voorzien te worden door de Functionaris Gegevensbescherming.

Afspraken met leveranciers

De directeur-bestuurder moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Spreek af:

- Hoe je elkaar informeert over datalekken, en zorg ook voor bereikbaarheid op vrije dagen.
- Wie melding doet bij de Autoriteit Persoonsgegevens.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding.
- Binnen welke tijd de verwerker de gegevens moet aanleveren.
- Wie de communicatie met de betrokkenen voor haar rekening neemt, als dat nodig is.

Leg afspraken met verwerkers over datalekken schriftelijk vast. Hiervoor kan bijvoorbeeld gebruik worden gemaakt van de Model Verwerkersovereenkomst die hoort bij het Privacy convenant Onderwijs.

Werkwijze

Uitgangssituatie

- Er is een actueel Informatiebeveiligings- en Privacy beleid;
- Er is een actueel document betreffende het gebruik van bedrijfsmiddelen, ICT en internet.

De rollen

De volgende rollen worden onderscheiden om een beveiligingsincident of Datalek succesvol af te handelen:

1. **Ontdekker**; degene (medewerker, kind, ouder/verzorger of externe) die het beveiligingsincident of Datalek op het spoor komt en het proces in werking stelt. **Afspraak:** Deze persoon meldt zo snel mogelijk bij het **Meldpunt** via privacy@swv-peellandpo.nl.
2. **Meldpunt**; een centrale locatie onder beheer van de **Privacy Officer** en de **Functionaris Gegevensbescherming** waar alle incidenten worden geregistreerd en worden verwerkt. **Afspraak:** Melding Datalek gaat altijd via privacy@swv-peellandpo.nl.
3. **Functionaris Gegevensbescherming (FG)**; degene die verantwoordelijk is voor het beoordelen van het Datalek, het opstellen van het advies richting directeur-bestuurder over het nemen van correctieve en preventieve maatregelen en het eventueel melden bij Autoriteit Persoonsgegevens (AP) en betrokkene(n).
4. **Verantwoordelijke (directeur-bestuurder);** degene die verantwoordelijk is voor het beoordelen van het advies van de FG over de maatregelen, het melden bij de AP, en het inlichten van de betrokkene(n).
5. **Privacy Officer (PO)**; degene verantwoordelijk voor het zoeken naar de oorzaak van het Datalek (bijv. opvragen logging), het implementeren van de maatregelen, het adviseren over eventuele berichtgeving aan betrokkene(n), en de afstemming met de leverancier en/of ouders/verzorgers/medewerkers.

De stappen

1. **Ontdekken [via de Ontdekker]**
   De Ontdekker merkt een beveiligingsincident op via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie in het Datalek-formulier. Dit betreft in ieder geval de volgende informatie: Datum/periode van het Datalek, of het een inbreuk is op beschikbaarheid, integriteit of vertrouwelijkheid, wat er met de gegevens is gebeurd, samenvatting van het beveiligingsincident; wat voor gegevens het betreft (bijv. bijzondere gegevens of van gevoelige aard); omschrijving van de betrokkene(n) en het aantal; wat de gevolgen zijn; de ernst en de acties/maatregelen.

2. **Inventariseren [via het Meldpunt, in eerste instantie de Privacy Officer en evt. de FG]**
   Via het Meldpunt wordt bepaald of er voldoende informatie omtrent het (beveiligings)incident bekend is. Zo niet, dan volgen aanvullende vragen richting de Ontdekker en/of leverancier/betrokkenen. Als leidraad hierbij wordt gebruik gemaakt van het Datalek-formulier van de Autoriteit Persoonsgegevens.

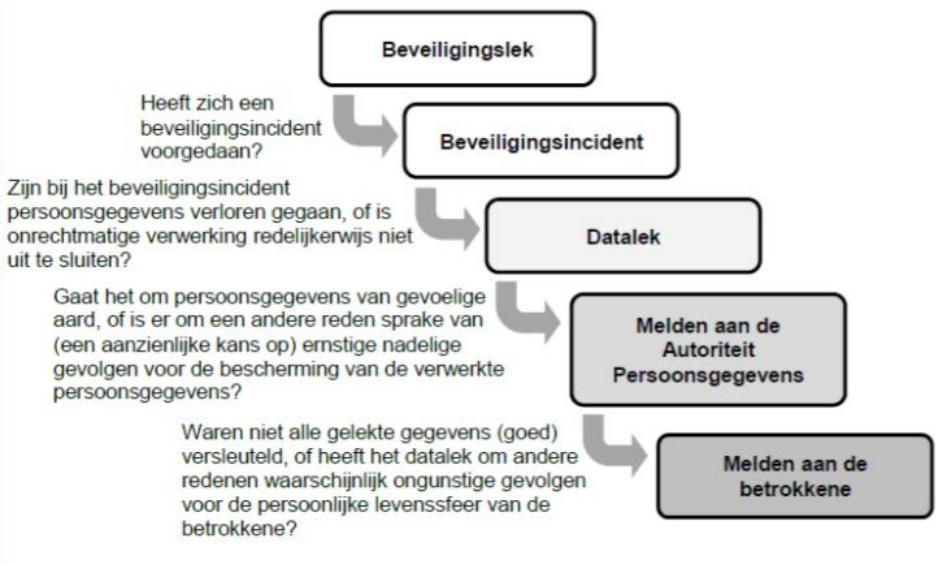
3. **Beoordelen [via de FG]**
   Op basis van de informatie bij het Meldpunt wordt door de FG bepaald of er sprake is (van een vermoeden) van een Datalek. Hij beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is, en zo ja, dan adviseert hij over de

inhoud. Vooral wanneer het advies is om niet te melden aan AP en/of betrokkenen, wordt dat goed onderbouwd.

Bij de beoordeling of er sprake is van een 'meldingsplichtig Datalek' wordt rekening gehouden met het type gegevens, met de hoeveelheid gegevens, en de impact op de betrokkene(n). Indien het Datalek leidt tot een kans op nadelige gevolgen voor de bescherming van persoonsgegevens, moet er gemeld worden.

Van die nadelige gevolgen of de kans op 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 bijzonder zijn zoals bijvoorbeeld persoonsgegevens over gezondheid, of wanneer deze gevoelig zijn, bijv. over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan pesten, uitsluiten of discriminatie).

De volgende beslisboom kan gebruikt worden



4. **Repareren [via de PO, en evt. de FG]**
   De PO wordt gevraagd te achterhalen wat de oorzaak van het (beveiligings)incident is en moet de oorzaak via maatregelen (laten) verhelpen. De PO van SWV Helmond-Peelland PO legt in ieder geval vast:
   - Welke technische en organisatorische maatregelen zijn genomen om de inbreuk te verhelpen en verdere (toekomstige) inbreuk te voorkomen? Voorgaande voor zover de oorzaak bekend is.

5. **Melden [via de FG]**

Indien op basis van het advies van de FG bij stap 3 de Verantwoordelijke besluit dat er melding gedaan moet worden bij de AP (en eventueel betrokkenen, zie stap 7), dan zal de FG dit binnen drie dagen (72 uur) na het ontdekken doen, eventueel op basis van een voorlopige melding. De melding bevat alle verzamelde informatie en de getroffen maatregelen. Het lek wordt gemeld bij het meldloket datalekken van de AP.

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan (en die in stap 7 ontstaat), wordt gearchiveerd door de het Meldpunt waarmee het incident is afgesloten, ook wanneer de Verantwoordelijke het advies van de FG niet overneemt (wat om onderbouwing vraagt). Het Meldpunt verstuurt een samenvatting naar de Ontdekker.

7. **Informeren betrokkene(n): kinderen, ouders/verzorgers, medewerkers of externen**
   Heeft het Datalek mogelijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene(n)? Dan moet het Datalek ook aan de betrokkene(n) zelf worden gemeld. Dat zijn kinderen, hun ouders/verzorgers als zij jonger zijn dan 16 jaar zijn, medewerkers of externen. Bij het informeren van de betrokkene(n) moeten een aantal vragen beantwoord worden (voor info, zie website AP). In principe kan ervan worden uitgegaan dat het lekken van persoonsgegevens gemeld moet worden bij de betrokkenen, tenzij er een hele goede reden is om dat niet te doen, bijvoorbeeld: de inspanning is onevenredig. **NB:** Wanneer persoonsgegevens zijn gelekt die zijn beveiligd of versleuteld, en de data is onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat ook 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 SWV Helmond-Peelland PO maakt minimaal een keer per jaar een analyse van de meldingen van beveiligingsincidenten en Datalekken in samenwerking met de FG. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen. De directeur-bestuurder wordt geïnformeerd over de uitkomsten van de analyse.

Communicatie

Een beveiligingsincident of Datalek met een aanzienlijke impact dient gezien te worden als een calamiteit. Daarbij dient aansluiting gezocht te worden met een Integraal Veiligheidsplan en/of een Calamiteitenplan. In het kader van mogelijke calamiteiten, is het raadzaam om vooraf bijvoorbeeld na te denken over:

- De manier van communiceren met betrokkenen en eventueel de pers.

- Hoe kan worden omgegaan met signalen van buitenaf over een mogelijk Datalek?
- Is het inschakelen van externe deskundigen gewenst?