**Procedure incidentmelding**

**Doel**

Het doel van deze procedure is omschrijven hoe

* een informatieveiligheidsincident moet worden gemeld door medewerkers van het CLB aan het aanspreekpunt
* een datalek moet worden gemeld door het aanspreekpunt (*naam aanspreekpunt van jouw CLB)* aan de functionaris voor gegevensbescherming/ informatieveiligheidsconsulent van jouw CLB die het lek meldt aan de Autoriteit Gegevensbescherming en eventueel aan de betrokkene

Een informatieveiligheidsincident kan de werking van de organisatie en/of de belangen van één of meerdere personen negatief beïnvloeden. Er bestaat een heel brede waaier van mogelijke incidenten. Herkenbare voorbeelden zijn o.m. verlies of diefstal van een laptop (en dus alle informatie die de laptop bevatte), poging tot hacking, omzeilen van de toegangscontrole,…

Het is dan ook van groot belang dat alle kwetsbaarheden, twijfels over oprechtheid van communicatie e.d., bedreigingen en incidenten zo snel mogelijk gemeld worden zodat we:

* zo snel mogelijk kunnen reageren, ingrijpen en de problemen oplossen
* er kunnen uit leren en kennis over de analyse en het oplossen van incidenten kunnen aanwenden om herhaling en impact in de toekomst te verminderen
* kunnen detecteren waarover meer uitleg en/ of bewustmaking wenselijk/noodzakelijk is
* kunnen rapporteren
* indien nodig bevoegde instanties kunnen informeren

**Definities**

Een **informatieveiligheidsincident** is elke ongewenste en/of onverwachte gebeurtenis met een betekenisvolle of mogelijke impact op de informatieveiligheid (beschikbaarheid, integriteit, vertrouwelijkheid en onweerlegbaarheid van informatie en -systemen).

Een melding over informatieveiligheid kan gaan over:

* mogelijke bedreigingen of kwetsbaarheid zonder dat er een concrete inbreuk plaatsgevonden heeft, voorbeeld: ontvangen van phishing-mail
* kwetsbaarheid of voorval waaruit schade ontstaan is, voor het CLB of andere partijen (personen, organisaties, overheden,…), voorbeeld: verlies van laptop met persoonsgegevens op

**Een datalek** is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4.12 Algemene Verordening Gegevensbescherming)

**Verantwoordelijkheden en bevoegdheden**

* Iedere medewerker van het CLB is verplicht informatieveiligheidsincidenten en datalekken te melden.
* Het aanspreekpunt informatieveiligheid (*naam aanspreekpunt van jouw CLB)* is verantwoordelijk om deze gebeurtenissen op te volgen, oplossingen te zoeken door de juiste personen te betrekken, te registreren en te rapporteren
* De functionaris voor gegevensbescherming/informatieveiligheidsconsulent van jouw centrum meldt een datalek aan de Autoriteit Gegevensbescherming
* Bij een datalek met zware gevolgen voor de betrokkene informeert de directeur van het CLB de betrokkene.

**Doelgroep**

Deze procedure is van toepassing op personeelsleden (ook personeelsleden die een tijdelijke opdracht opnemen, bv. stagiairs,…)

**Middelen**

Incidentenregister

Mailadres om incidenten te melden:

Telefoonnummer om incidenten te melden:

*Formulier melden incidenten*

**Referenties**

Algemene Verordening Gegevensbescherming (VERORDENING (EU)　2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)<http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679>)

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken>

**Werkwijze**

* 1. **Melden beveiligingsincidenten door de medewerker**

Een medewerker merkt een kwetsbaarheid of incident of wordt hierop geattendeerd door een andere/externe persoon.

De medewerker verwittigt zo snel mogelijk het aanspreekpunt (*naam aanspreekpunt van jouw CLB)* via ….( hoe/kanaal).

Bij de incidentmelding is het de bedoeling volgende gegevens te verzamelen:

* **Datum** van melding
* **Wie** meldt het incident
* **Soort gebeurtenis + omschrijving**

**Wat** heeft zich voorgedaan?: Omschrijving van de bedreiging/kwetsbaarheid of het incident. Zijn er persoonsgegevens betrokken?

* **Wie is betrokken?**

Zelf ontdekt of op geattendeerd door extern persoon (bv. persoon meldt dat hij mail met vertrouwelijke info ontvangen heeft die niet voor hem bestemd was)

Op wie slaat het?: Bv. enkel de persoon die meldt, een deel van de medewerkers, of op meerdere personen over verschillende diensten,…

* **Wanneer** heeft de gebeurtenis zich voorgedaan?

**Wat is de** **frequentie** (bv. éénmalig, meermaals,…)?

* **Locatie** waar de gebeurtenis zich heeft voorgedaan
* **Wat zijn de gevolgen/schade?**
* **Zijn er persoonsgegevens bij betrokken?**
* **Is er sprake van een datalek? Zo ja:**
* Omschrijving van de groep betrokkenen
* Aantal betrokkenen
* Soort persoonsgegevens
* Aantal persoonsgegevens
* Waarschijnlijke gevolgen
* Genomen maatregelen
* **Zijn er al maatregelen genomen na het vaststellen van de gebeurtenis?** : vb. de laptop werd onmiddellijk van het netwerk gekoppeld, wifi werd uitgeschakeld, de kabel werd uitgetrokken, geen specifieke acties ondernomen maar ik heb de computer niet meer aangeraakt,…
* **Bijlagen**: Stuur indien mogelijk **bijlagen** door (bv. in de vorm van screenshots)

Het aanspreekpunt probeert te achterhalen wat de oorzaak is en hoe die verholpen moet worden. Vervolgens start de behandeling van het incident.

De melder krijgt een terugkoppeling dat de melding behandeld wordt.

Na afsluiten ontvangt de melder bericht dat de melding afgesloten werd.

De melder wordt op de hoogte gebracht (zonder detaillering) wat ondernomen werd en waarom.

Alle informatie betreffende het incident en de organisatorische en technische maatregelen die genomen zijn om het incident te verhelpen en verder te voorkomen worden vastgelegd in het incidentenregister.

**2. Melden van datalekken aan de Autoriteit Gegevensbescherming en eventueel aan betrokkene**

In de Algemene Verordening Gegevensbescherming is een meldplicht van datalekken opgenomen. Het nalaten van melden kan leiden tot sancties door de Gegevensbeschermingsautoriteit.

Van een　datalek　is sprake als een beveiligingsincident heeft plaatsgevonden, waarbij persoonsgegevens verloren zijn gegaan of niet is uit te sluiten dat persoonsgegevens in handen van derden zijn gevallen. Daarbij is niet relevant of een beveiligingsincident opzettelijk of per ongeluk heeft plaatsgevonden.

Als een organisatie voor de beveiliging van de systemen een verouderde versie van antivirussoftware gebruikt, is nog geen sprake van een　datalek, wel van een informatieveiligheidsincident. Maar zodra vervolgens een virusbesmetting van de systemen tot gevolg heeft dat persoonsgegevens (van bijvoorbeeld leerlingen) toegankelijk zijn geworden voor derden, is wel sprake van een　datalek. Een ander voorbeeld van informatieveiligheidssincidenten waarbij sprake kan zijn van een　datalek, is een e-mail verzonden aan een verkeerde geadresseerde, het vergeten in de trein van een niet-versleutelde USB-stick met persoonsgegevens,…

**2.1. Melden datalek aan de Autoriteit Gegevensbescherming**

Het aanspreekpunt (*naam aanspreekpunt van jouw CLB)* meldt de inbreuk zo snel mogelijk aan de functionaris voor gegevensbescherming/informatieveiligheidsconsulent en de verwerkingsverantwoordelijke van het centrum (directeur).

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de functionaris voor gegevensbescherming/informatieveiligheidsconsulent van jouw CLB dit zo snel mogelijk en uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de Gegevensbeschermingsautoriteit.

Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, moet hiervoor een motivering voor de vertraging worden meegegeven.

De inbreuk moet niet worden gemeld als het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van de betrokkene.

De melding van het datalek aan de autoriteit gegevensbescherming gebeurt via de procedure van de toezichthoudende autoriteit.

In de melding wordt ten minste het volgende medegedeeld:

* de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en type persoonsgegevens in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevens in kwestie
* de naam en de contactgegevens van de functionaris voor gegevensbescherming/informatieveiligheidsconsulent of een ander contactpunt (het aanspreekpunt) waar meer informatie kan worden verkregen
* de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens
* de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Het aanspreekpunt documenteert dit in het incidentenregister.

Die documentatie stelt de Gegevensbeschermingsautoriteit in staat de naleving van de meldplicht te controleren.

**3. Melden datalek aan de betrokkene**

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke (directeur) de inbreuk in verband met persoonsgegevens onmiddellijk mee aan de betrokkene.

De mededeling aan de betrokkene bevat

* een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens
* de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt (directeur) waar meer informatie kan worden verkregen
* de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

* De verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling
* De verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen
* De mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten.