

Protocol Informatiebeveiligingsincidenten en datalekken PCSV

Bron

Kennisnet

Vastgesteld door PCSV:

Versie	Datum	Naam	Functie
0.11	25-11-2021	Nancy Tebrugge	GMR (instemming)

Inhoud

Inleiding	2
Wet- en regelgeving datalekken	2
Afspraken met leveranciers	3
Werkwijze	3
Uitgangssituatie.....	3
De vier rollen	3
De zeven stappen	3
Monitoring beveiligingsincidenten en datalekken.....	5
Interne en externe communicatie bij datalekken.....	5
Intern	5
Extern	5

Inleiding

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

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 de PCSV, zoals vermeld in het IBP beleid en al haar medewerkers.

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, et cetera). 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 organisaties verplicht melding te maken van datalekken bij de AP. Het nalaten van deze melding kan leiden tot een fikse boete. Sinds 28 mei 2018 is de meldplicht onderdeel van de Algemene Verordening Gegevensbescherming (AVG).

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in je leerlingadministratie of digitale leermiddelen. Wanneer de school gebruik maakt van derden bij het uitvoeren van haar diensten en daarbij persoonsgegevens uitwisselt moet zij daarover afspraken maken met die partijen. Deze afspraken kunnen betrekking hebben op het handelen bij (mogelijke) datalekken. Zorg voor duidelijke afspraken over de wijze waarop gecommuniceerd wordt en dat duidelijk is welke partij waarvoor verantwoordelijk is.

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. Er is persoonlijke informatie 'gelekt'. Een datalek hoeft niet te betekenen dat er kwaad opzet in het spel is. De meeste datalekken (90% van de gevallen) wordt veroorzaakt door foutief menselijk handelen (denk aan het kwijtraken van laptops of USB-sticks).

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is het Toezichthoudend Bestuur van PCSV. Met dit protocol wordt beoogt de gehele organisatie te instrueren zodat het bestuur eventuele datalekken correct kan afhandelen, al dan niet met ondersteuning van een locatiemanager of –directeur.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens. Afhankelijk van de aard van het lek en de gelekte gegevens kan het nodig zijn om de betrokkenen te informeren.

Afspraken met leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Spreek af:

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatie gegevens de verwerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de verwerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Maak schriftelijke afspraken met verwerker(s) over datalekken. Hiervoor kan gebruik worden gemaakt van de model bewerkersovereenkomst die hoort bij het convenant "Digitale onderwijsmiddelen en privacy" (www.privacyconvenant.nl).

Werkwijze

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en/of gedragscode ict en internetgebruik.

De vier rollen

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

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming of privacy officer)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (ict medewerker/ict coördinator/leverancier)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

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 info@pcsv.nl

2. Inventariseren

Het Meldpunt 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 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 het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoedt, 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.

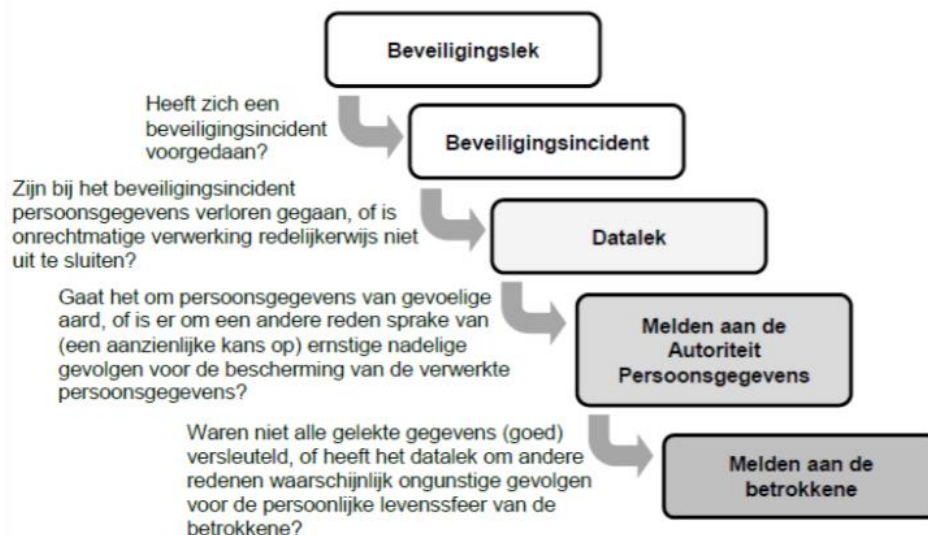
De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen.
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom 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’, hou je 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 gelect zijn, maar ook wanneer de gelecte 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 kan gebruikt worden



4. Repareren

De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van de PCSV 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 gelekke 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 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>. Het meldingsformulier is openbaar en neem eens een kijkje welke informatie er eigenlijk nodig is om een datalek te melden. Dan ben je voorbereid als dat ooit nodig mocht zijn.

6. Vastleggen

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 uitgegaan dat het lekken van gevoelige aard gelek gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelek maar die zijn beveiligd of versleuteld, en de gelekke 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.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van de PCSV 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 schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.

Interne en externe communicatie bij datalekken

Intern

Het meldpunt licht de directie en de FG in als er een melding binnenkomt. Vanaf dat moment treedt dit protocol in werking en komen het privacyteam en de FG in actie. Intern komt de communicatie dan ook vanuit het privacyteam of de directie. Het is uiteindelijk de directie die bepaalt of een melding aan de AP en/of betrokkenen moet worden gedaan. De FG geeft hierover advies.

Extern

Communicatie naar buiten toe, inclusief de melding aan betrokkenen, gaat vanuit de directeur-bestuurder die daarvoor verantwoordelijk is. Er dienen standaard brieven ter beschikking te staan van de organisatie die naar

verschillende partijen verstuurd kunnen worden in het geval van een datalek. Deze brieven kunnen slechts ter informatie worden verstuurd of om te voldoen aan de wettelijke meldplicht.

Wanneer derden (bijvoorbeeld de pers, maar ook klanten) inlichtingen vragen omtrent veiligheidsincidenten en/of datalekken wordt er alleen vanuit de directie hierop gereageerd. Het is medewerkers niet toegestaan hier uitlatingen over te doen. Vraag om de juiste contactgegevens en geef aan dat er later door een woordvoerder contact met hen wordt opgenomen.