PCPO Barendrecht en Ridderkerk

Protocol informatiebeveiligingsincidenten en datalekken
PCPO Barendrecht en Ridderkerk

Inhoud

Inleiding

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

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 PCPO Barendrecht en Ridderkerk, 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 ook scholen verplichting 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 leerlingadministratie of digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze bewerkers aanvullende afspraken over het melden van datalekken.

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 klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

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

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 bewerker 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 bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Maak schriftelijke afspraken met uw bewerker(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 (security officer/ict coördinator)**; 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 privacy@pcpobr.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

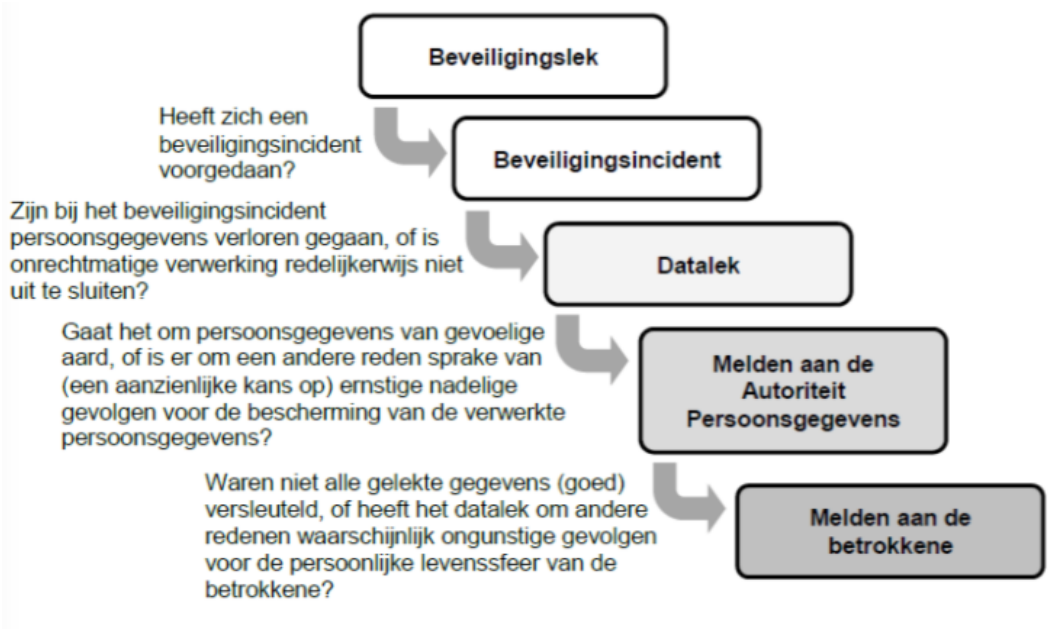
Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.

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 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).

De onderstaande beslisboom kan gebruikt worden (volgende pagina)



4. **Repareren**
   De Technicus (intern of extern) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen.
   De technicus van PCPO Barendrecht en Ridderkerk, eventueel in samenspraak met Cloudwise, 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 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 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 gelekt 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 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 PCPO Barendrecht en Ridderkerk 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.

Communicatie

Als er gecommuniceerd moet worden geschiedt dit in overleg met de betrokkenen. Het verdient aanbeveling om met elkaar goede afspraken te maken over wat/hoe/wanneer er gecommuniceerd wordt en door wie.
Voorts is het goed om in een plan een afspraak te maken over een mogelijk lek dat er van buiten de organisatie wordt gemeld.
Kan me voorstellen dat de (op te richten PR-groep) daar tezamen met bestuur en privacy officer bij betrokken worden.

Bijlage: Begrippen

AVG:	Algemene Verordening Gegevensbescherming.
WBP:	Wet Bescherming Persoonsgegevens.
Persoonsgegeven:	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“betrokkene”).
Betrokkene:	De persoon/personen van wie de persoonsgegevens zijn gelekt.
Beveiligingsincident:	Een beveiligingsincident is een gebeurtenis die zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
Datalek:	Een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, etc.) NB: Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
Informatievoorziening:	Het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van betrokkenen en organisatie.
Autoriteit:	Autoriteit Persoonsgegevens
Verantwoordelijke:	De verantwoordelijke stelt het doel van en de middelen voor de verwerking van persoonsgegevens vast. Dat wil zeggen de gemeente of (openbare of privaatrechtelijke) rechtspersoon waar de school onder valt: het bevoegd gezag. Wanneer er in dit reglement gesproken wordt over de Verantwoordelijke dan wordt daarmee het bevoegd gezag van PCPO Barendrecht en Ridderkerk bedoeld.
School:	PCPO Barendrecht en Ridderkerk
Verwerker:	Een natuurlijke of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verantwoordelijke persoonsgegevens verwerkt.

Bijlage: Artikel 33 en 34 AVG

Artikel 33 AVG

"Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit"

1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

2. De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

3. In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:
a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
d) 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.

4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

5. De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

Artikel 34 AVG

"Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene"

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

2. De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.

3. De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:
a) 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; ,

b) de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;

c) 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.

4. 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 of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan.

Voorbeelden

Datalekken melden aan de Autoriteit Persoonsgegevens

- ❏ Intern wordt binnen school gesignaleerd dat door een haperende beveiliging (technische storing) gegevens zijn ingezien door onbevoegden.
- ❏ Een medewerker verliest een laptop met onversleutelde persoonsgegevens.
- ❏ Een school krijgt te maken met een hack waarbij leerlinggegevens en wachtwoorden zijn ontvreemd.
- ❏ Een journalistiek programma confronteert een organisatie met het feit dat als gevolg van een beveiligingslek onder andere persoonlijke gegevens (zoals kopieën van id-bewijzen, bankgegevens en wachtwoorden) van werknemers op de server van het bedrijf door onbevoegden zijn ingezien;
- ❏ Vier laptops zijn gestolen bij een school. De laptops bevatten gevoelige gegevens over gezondheid en welzijn en andere persoonsgegevens van kinderen/ouders/begeleiders.
- ❏ Een medewerker geeft zijn login/wachtwoordgegevens aan een derde partij gegeven die daardoor nagenoeg onbeperkt bij alle gegevens kan komen.
- ❏ Een internetprovider biedt de gebruikers de mogelijkheid om details van hun account te zien, zoals onder andere historische zoekgegevens en vaak bezochte websites. Door een fout in de website had een ieder via een simpele truc de mogelijkheid om de accounts van andere gebruikers vrijelijk in te zien. Zonder een sluitende logging is hier niet vast te stellen of dat daadwerkelijk is gebeurd en welke gegevens dan zijn geraadpleegd.

Gebeurtenissen die niet onder de meldplicht vallen

- ❏ Een brief met daarin persoonsgegevens wordt naar een foutief adres gestuurd, en wordt ongeopend retour gezonden.
- ❏ Iemand laat een koffer met daarin persoonsgegevens achter in de trein/bus. De koffer is voorzien van een deugdelijk slot, en komt via 'gevonden voorwerpen' ongeopend terug bij de rechtmatige eigenaar.
- ❏ Het zoekraken of hacken van de ledenadministratie van een sportvereniging zal doorgaans leiden tot het nodige ongemak voor vereniging en leden, maar zal niet snel aanleiding geven tot een melding bij de Autoriteit Persoonsgegevens. Dit kan overigens anders liggen als de sportvereniging zich bijvoorbeeld richt op personen met een specifieke levensovertuiging of seksuele geaardheid, of als er fraudegevoelige gegevens gelekt zijn.
- ❏ Als ziekenhuispersoneel gebruik maakt van het wachtwoord van een arts om toegang te krijgen tot medische persoonsgegevens, dan is er niet zo zeer sprake van een datalek, als van schending van interne voorschriften. In eerste instantie liggen dan disciplinaire maatregelen voor de hand.