AVG-beleid

Bijlage 1: Protocol Datalekken

Datum: februari 2023
Directeur-bestuurder: Peter Schutte
Vastgesteld in GMR op: 11-04-2023

Onderwijsgroep Buitengewoon

Protocol Datalekken

Inleiding

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 alle scholen van Onderwijsgroep Buitengewoon zoals vermeld in het IBP-beleid.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die ervoor 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 school.
- **Datalek;** een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt zoals 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 scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Vanaf 25 mei 2018 is dit opgenomen in de Algemene Verordening Persoonsgegevens (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in het leerling administratiesysteem, salarispakket, mail 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 verwerkers aanvullende afspraken over het melden van datalekken.

Beveiligingsincident datalek

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’.

Voorbeelden van beveiligingsincidenten zijn:

- Verlies of diefstal van waardepapier, dossier, usb-stick, tablet of andere gegevensdragers
- Niet naleven van beleid of richtlijnen
- Inbreuk op fysieke beveiligingsvoorzieningen
- Toegangsovertredingen
- Opzettelijk foutief handelen (fraude, diefstal)
- Beschadigen of vernielen van (kritische) apparatuur
- Virusbesmetting als gevolg van het aanklikken van een onbetrouwbare bijlage
- Onbevoegd inzien van vertrouwelijke informatie
- Onbedoelde openbaarmaking van vertrouwelijke informatie
- Geen gescreend personeel
- Illegale licenties
- Illegaal kopiëren van gegevens
- E-mail met niet versleutelde vertrouwelijke informatie
- Kenbaar maken van of onzorgvuldig omgaan met wachtwoorden

Maar ook cyberaanvallen zoals een DDoS, computer hacking of besmetting met ransomware of het technische falen van apparatuur, stroomuitval, wateroverlast en dergelijke zijn aan te merken als incidenten.

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.
   1.1. **Ontdekker** (externe); een ouder of verwerker die een beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt** (Functionaris Gegevensbescherming); het aanspreekpunt waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder** (Functionaris Gegevensbescherming); degene die in opdracht van de verwerkingsverantwoordelijke, de Directeur-bestuurder de melding van een datalek bij de Autoriteit Persoonsgegevens doet.
4. **Technicus** (ICT-Coördinator, Bovenschoolse ICT-Coördinator, Applicatiebeheerder of externe ICT-dienstverlener); degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is de Directeur-bestuurder. Een leverancier is een verwerker voor de school. De FG doet in overleg met de verantwoordelijke, de Directeur-bestuurder, de melding.

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

De 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, de Functionaris Gegevensbescherming via j.schildwacht@cedgroep.nl én informeert daarnaast de directeur en ICT-Coördinator van de eigen school. De Functionaris Gegevensbescherming informeert de Bovenschoolse ICT-Coördinator en de Directeur-bestuurder.

2. Inventariseren

Het Meldpunt bepaalt aan de hand van een formulier 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 in het formulier 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 betrokkene
  - Aantal betrokkene
  - Type persoonsgegevens in kwestie

- Worden de gegevens binnen een keten gedeeld

3. Beoordelen

Wanneer er voldoende informatie is verzameld en een datalek wordt vermoed, beoordeelt de FG in samenwerking met de Bovenschoolse ICT-Coördinator de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkenen vereist is.

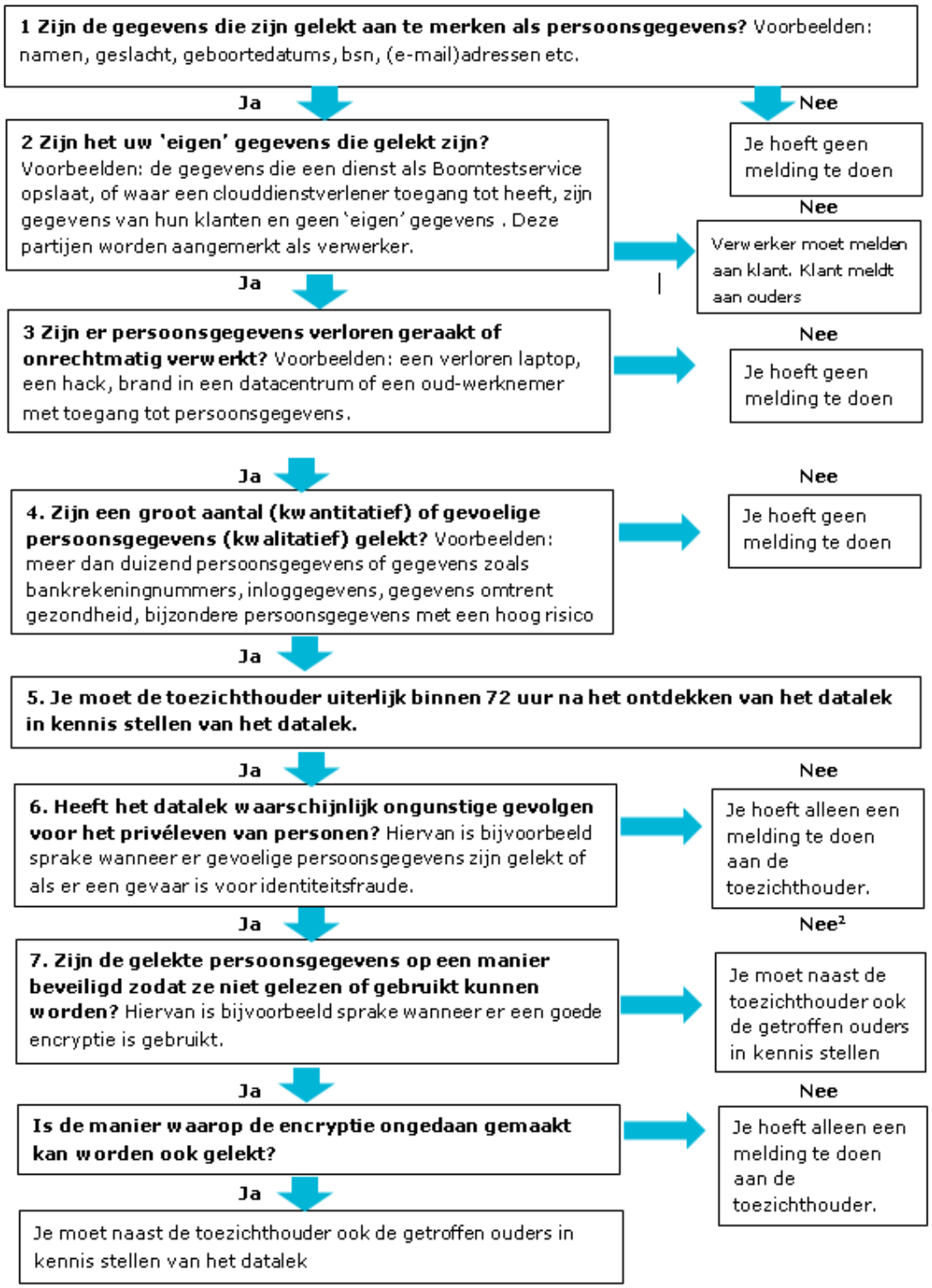
De volgende informatie wordt vastgelegd door de Functionaris Gegevensbescherming (FG):

- Impact van de melding
- Welk type gegevens er verloren gegaan zijn
- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene
- Aard van de inbreuk
- Gaat het om gegevens die uitbesteed zijn aan een verwerker
- Aantal betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkene gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?
- Wordt er melding gedaan via de Pers?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', wordt er rekening gehouden 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.

Jaarlijks worden zowel de Raad van Toezicht als de GMR ingelicht over het aantal meldingen en de genomen maatregelen. Indien er sprake is van een ernstig en of 'groot' datalek zal de Raad van toezicht en de GMR eerder ingelicht worden.

De beslisboom op de volgende pagina kan worden gebruikt:



4. Repareren

De Bovenschoolse ICT-Coördinator wordt gevraagd te (laten) achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De Functionaris Gegevensbescherming 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)?

4.1. Herstelaanpak datalekken

Bij de herstelaanpak wordt rekening gehouden met de volgende twee vragen:

- Hoe herstel je de schade bij betrokkene?
  - Wat kun je doen om betrokkenen te ondersteunen in het beperken van de schade door een datalek?
  - Op welke wijze ga je deze nazorg leveren?
  - Wie worden hierbij betrokken? *(Denk aan ICT-Coördinator, Bovenschoolse ICT-Coördinator, directeur, beleidsmedewerker communicatie, leverancier, Directeur-bestuurder, HRM)*
- Hoe herstel van de schade van de school?
  - Op welke wijze kan de schade van de school beperkt blijven dan wel hersteld worden?
  - Wie worden hierbij betrokken? *(Bovenschoolse ICT-Coördinator. beleidsmedewerker communicatie, leverancier, MT en Directeur-bestuurder, HRM)*
  - Maakt het datalek de uitvoering van een bedrijfsproces onmogelijk en bestaat daarvoor een alternatieve werkwijze?
  - Wat voor acties ga je ondernemen om de reputatieschade te beperken en om de reputatie te herstellen?
  - Wat voor acties ga je ondernemen rondom de afwikkeling van aansprakelijkheidsstelling en boetes?
  - Welke acties worden ondernomen ter voorkomen en communicatie aan medewerkers?

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 Functionaris Gegevensbescherming (FG) dit binnen 72 uur in overleg met de Directeur-bestuurder 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/

6. Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de Functionaris Gegevensbescherming (FG) waarmee het incident is afgesloten. De FG verstuurt een samenvatting van de genomen maatregelen naar de Directeur-bestuurder en de Bovenschoolse ICT-Coördinator.

7. Informeren betrokkene

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkene zelf worden gemeld. Dat zijn medewerkers en leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgaan dat lekken van gevoelige aard gemeld moeten 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.

8. Stappenplan

Onderstaande stappen wordt gebruikt voor communicatie naar de medewerkers.

	Procedurestap	Termijn	Wie
1	**Beveiligingsincident** • Verlies USB-stick • Verlies tablet, smartphone, laptop • Verzending naar verkeerd mailadres • Verlies dossier • Onbevoegde die toegang had tot netwerk of bestand • Phishing • Hacking	Direct	Ontdekker lek
1	**Beveiligingsincident** melden bij ICT-Coördinator, Functionaris Gegevensbescherming (FG), Bovenschoolse ICT-Coördinator en directeur	Direct	Ontdekker lek
1a	Indien telefoon verloren etc. direct gaan blokkeren (ook privé telefoon)	Direct	Ontdekker lek Applicatiebeheerder
1b	Ook persoonsgegevens gelekt? Dan ook melden bij Functionaris Gegevensbescherming (FG) en eigen ICT-Coördinator en directeur	Direct	Ontdekker lek
2	In behandeling nemen beveiligingsincident	Direct	FG
3	Beoordelen	Direct	FG/Bovenschoolse ICT-Coördinator
3a	Informeren Directeur-bestuurder over datalek	Direct	FG
3b	Beoordelen of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) 1. Of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) 2. Of betrokkene(n) wiens gegevens gelekt zijn geïnformeerd moet(en) worden 3. Of er actie ondernomen moet worden naar derden: • Informatie • Maatregelen • Onderzoek 4. Of de RvT e/o GMR geïnformeerd moeten worden 5. Of externe communicatie nodig is	Binnen 72 uur na ont-dekken van lek	FG in overleg met: • Bovenschoolse ICT-Coördinator • Directeur-bestuurder
4	Maatregelen treffen om datalek te stoppen	Direct	Bovenschoolse ICT-Coördinator i.o.m. FG
4a	Informeren bestuurder over stand van zaken en beoordeling	Binnen 72 uur	FG
5	Bij meldingsplichtig datalek: melden bij AP via meldloket: https://datalekken.autoriteitpersoonsgegevens.nl/	Binnen 72 uur	FG i.o.m. Directeur-bestuurder
6	Registeren datalek	Direct	FG
7	Als betrokkene(n) wiens gegevens gelekt zijn geïnformeerd moet(en) worden, versturen kennisgeving met vermelding van: • Aard inbreuk • Contactgegevens • De maatregelen die betrokkene kan nemen om negatieve gevolgen te beperken Afhankelijk van de omvang van het datalek overwegen om andere kanalen in te zetten.	Zo snel mogelijk, uiterlijk binnen 72 uur	FG in overleg met Bovenschoolse ICT-Coördinator FG in overleg met Directeur-bestuurder

	Procedurestap	Termijn	Wie
7a	Externe communicatie (indien nodig)	Zo snel mogelijk	Directeur-bestuurder / FG en beleidsmedewerker communicatie
7b	Controle op effectiviteit van de afhandeling van incidenten en datalekken per kwartaal	PO	Per kwartaal
7c	Jaarlijkse rapportage over aantal datalekken aan RvT en (G)MR	Per jaar	Via Directeur-bestuurder