SAMENWERKINGSVERBAND VO/VSO
MIDDEN-HOLLAND & RIJNSTREEK

1. 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 de organisatie van swv v(s)o Midden-Holland Rijnstreek, zoals vermeld in het IBP-beleid en al haar medewerkers.

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 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.

2. Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn organisaties verplicht om 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. Als de organisatie gebruik maakt van leveranciers, die persoonsgegevens ontvangen van de organisatie, dan moet de organisatie met deze verwerkers aanvullende afspraken maken over het melden van datalekken.

3. 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 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
- Email met onversleutelde vertrouwelijke informatie
- Kenbaar maken van of onzorgvuldig omgaan met wachtwoorden

Maar ook cyberaanvallen zoals een ddos, computerhacking of besmetting met ransomware , of het technisch 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.

4. 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** (de manager IBP); een aanspreekpunt binnen de organisatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder** (Functionaris voor Gegevensbescherming); degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus** (Security Officer of externe ict-dienstverlener); degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

5. 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 via de mail of mondeling.

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 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 Functionaris voor Gegevensbescherming (FG) een verzoek om de verzamelde informatie te bekijken. De FG beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.

SAMENWERKINGSVERBAND VO/VSO
MIDDEN-HOLLAND & RIJNSTREEK

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

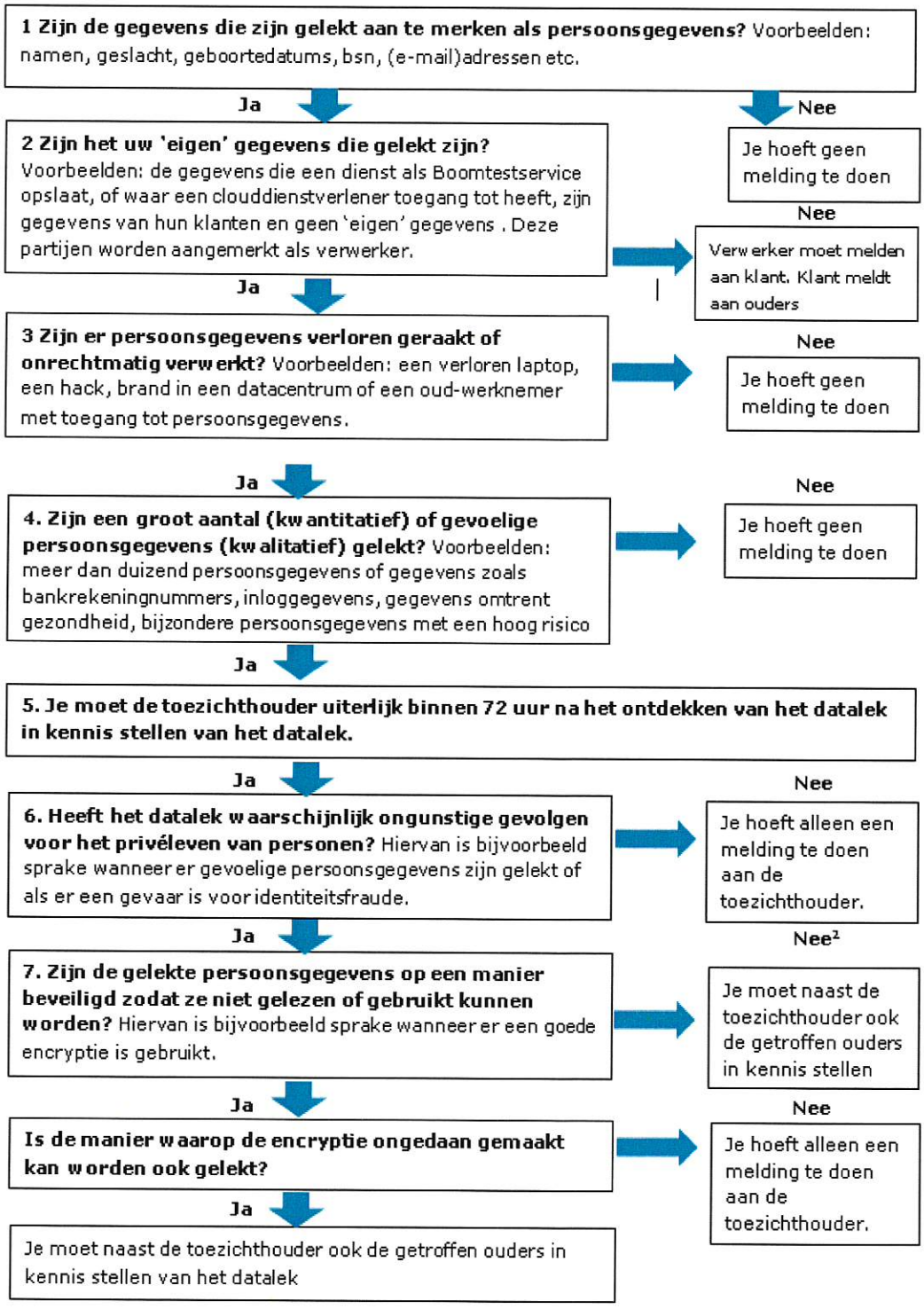
- Impact van de melding
- Welk type gegevens er verloren gegaan zijn
- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene
- Aard van de inbreuk
- Gaat het om gegevens die uitbesteed zijn aan een verwerker
- Aantal betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen 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 Algemene Vergadering als de OPR ingelicht over het aantal meldingen en de genomen maatregelen. Indien er sprake is van een ernstig en of 'groot' datalek zullen de Algemene Vergadering en de OPR eerder ingelicht worden.

De beslisboom op de volgende pagina kan worden gebruikt:

SAMENWERKINGSVERBAND VO/VSO
MIDDEN-HOLLAND & RIJNSTREEK



SAMENWERKINGSVERBAND VO/VSO
MIDDEN-HOLLAND & RIJNSTREEK

4. Repareren

De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De Technicus 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 betrokkenen?
  - 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?
- Hoe herstel van de schade van de organisatie?
  - Op welke wijze kan de schade van de organisatie beperkt blijven dan wel hersteld worden?
  - Wie worden hierbij betrokken?
  - 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 voorkoming van herhaling en t.a.v. 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 voor 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/actionpage?0.

6. Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de Functionaris voor Gegevensbescherming (FG) waarmee het incident is afgesloten. De FG verstuurt een samenvatting van de genomen maatregelen aan de directeur-bestuurder en hij communiceert deze naar de Ontdekker.

7. Informeren betrokkenen

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 niet aan

SAMENWERKINGSVERBAND VO/VSO
MIDDEN-HOLLAND & RIJNSTREEK

betrokkene te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

6. Stappenplan

Onderstaande stappen wordt gebruikt voor communicatie naar de medewerkers.

	Procedurestap	Termijn	Wie
1	**Beveiligingsincident** • Verlies USB stick • Verlies iPad, smartphone, laptop • Verzending naar verkeerd mailadres • Verlies dossier • Onbevoegde die toegang had tot netwerk of bestand • Phishing • Hacking		Ontdekker lek
1	**Beveiligingsincident** melden bij de manager IBP, mw. Hardenbol	Direct	Ontdekker lek
1a	Indien telefoon verloren etc. direct gaan blokkeren (ook privé telefoon)	Direct	Ontdekker lek/ manager IBP
1b	Ook persoonsgegevens gelekt? Dan ook melden bij functionaris gegevensbescherming (FG) FG: CED groep Rotterdam, Mw. van der Horst	Direct	Ontdekker lek / manager IBP
2	In behandeling nemen beveiligingsincident	Direct	FG
3	Maatregelen treffen om datalek te stoppen	Direct	Manager IBP i.o.m. FG
3a	Informeren directeur-bestuurder over datalek	Direct	FG
4	Beoordelen: 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 Algemene Vergadering e/o OPR geïnformeerd moeten worden 5. Of externe communicatie nodig is	Binnen 72 uur na ont-dekken van lek	FG in overleg met: • Medewerker /Manager IBP
5	Informeren directeur-bestuurder over stand van zaken en beoordeling	Binnen 72 uur	FG
6	Bij meldingsplichtig datalek: melden bij AP via meldloket: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0	Binnen 72 uur	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	Zo snel mogelijk, uiterlijk binnen 72 uur	FG in overleg met medewerker / Manager IBP die gegevens verwerkt

SAMENWERKINGSVERBAND VO/VSO
MIDDEN-HOLLAND & RIJNSTREEK

	Afhankelijk van de omvang van het datalek overwegen om andere kanalen in te zetten.		
7a	Externe communicatie (indien nodig)	Zo snel mogelijk	Manager IBP, Directeur-bestuurder /FG
7b	Controle op effectiviteit van de afhandeling van incidenten en datalekken per kwartaal	FG	Per kwartaal
7c	Jaarlijkse rapportage over aantal datalekken aan Algemene Vergadering en OPR	Per jaar	FG iom directeur-bestuurder

Aldus vastgesteld, na positief advies van de Medezeggenschapsraad "personeel", door de directeur-bestuurder d.d. 16 oktober 2018

B.B. Verkerk, directeur-bestuurder