Brabantse Wal

Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

Protocol datalekken

Samenwerkingsverband Brabantse Wal VO

Vastgesteld door Samenwerkingsverband Brabantse Wal VO

Versie	Datum	Naam	Functie
1.0	9 juli 2020	T. J. van Rijzewijk	Directeur-bestuurder
2.0	1-3-2022	T. J. van Rijzewijk	Directeur-Bestuurder
2.0	11-4-2022	E. van den Bosch	Ondersteuningsplanraad

T.J. van Rijzewijk
Directeur-bestuurder

E. van den Bosch
Voorzitter Ondersteuningsplanraad

Brabantse Wal

Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

Inhoud

Brabantse Wal
Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

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 binnen Samenwerkingsverband Brabantse Wal VO ('het samenwerkingsverband') zoals vermeld in het Informatiebeveiligings en Privacy Beleid (IBP-beleid) en van toepassing op alle 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 school.
- **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 samenwerkingsverbanden verplicht 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 het leerling administratiesysteem, salarispakket of digitale leermiddelen. Als het samenwerkingsverband gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van het samenwerkingsverband, dan moet het samenwerkingsverband 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
- Ook cyberaanvallen zoals een ddos, computerhacking 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 IBP-beleid;
- Er is een actuele gedragscode voor het aanvaardbaar gebruik van bedrijfsmiddelen, 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.
   Ontdekker (extern): een ouder of verwerker die een beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt**: de melding zal intern worden opgepakt door de beleidsmedewerker(s) kwaliteitszorg en/of de directeur-bestuurder (in combinatie met de Functionaris voor Gegevensbescherming). Zij zijn de eerste aanspreekpunten binnen het samenwerkingsverband die ervoor zorgdragen dat 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** (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 Raad van Bestuur. Een leverancier is een verwerker voor het samenwerkingsverband. De verwerkingsverantwoordelijke ((directeur-)bestuurder) doet de melding. De verwerker kan een melding doen, echter dit is dan afgesproken met de verwerkingsverantwoordelijke.

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

Brabantse Wal
Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

De stappen

De te nemen stappen bij een (vermoedelijk) datalek zijn opgenomen in de 'Instructiekaart en stroomschema datalekken', zoals hieronder.

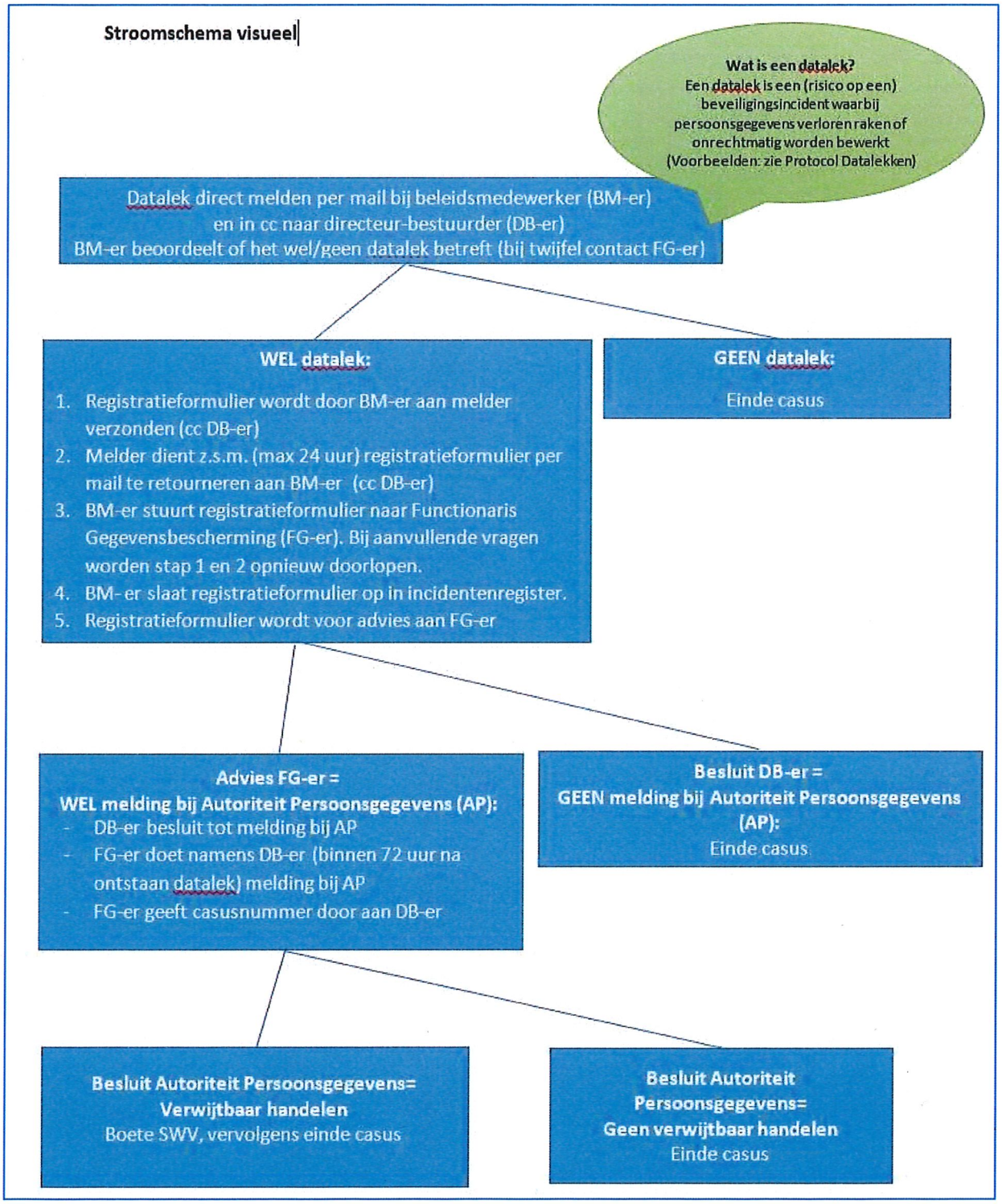
BM-er = Beleidsmedewerker
AVG-er = Verantwoordelijke AVG-beleid (= beleidsmedewerker)
DB-er = Directeur-bestuurder
FG-er = Functionaris gegevensbescherming

Stroomschema tekstueel:

- Melding datalek door melder bij BM-er via telefoon → vervolgens altijd ook per mail (incl. cc. DB-er)
  - Als het zeker geen datalek betreft: einde casus
- BM-er neemt bij twijfel contact op met Functionaris Gegevensbescherming (FG-er). Indien:
  - Nee, casus wordt afgesloten.
  - Ja, registratieformulier wordt door BM-er aan melder verzonden (cc. naar DB-er).
- Melder vult registratieformulier in en stuurt het terug naar BM-er
- BM-er stuurt registratieformulier door naar FG-er
  - Geen aanvullende vragen FG-er
  - Wel aanvullende vragen FG-er: formulier komt nog een keer terug bij melder via AVG-er
- Definitief ingevuld registratieformulier wordt opgeslagen in incidentenregister SWV PO of VO door BM-er → komt op agenda expertiseteam PO of werkoverleg VO
- Definitief ingevuld registratieformulier wordt verzonden naar FG-er
- FG-er adviseert aan DB-er:
  - Geen melding bij Autoriteit Persoonsgegevens (AP), einde casus
  - Melding bij Autoriteit Persoonsgegevens (AP) namens DB-er → melding casusnummer bij DB-er door FG-er.
- AP besluit:
  - Verwijtbaar handelen→ boete SWV PO of VO→ einde casus
  - Geen verwijtbaar handelen: einde casus

Brabantse Wal
Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

Stroomschema visueel



Vervolg na proces datalek

Repareren
Het Meldpunt binnen het samenwerkingsverband probeert te achterhalen wat de oorzaak van het beveiligingsincident is en zal de oorzaak (laten) verhelpen. Onderstaande wordt door hem vastgelegd:

- 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)?

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

- Hoe herstel van 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? *(Denk aan marketing, leverancier, bestuurder, HRM.)*
- Hoe herstel van de schade van het samenwerkingsverband?
  - Op welke wijze kan de schade van het samenwerkingsverband beperkt blijven dan wel hersteld worden?
  - Wie worden hierbij betrokken? *(Denk aan marketing/communicatie, leverancier, 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 voorkoming en communicatie aan medewerkers?

Vastleggen
Alle informatie die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de Functionaris voor Gegevensbescherming waarmee het incident is afgesloten. De Functionaris voor Gegevensbescherming verstuurt een samenvatting van de genomen maatregelen aan de beleidsmedewerker kwaliteitszorg en de directeur-bestuurder en laatstgenoemde stuurt door naar de Ontdekker.

Informeren betrokkenen
Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers en leerlingen (of hun ouders c.q. wettelijk vertegenwoordigers 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.

Brabantse Wal
Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

Bijlage 1 : Registratieformulier datalek/melding beveiligingsincident

Registratieformulier datalek/melding beveiligingsincident

Intern nummer:	
Tijdstip melding:	
Naam melder:	
Locatie melding:	
Inhoud melding:	
Impact eerste inschatting:	☐ Klein ☐ Middel ☐ Groot
AVG of telecommunicatiewet:	☐ AVG ☐ Telecommunicatiewet
Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie?	☐ Ja ☐ Nee
Indien Ja, welke organisatie:	
In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?	
Aard van de inbreuk:	☐ Inbreuk op de vertrouwelijkheid van de gegevens ☐ Inbreuk op de integriteit van de gegevens ☐ Inbreuk op de beschikbaarheid van de gegevens
Wat is de aard van de incident?	☐ Apparaat, gegevensdrager (B.v. USB stick en of papier met persoonsgegevens kwijtgeraakt of gestolen ☐ Brief Postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen ☐ Hacking, malware (bijv Ransomware) en/of Phishing ☐ Overig ☐ Persoonsgegevens bij oud papier gezet ☐ Persoonsgegevens mondeling gedeeld met onbevoegde ontvanger ☐ Persoonsgegevens nog aanwezig op afgedankt apparaat of afgedankte gegevensdrager (bv usb stick)

	☐ Persoonsgegevens per ongeluk gepubliceerd ☐ Persoonsgegevens van verkeerde klant getoond in klantportaal ☐ Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger.
Persoonsgegevens die betrokken zijn bij het datalek:	☐ Naam-, adres- en woonplaatsgegevens ☐ Geslacht, geboortedatum en/of leeftijd ☐ Burgerservicenummer (BSN) ☐ Contactgegevens ☐ Toegangs- of identificatiegegevens ☐ Financiële gegevens ☐ Paspoortkopieën of kopieën van andere legitimatiebewijzen ☐ Locatiegegevens ☐ Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. ☐ Onbekend/anders nl:
Bijzondere categorieën van persoonsgegevens.	☐ Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt ☐ Persoonsgegevens waaruit iemands politieke opvattingen blijken ☐ Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken ☐ Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt ☐ Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid ☐ Gegevens over iemands gezondheid ☐ Genetische gegevens ☐ Biometrische gegevens
Hoeveelheid persoonsgegevens? (bij benadering hoeveel gegevensrecords)	
De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek.	☐ Werknemers ☐ Klanten (huidig en potentieel) ☐ Leerlingen of studenten ☐ Patiënten ☐ Minderjarige

	☐ Personen uit kwetsbare groepen
Omschrijving van de groep personen.	
Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	
Maatregelen die zijn getroffen voordat het datalek plaatsvond.	Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden? ☐ Ja ☐ Nee
Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om welk deel gaat dat dan?	
Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens. Gevolgen van het datalek	☐ Onbevoegde hebben kennis kunnen nemen van de gegevens ☐ De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt ☐ Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt ☐ Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties ☐ Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen ☐ Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen ☐ Anders, namelijk:
Lichamelijke, materiële en immateriële schade voor de betrokkenen.	☐ Discriminatie ☐ Identiteitsdiefstal of fraude ☐ Financiële verliezen ☐ Reputatieschade

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?	☐ Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens ☐ Ongeoorloofde ongedaanmaking van pseudonimisering ☐ Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen ☐ Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen ☐ Andere gevolgen namelijk:
Geef een inschatting van de ernst van de mogelijke gevolgen door betrokkenen	☐ Verwaarloosbaar ☐ Beperkt ☐ Aanzienlijk ☐ Zeer groot
Tijdstip melding aan FG van datalekken; tijd, datum en door wie:	
Meldingen aan directeur-bestuurder; tijd, datum en door wie:	
Beoordeling of er sprake is van een datalek	
Onderzoeksvragen:	
Is er sprake van een datalek?	
Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?	
Melding gemaakt bij Meldloket Autoriteit Persoonsgegevens?	☐ Nee ☐ Ja **Meldingsnummer:**
Indien Nee, waarom niet?	
Indien Ja: Datalek melden aan betrokkenen	☐ **Ja**

Informeren van de betrokkenen	Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? ☐ Ja ☐ Nee
Wanneer heeft u het datalek gemeld aan de betrokkenen?	
Wanneer gaat u het datalek melden aan de betrokkenen?	
Wat is de inhoud van de melding aan de betrokkenen?	
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	
Waarom ziet u af van het melden van het datalek aan de betrokkenen?	☐ De maatregelen die ik heb getroffen voordat de datalek plaatsvond bieden voldoende bescherming om de melding aan betrokkenen achterwege te kunnen laten. ☐ Het zou onevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren ☐ Ik heb na het datalek maatregelen getroffen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkenen.
Als het informeren van alle betrokkenen een onevenredige inspanning zou vergen, licht dan toe hoe u door een openbare mededeling of een soortgelijke maatregel de betrokkenen gaat informeren.	

Brabantse Wal
Samenwerkingsverband passend onderwijs
Voortgezet onderwijs

Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?	
Welke andere redenen heeft u om de betrokkenen niet te informeren?	
Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?	
Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de Autoriteit Persoonsgegevens voor deze verwerking de leidende toezichthouder?	☐ Nee ☐ Ja
Verdere opmerkingen:	

Afgerond Datum: Tijd:

Door: Angela Groen, CED-Groep
Functie: Functionaris voor Gegevensbescherming Samenwerkingsverband Brabantse Wal VO