

Brabantse Wal

Samenwerkingsverband passend onderwijs

PROTOCOL DATALEKKEN

Samenwerkingsverband passend onderwijs Brabantse Wal PO

Vastgesteld door Samenwerkingsverband Brabantse Wal PO

Versie	Datum	Naam	Functie
1.0	10.02.2021	Mevr. H. Persoon	Directeur-bestuurder
	10.02.2021	Mevr. P. Pellis	Voorzitter OPR

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 binnen Samenwerkingsverband Brabantse Wal PO ('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.

2. 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 leerlingadministratiesysteem, 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.

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 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 onversleutelde 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.

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.
Ontdekker (extern): een ouder of verwerker die een beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt** (privacy@swvbrabantsewal.nl en telefoonnummer 0164-745091): 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 directeur-bestuurder. Een leverancier is een verwerker voor het samenwerkingsverband. De verwerkingsverantwoordelijke directeur-bestuurder doet de melding of delegeert dit naar de beleidsmedewerker Kwaliteitszorg en AVG. 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.

5. De stappen

a. 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 dit bij het Meldpunt door een e-mail te sturen naar privacy@swvbrabantsewal.nl. Tevens neemt de ontdekker telefonisch contact op met het samenwerkingsverband op telefoonnummer 0164-745091 om de beleidsmedewerker kwaliteitszorg en/of de directeur-bestuurder te informeren.

b. Inventariseren

Het Meldpunt bepaalt aan de hand van een formulier (zie bijlage bij dit protocol) 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.

c. Beoordelen

Wanneer het Meldpunt voldoende informatie heeft verzameld en een datalek vermoedt, stuurt het Meldpunt de Functionaris voor Gegevensbescherming een verzoek om de verzamelde informatie te bekijken. De Functionaris voor Gegevensbescherming beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkene(n) vereist is.

De volgende informatie wordt vastgelegd door de Functionaris voor Gegevensbescherming:

- Impact van de melding
- Welk type gegevens er verloren gegaan zijn
- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- 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?

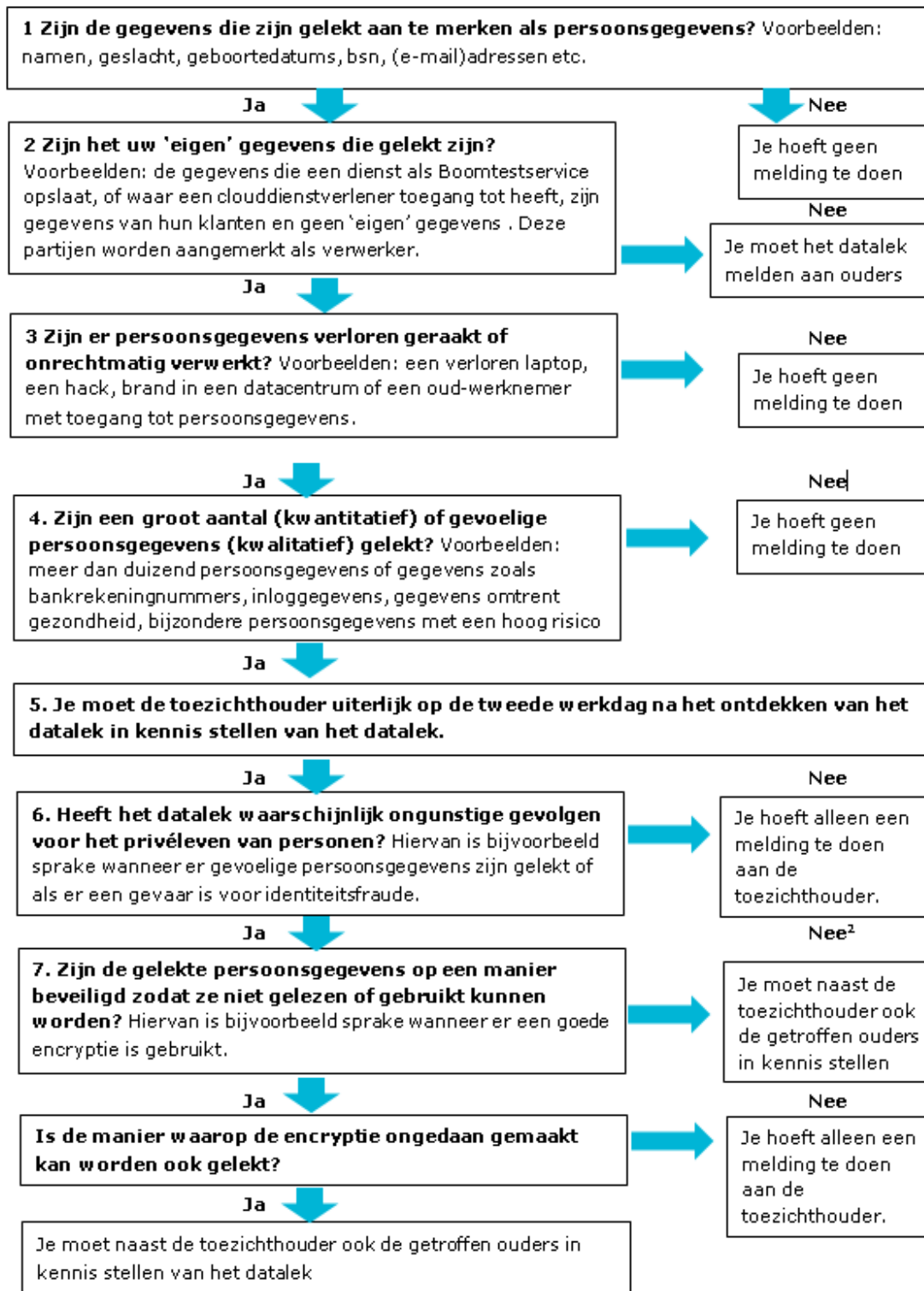
Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', wordt er rekening gehouden met het type gegevens, en met de hoeveelheid gegevens.

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 betrokkenen of als de gegevens kunnen leiden tot stigmatisering van de betrokkenen.

Jaarlijks worden zowel de Raad van Toezicht als de Ondersteuningsplanraad (de OPR) ingelicht over het aantal meldingen en de genomen maatregelen. Indien er sprake is van een ernstig en of 'groot' datalek zullen de Raad van Toezicht en de OPR eerder ingelicht worden.

De beslisboom op de volgende pagina kan worden gebruikt.



d. 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?

e. Melden

Indien de conclusie is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Functionaris voor Gegevensbescherming dit binnen 72 uur in overleg met de 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>.

f. 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.

g. 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.

6. Stappenplan

Onderstaande stappen worden gebruikt voor communicatie naar de medewerkers.

	Procedurestap	Termijn	Wie
1	Beveiligingsincident <ul style="list-style-type: none"> • 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 via privacy@swvbrabantsewal.nl en stel telefonisch de beleidsmedewerker kwaliteitszorg en/of directeur-bestuurder op de hoogte.	Direct	Ontdekker lek
1a	Indien telefoon verloren etc. direct gaan blokkeren (ook privételefoon als deze voor het werk gebruikt wordt en persoonsgegevens kan bevatten).	Direct	Beleidsmedewerker kwaliteitszorg / directeur-bestuurder of, indien niet direct bereikbaar, Ontdekker zelf
1b	Ook persoonsgegevens gelekt? Dan ook melden bij Functionaris voor Gegevensbescherming. Voor Samenwerkingsverband Brabantse Wal PO is dat mevrouw A. Groen-Vendrig (CED-Groep), 010-4071993 of a.groen@cedgroep.nl .	Direct	Ontdekker lek / beleidsmedewerker kwaliteitszorg / directeur-bestuurder
2	In behandeling nemen beveiligingsincident.	Direct	Functionaris voor Gegevensbescherming
3	Maatregelen treffen om datalek te stoppen.	Direct	Beleidsmedewerker kwaliteitszorg en/of directeur-bestuurder, met Functionaris voor Gegevensbescherming
3a	Informereren directeur-bestuurder over datalek.	Direct	Functionaris voor Gegevensbescherming ¹
4	Beoordelen of: <ol style="list-style-type: none"> 1. Er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens 2. Betrokkene(n) wiens gegevens gelekt zijn geïnformeerd moet(en) worden 	Binnen 72 uur na ont-	Functionaris voor Gegevensbescherming in overleg met beleidsmedewerker

¹ Samenwerkingsverband Brabantse Wal PO is dusdanig kleinschalig dat de directeur-bestuurder veelal reeds op de hoogte en/of betrokken zal zijn van/bij het beveiligingsincident, dan wel door de betreffende Ontdekker/medewerker of de beleidsmedewerker kwaliteitszorg betrokken zal worden.

	<p>3. Er actie ondernomen moet worden naar derden:</p> <ul style="list-style-type: none"> • Informatie • Maatregelen • Onderzoek <p>4. De Raad van Toezicht e/o Ondersteuningsplanraad geïnformeerd moeten worden</p> <p>5. Externe communicatie nodig is</p>	dekken van lek	kwaliteitszorg en/of directeur-bestuurder
5	Informeren directeur-bestuurder over stand van zaken en beoordeling.	Binnen 72 uur	Functionaris voor Gegevensbescherming
6	Bij meldingsplichtig datalek: melden bij Autoriteit Persoonsgegevens via meldloket: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage .	Binnen 72 uur	Functionaris voor Gegevensbescherming
7	<p>Als betrokkene(n) wiens gegevens gelekt zijn geïnformeerd moet(en) worden, versturen kennisgeving met vermelding van:</p> <ul style="list-style-type: none"> • Aard inbreuk • Contactgegevens • De maatregelen die betrokkene kan nemen om negatieve gevolgen te beperken. <p>Afhankelijk van de omvang van het datalek overwegen om andere kanalen in te zetten.</p>	Zo snel mogelijk, uiterlijk binnen 72 uur	Functionaris voor Gegevensbescherming in overleg met beleidsmedewerker kwaliteitszorg en/of directeur-bestuurder
7a	Externe communicatie (indien nodig)	Zo snel mogelijk	Directeur-bestuurder/ Functionaris voor Gegevensbescherming en PR/communicatie
7b	Controle op effectiviteit van de afhandeling van incidenten en datalekken	Per kwartaal	Functionaris voor Gegevensbescherming
7c	Jaarlijkse rapportage over aantal datalekken aan Raad van Toezicht en Ondersteuningsplanraad	Per jaar	Functionaris voor Gegevensbescherming i.o.m. directeur-bestuurder

Bijlage:

Registratieformulier datalek/melding beveiligingsincident:

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

	<input type="checkbox"/> Persoonsgegevens van verkeerde klant getoond in klantportaal <input type="checkbox"/> Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger.
Persoonsgegevens die betrokken zijn bij het datalek:	<input type="checkbox"/> Naam-, adres- en woonplaatsgegevens <input type="checkbox"/> Geslacht, geboortedatum en/of leeftijd <input type="checkbox"/> Burgerservicenummer (BSN) <input type="checkbox"/> Contactgegevens <input type="checkbox"/> Toegangs- of identificatiegegevens <input type="checkbox"/> Financiële gegevens <input type="checkbox"/> Paspoortkopieën of kopieën van andere legitimatiebewijzen <input type="checkbox"/> Locatiegegevens <input type="checkbox"/> Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. <input type="checkbox"/> Onbekend/anders nl:
Bijzondere categorieën van persoonsgegevens.	<input type="checkbox"/> Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt <input type="checkbox"/> Persoonsgegevens waaruit iemands politieke opvattingen blijken <input type="checkbox"/> Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken <input type="checkbox"/> Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt <input type="checkbox"/> Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid <input type="checkbox"/> Gegevens over iemands gezondheid <input type="checkbox"/> Genetische gegevens <input type="checkbox"/> Biometrische gegevens
Hoeveelheid persoonsgegevens? (bij benadering hoeveel gegevensrecords)	
De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek.	<input type="checkbox"/> Werknemers <input type="checkbox"/> Klanten (huidig en potentieel) <input type="checkbox"/> Leerlingen of studenten <input type="checkbox"/> Patiënten <input type="checkbox"/> Minderjarige <input type="checkbox"/> 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.	<p>Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?</p> <input type="checkbox"/> Ja <input type="checkbox"/> Nee
Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om welk deel gaat dat dan?	
<p><i>Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.</i></p> <p>Gevolgen van het datalek</p>	<input type="checkbox"/> Onbevoegde hebben kennis kunnen nemen van de gegevens <input type="checkbox"/> De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt <input type="checkbox"/> Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt <input type="checkbox"/> Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties <input type="checkbox"/> Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen <input type="checkbox"/> Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen <input type="checkbox"/> Anders, namelijk:
<p><i>Lichamelijke, materiële en immateriële schade voor de betrokkenen.</i></p> <p>Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?</p>	<input type="checkbox"/> Discriminatie <input type="checkbox"/> Identiteitsdiefstal of fraude <input type="checkbox"/> Financiële verliezen <input type="checkbox"/> Reputatieschade <input type="checkbox"/> Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens <input type="checkbox"/> Ongeoorloofde ongedaanmaking van pseudonimisering <input type="checkbox"/> Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen <input type="checkbox"/> Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen <input type="checkbox"/> Andere gevolgen namelijk:

Geef een inschatting van de ernst van de mogelijke gevolgen door betrokkenen	<input type="checkbox"/> Verwaarloosbaar <input type="checkbox"/> Beperkt <input type="checkbox"/> Aanzienlijk <input type="checkbox"/> 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?	<input type="checkbox"/> Nee <input type="checkbox"/> Ja Meldingsnummer:
Indien Nee, waarom niet?	
Indien Ja: Datalek melden aan betrokkenen	<input type="checkbox"/> Ja
Informeren van de betrokkenen	Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? <input type="checkbox"/> Ja <input type="checkbox"/> 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?	<input type="checkbox"/> De maatregelen die ik heb getroffen voordat de datalek plaatsvond bieden voldoende bescherming om de melding aan betrokkenen achterwege te kunnen laten. <input type="checkbox"/> Het zou onevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren <input type="checkbox"/> 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.	
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?	<input type="checkbox"/> Nee <input type="checkbox"/> Ja
Verdere opmerkingen:	

Afgerond d.d. tijd:

Door:

Functie: Functionaris voor Gegevensbescherming