STICHTING
Openbaar Onderwijs
WIJK BIJ DUURSTEDE

Waar kinderen belangrijk zijn!

Datalekken protocol

Versie	Datum
2.0	10-11-2021

INHOUD

1 Inleiding

Het Datalekken protocol is gebaseerd op het model van Kennisnet (2016) herzien in 2021 en sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van Stichting Openbaar Onderwijs Wijk bij Duurstede.

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 Stichting Openbaar Onderwijs Wijk bij Duurstede.

Definities:

- **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 schools verplichting melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Vanaf 25 mei 2018 is dit opgenomen in de Algemene Verordening Persoonsgegevens (AVG). 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.

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:

A. Verlies of diefstal van waardepapier, dossier, usb-stick, tablet of andere gegevensdragers
B. Niet naleven van beleid of richtlijnen
C. Inbreuk op fysieke beveiligingsvoorzieningen
D. Toegangsovertredingen
E. Opzettelijk foutief handelen (fraude, diefstal)
F. Beschadigen of vernielen van (kritische) apparatuur
G. Virusbesmetting als gevolg van het aanklikken van een onbetrouwbare bijlage
H. Onbevoegd inzien van vertrouwelijke informatie
I. Onbedoelde openbaarmaking van vertrouwelijke informatie
J. Geen gescreend personeel
K. Illegale licenties
L. Illegaal kopiëren van gegevens
M. Email met onversleutelde vertrouwelijke informatie
N. Kenbaar maken van of onzorgvuldig omgaan met wachtwoorden

Maar 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.

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 directeur en de bureaumanager); een aanspreekpunt binnen de school waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder** (Functionaris voor Gegevensbescherming); degene die in opdracht van de verwerkingsverantwoordelijke de melding van een datalek bij de Autoriteit Persoonsgegevens doet.
4. **Technicus** (Security Officer 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 Voorzitter College van Bestuur. Een leverancier is een verwerker voor de school. De FG doet in overleg met de verantwoordelijke (bestuurder) de melding De verwerker kan een melding doen, echter dit is dan afgesproken met de verantwoordelijke.

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

5 De stappen

5.1 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 (eigen directeur en bureaumanager: secr@obswijk.nl).

5.2 Inventariseren

Het Meldpunt/De bureaumanager 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:

A. Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
B. Datum/periode van het beveiligingsincident
C. Aard van het beveiligingsincident
D. Wanneer van toepassing (bij een datalek):

- Omschrijving van de groep betrokkene
- Aantal betrokkene
- Type persoonsgegevens in kwestie
- Worden de gegevens binnen een keten gedeeld

5.3 Beoordelen

Wanneer het Meldpunt (bureaumanager) 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 betrokkene vereist is.

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

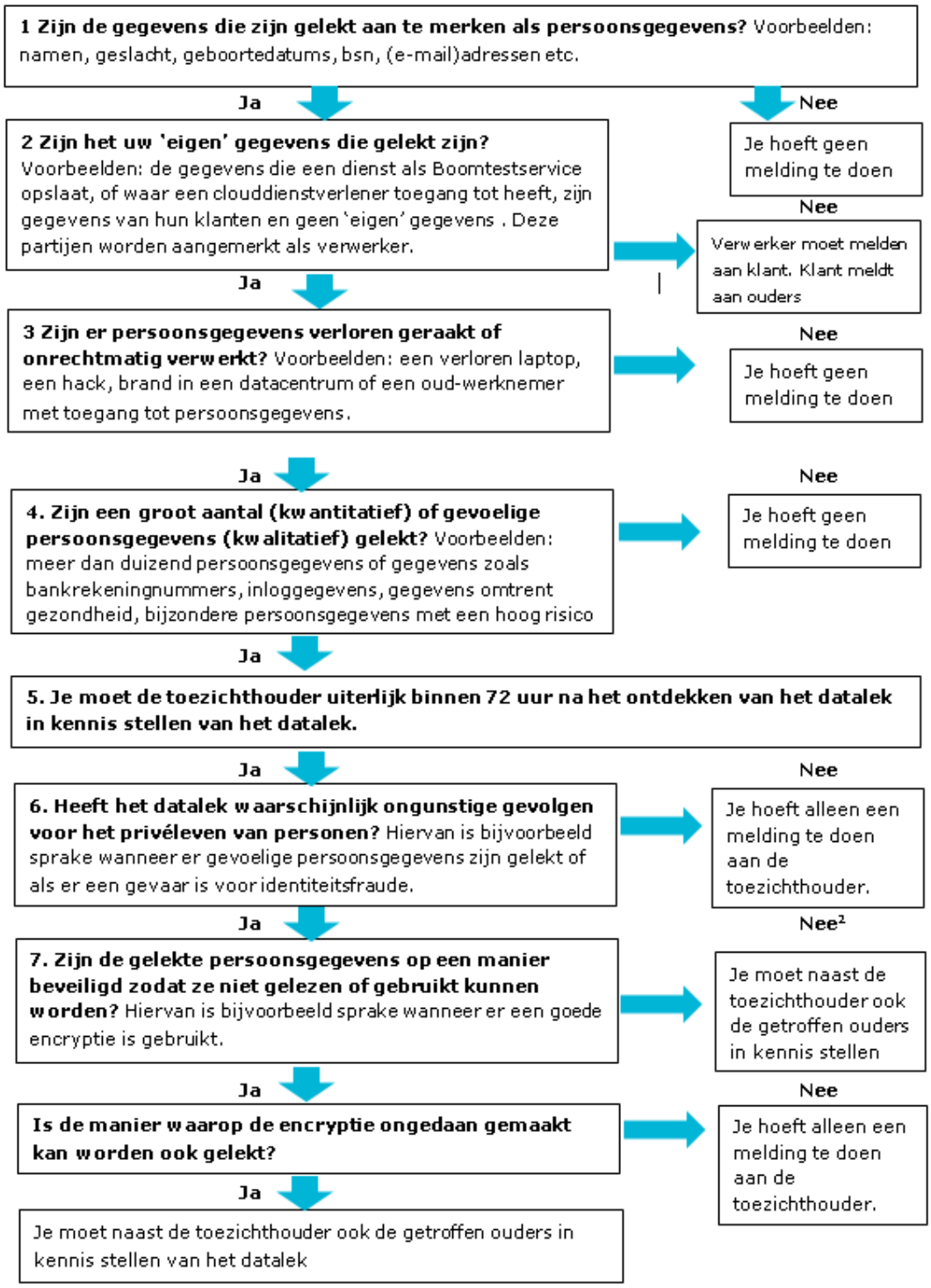
A. Impact van de melding
B. Welk type gegevens er verloren gegaan zijn
C. Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene
D. Aard van de inbreuk
E. Gaat het om gegevens die uitbesteed zijn aan een verwerker
F. Aantal betrokkenen
G. Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
H. Wordt het datalek aan betrokkene gemeld? Waarom niet?
I. Hoe worden meldingen gedaan? Wat is de inhoud van de melding?
J. 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:


1 Zijn de gegevens die zijn gelekt aan te merken als persoonsgegevens? Voorbeelden: namen, geslacht, geboortedatums, bsn, (e-mail)adressen etc.
Ja
Nee
Je hoeft geen melding te doen
2 Zijn het uw 'eigen' gegevens die gelekt zijn? Voorbeelden: de gegevens die een dienst als Boomtestservice opslaat, of waar een clouddienstverlener toegang tot heeft, zijn gegevens van hun klanten en geen 'eigen' gegevens . Deze partijen worden aangemerkt als verwerker.
Nee
Verwerker moet melden aan klant. Klant meldt aan ouders
Ja
3 Zijn er persoonsgegevens verloren geraakt of onrechtmatig verwerkt? Voorbeelden: een verloren laptop, een hack, brand in een datacentrum of een oud-werknemer met toegang tot persoonsgegevens.
Nee
Je hoeft geen melding te doen
Ja
4. Zijn een groot aantal (kwantitatief) of gevoelige persoonsgegevens (kwalitatief) gelekt? Voorbeelden: meer dan duizend persoonsgegevens of gegevens zoals bankrekeningnummers, inloggegevens, gegevens omtrent gezondheid, bijzondere persoonsgegevens met een hoog risico
Nee
Je hoeft geen melding te doen
Ja
5. Je moet de toezichthouder uiterlijk binnen 72 uur na het ontdekken van het datalek in kennis stellen van het datalek.
Ja
6. Heeft het datalek waarschijnlijk ongunstige gevolgen voor het privéleven van personen? Hiervan is bijvoorbeeld sprake wanneer er gevoelige persoonsgegevens zijn gelekt of als er een gevaar is voor identiteitsfraude.
Nee
Je hoeft alleen een melding te doen aan de toezichthouder.
Ja
7. Zijn de gelekte persoonsgegevens op een manier beveiligd zodat ze niet gelezen of gebruikt kunnen worden? Hiervan is bijvoorbeeld sprake wanneer er een goede encryptie is gebruikt.
Nee[2]
Je moet naast de toezichthouder ook de getroffen ouders in kennis stellen
Ja
Is de manier waarop de encryptie ongedaan gemaakt kan worden ook gelekt?
Nee
Je hoeft alleen een melding te doen aan de toezichthouder.
Ja
Je moet naast de toezichthouder ook de getroffen ouders in kennis stellen van het datalek

5.4 Repareren

De Security Officer wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De Security Officer legt onderstaande vast:

A. Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
B. 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 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 marketing, leverancier, 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? *(marketing/communicatie, leverancier, MT en 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?

5.5 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 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.

5.6 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 bureaumanager en deze stuurt door naar de Ontdekker.

5.7 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 betrokkene.
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 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 bureaumanager en direct leidinggevende	Direct	Ontdekker lek
1 a	Indien telefoon verloren etc. direct gaan blokkeren (ook privé telefoon)	Direct	Security Officer
1 b	Ook persoonsgegevens gelekt? Dan ook melden bij functionaris gegevensbescherming (FG) FG: Marion van der Horst (m.vanderhorst@cedgroep.nl)	Direct	Ontdekker lek/ Security Officer/ Directeur
2	In behandeling nemen beveiligingsincident	Direct	FG
3	Beoordelen	Direct	SO/FG
3 a	Informeren bestuurder over datalek	Direct	FG
3 b	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: • Medewerker /Directeur • Direct leidinggevende • Bestuurder
4	Maatregelen treffen om datalek te stoppen	Direct	Security Officer i.o.m. FG
4	Informeren bestuurder over stand van zaken en	Binnen	FG

a	beoordeling	72 uur	
5	Bij meldingsplichtig datalek: melden bij AP via meldloket: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0	Binnen 72 uur	FG i.o.m bestuurder
6	Registeren datalek	Direct	SO/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 medewerker/ directeur dat gegevens verwerkt FG in overleg met bestuurder
7 a	Externe communicatie (indien nodig)	Zo snel mogelijk	Bestuurder/ directeur /FG en PR/communicatie
7 b	Controle op effectiviteit van de afhandeling van incidenten en datalekken per kwartaal	FG	Per kwartaal
7 c	Jaarlijkse rapportage over aantal datalekken aan RvT en GMR	Per jaar	via bestuurder

7 (Preventieve) beschermingsmaatregelen

Indien het Datalek Onderzoeksteam heeft vastgesteld dat er preventieve beschermingsmaatregelen genomen moeten worden om de (mogelijke) gevolgen van het (mogelijke) datalek in een vroegtijdig stadium te beperken, komen -afhankelijk van de aard en omvang van het lek- de volgende maatregelen in aanmerking:

- het veranderen van toegangscodes en wachtwoorden voor apparaten en/of systemen en/of het blokkeren van (een) account(s);
- de wachtwoorden van computeraccounts en Office365 worden in ieder geval 1 x per jaar gewijzigd.
- het zoeken/opsporen van het verloren/gestolen (deel van een) goed/apparaat;
- het op afstand leegmaken van de e-mail van mobiele apparatuur (remote wipe);
- het isoleren of afsluiten van een (deel van) het netwerk/systeem;
- het gebruik maken van back-ups om verloren/gestolen gegevens te herstellen;
- het identificeren van de (mogelijke) betrokkenen die op de hoogte gesteld moeten worden van het (mogelijke) datalek en hen, indien nodig, alvast instructies geven en/of assisteren ter voorkoming van eventuele schade van het datalek;
- het informeren van betrokken organisaties die advies kunnen geven en/of moeten krijgen om het datalek zo snel mogelijk te verhelpen en de (mogelijke) gevolgen hiervan zoveel mogelijk te beperken;
- het informeren van de bestuurder opdat deze zich vast voor kan bereiden op de berichtgeving naar buiten en/of aan (eventuele) betrokkenen en/of vragen van de pers;
- het doen van aangifte bij de politie in gevallen waarin (waarschijnlijk) sprake is (geweest) van illegale activiteiten of wanneer dit in de toekomst verwacht kan worden (denk hierbij aan identiteitsfraude, hacking etc.);
- enige andere maatregel die in het specifieke geval noodzakelijk wordt geacht.

Het treffen van (voorlopige) beschermingsmaatregelen gebeurt altijd in overleg en met goedkeuring van de bestuurder.

8 Vaststelling en ondertekening

Door ondertekening wordt akkoord gegaan met de inhoud van dit beleid Datalekken Protocol.

College van Bestuur

Mevrouw H.J. Sikken
Voorzitter College van Bestuur
Datum: 10-11-2021

Namens de Gemeenschappelijke Medezeggenschapsraad

De heer G. van Rijswijk
Voorzitter Gemeenschappelijke Medezeggenschapsraad
Datum:

9 Bijlage 1: Intern formulier melding datalek

Tijdstip melding:	
Inhoud melding:	
Impact:	☐ Klein ☐ Middel ☐ Groot
Welke type gegevens bevat het:	☐ Naam-, adres- en woonplaatsgegevens ☐ Telefoonnummers ☐ E-mailadressen of andere adressen voor elektronische communicatie ☐ Toegangs- of identificatiegegevens ☐ Financiële gegevens ☐ Burgerservicenummer (BSN) ☐ Paspoortkopieën of kopieën van andere legitimatiebewijzen ☐ Geslacht, geboortedatum en/of leeftijd ☐ Bijzondere persoonsgegevens ☐ Anders nl;
Inbreuk voor de persoonlijke levenssfeer van de betrokkenen?	☐ Stigmatisering of uitsluiting ☐ Schade aan de gezondheid ☐ Blootstelling aan (identiteits)fraude ☐ Blootstelling aan spam of phishing ☐ Nog onbekend
Wat is de aard van de inbreuk?	☐ Lezen (vertrouwelijkheid) ☐ Kopiëren ☐ Veranderen (integriteit) ☐ Verwijderen of vernietigen (beschikbaarheid) ☐ Diefstal ☐ Nog niet bekend
Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie?	☐ Ja ☐ Nee
Indien Ja, welke organisatie:	
Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	
Tijdstip melding coördinator datalekken (ICT Beheerder):	
Meldingen aan bestuurder:	
Beoordeling of er sprake is van een data lek:	
Onderzoeksvragen:	

Is er sprake van een data lek?	
Melding gemaakt bij Meldloket autoriteit persoonsgegevens	**Nee** **Meldingsnummer:**
Indien Nee waarom niet?	
Indien Ja: Data lek melden aan betrokkenen	☐ **Ja** ☐ **Nee**
Indien **Nee** waarom niet?	
Zijn er technische maatregelen genomen?	
Externe partij ingeschakeld?	☐ **Ja** ☐ **Nee**
Zo Ja welke	
Indien Nee waarom niet?	
Hoe is de lek ontstaan:	☐ Verlies van papieren data ☐ Verlies van data op gegevensdrager (usb, harde schijf etc.) ☐ Verlies van data d.m.v. verkeerd zenden e-mail ☐ Verlies van data ☐ Verlies telefoon en of tablet met mailgegevens en of andere gegevens ☐ Hacken van een cloudservice ☐ Virus/ Ransomware ☐ anders……
Verdere opmerkingen:	

Afgerond dd. tijd:

Door:
Functie:

https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

10 Bijlage 2: Formulier medewerker Wet meldplicht datalekken

Wet meldplicht datalekken
Vanaf 1 januari 2016 is het wettelijk verplicht om datalekken te melden. Zowel grootschalige inbraak in gegevens als het kwijtraken van, diefstal of onbevoegd gebruik van persoonsgegevens telt als een datalek.

Wat is een datalek?
We spreken van een datalek als persoonsgegevens in handen vallen van derden, die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsprobleem, verkeerd gebruik of een verlies. Het kan gaan om gestolen computerbestanden (gehackt), al kan een gestolen geprinte klantenlijst evengoed een datalek vormen. Voorbeelden in onze organisatie zijn; het verlies/diefstal van een usb stick, het verlies/diefstal van een laptop of telefoon, het verlies/slordig omgaan met vertrouwelijke prints, delen met onbevoegde derden of te lang bewaren.

Hoe voorkom je als medewerker datalekken?
- Als eerste; gebruik niet meer gegevens dan nodig. Verzamel geen persoonsgegevens die geen waarde toevoegen.
- Na opdracht printen: haal de stukken direct op bij de printer
- Indien een print gestuurd en niet bij de printer, kijk printerinstellingen na of de juiste printer gekozen is. Spoor de fout geprinte documenten op! En vernietig.
- Vind je documenten van een collega, -die persoonsgegevens bevatten- bij een printer, breng ze bij de collega en wijs deze op het feit dat die open en bloot lag.
- Bij verlies/diefstal van de (privé) smartphone en of tablet waarop school mail gesynchroniseerd wordt direct melding maken bij de directeur van de school, indien niet bereikbaar bij de bestuurder.
- Op Usb/externe harde schijf geen data met persoonsgegevens plaatsen. Indien het nodig is/was, omdat het netwerk niet beschikbaar was/is. Direct nadat het netwerk weer beschikbaar is op het netwerk plaatsen en verwijderen van de usb stick.
- Bij verlies/diefstal van een USB/ externe harde schijf waarop documenten van de school staan, direct melding maken bij de ICT beheerder, indien niet bereikbaar bij de bestuurder.
- Geen persoonsgegevens van leerlingen rechtstreeks op de laptops plaatsen, altijd op het netwerk.
- Niet mailen naar eigen privé mail maar mailen naar je eigen school-mail benaderen dan buiten het netwerk via webmail.
- Verspreid geen persoonsgegevens via de e-mail en/of Clouddiensten waar geen contract mee is afgesloten zoals Dropbox. Hiervoor mag alleen office 365 gebruikt worden.
- Gebruik op het netwerk andere wachtwoorden dan privé. Wijzig regelmatig je wachtwoorden.
- Geen mails meer verzenden met Gmail en of andere privé accounts.
- Indien er toch documenten gemaild moeten worden met daarin persoonsgegevens. Check eerst het email adres door de ontvanger een mail te sturen met het verzoek deze te beantwoorden. Vervolgens kun je op die mail het document mailen. Je weet dan zeker dat je het juiste email adres hebt. Vraag voor de zekerheid een ontvangstbevestiging.
- Stuur geen mail met meerdere namen (bijv. alle ouders van een groep) in cc maar altijd in BCC
- Bij twijfel van een of ander mogelijk verlies van data neem altijd contact op met de directeur en/of bestuurder.

11 Bijlage 3: Voorbeeldbrief datalek

Geachte heer, mevrouw XXXX

U ontvangt deze brief omdat u als ouder bij ons bent of geweest bent. Een laptop van een van onze medewerkers is gestolen. De laptop is beveiligd met een wachtwoord. Op de laptop zijn in het verleden gegevens van leerlingen verwerkt. Daardoor kunnen wij niet helemaal uitsluiten dat er persoonsgegevens, met name gebruikt voor groepsoverzichten en foto's, op de laptop zijn achtergebleven. Wij hebben aangifte gedaan van diefstal. Bovendien hebben wij dit gemeld bij de Autoriteit Persoonsgegevens. Wij willen nogmaals benadrukken dat het niet zeker is dat er persoonsgegevens van uw zoon/ dochter of andere leerlingen op de laptop zichtbaar waren. Wij willen u uit zorgvuldigheid toch persoonlijk informeren.

Heeft u vragen naar aanleiding van deze brief dan kunt u ons op schooldagen tussen 09.00 en 17.00 uur bellen via xxxxx. Wij zien op dit moment geen noodzaak voor u om zelf actie te ondernemen.

Wij betreuren dit voorval zeer en bieden u hiervoor onze welgemeende excuses aan.

Met vriendelijke groet,