STICHTING
Openbaar Onderwijs
WIJK BIJ DUURSTEDE

Waar kinderen belangrijk zijn!

# Datalekken protocol

## INHOUD

INHOUD ..... 2
1 Inleiding ..... 3
1.1 Wet- en regelgeving datalekken ..... 3
1.2 Onverwijlde mededeling ..... 4
1.3 Onderzoek ..... 4
1.4 (Preventieve) beschermingsmaatregelen ..... 6
1.5 Melding aan de AP ..... 6
1.6 Melding aan betrokkene ..... 8
1.7 Beoordeling en evaluatie ..... 9
2 Bijlage 1 : Beslisboom datalek ..... 10
3 Bijlage 2 : Intern formulier melding datalek ..... 11
4 Bijlage 3 : Formulier medewerker Wet meldplicht datalekken ..... 13
5 Bijlage 4 : Voorbeeldbrief datalek ..... 14
6 Vaststelling en ondertekening ..... 15

# 1 Inleiding

Het Datalekken protocol is gebaseerd op het model van Kennisnet (2016) 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:**

- *Betrokkene:* degene op wie een persoonsgegeven betrekking heeft.
- *Datalek:* een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van Persoonsgegevens
- *Persoonsgegevens:* elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
- *Verwerking:* elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen, of vernietigen van gegevens.

## 1.1 Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen 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 de leerling administratie en 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 bewerkers aanvullende afspraken over het melden van datalekken.

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’. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van een klas is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

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

## 1.2 Onverwijlde mededeling

a. Alle coördinatie en communicatie aangaande het (vermeende) datalek verloopt uitsluitend via de coördinator datalekken, ICT beheerder of diens waarnemer. Een ieder is gehouden alle verzoeken van externen, waaronder de media, door te verwijzen naar de coördinator datalekken of diens waarnemer.

b. Een ieder die een (mogelijk) datalek constateert meldt dit onverwijld aan zijn/haar leidinggevende. Indien de constatering buiten werktijd plaatsvindt, wordt zo spoedig mogelijk contact opgenomen met de coördinator datalekken.

c. De leidinggevende meldt aan de coördinator datalekken. Ook wanneer de leidinggevende twijfelt of sprake is van een datalek wordt dit eveneens gemeld bij de coördinator datalekken.

d. De coördinator datalekken beoordeelt vervolgens onverwijld of (mogelijk) sprake is van een datalek.

e. De coördinator datalekken beoordeelt vervolgens onverwijld of (1) mogelijk sprake is van een Datalek (zie 1.3 voor de beleidsregels die hierbij van belang zijn) en (2) of de Stichting Openbaar Onderwijs Wijk bij Duurstede voor het melden van dit datalek de verantwoordelijkheid draagt.

f. Indien de coördinator datalekken of diens waarnemer door omstandigheden afwezig, dan wel onbereikbaar is, fungeert de bestuurder als zijn/haar waarnemer. Op de website www.obswijk.nl wordt aangegeven hoe in het geval van calamiteiten de bestuurder of zijn/haar waarnemer bereikbaar is.

## 1.3 Onderzoek

1) Indien de coördinator datalekken van oordeel is dat sprake is van een datalek, waarvoor de Stichting Openbaar Onderwijs Wijk bij Duurstede de verantwoordelijkheid draagt, dan wordt onderzocht hoe dit lek is ontstaan en welke (preventieve) beschermingsmaatregelen ingezet worden.

2) Als besloten wordt om de oorzaak van het datalek niet te onderzoeken, dient de reden hiervoor gedocumenteerd te worden. Indien de reden is dat de Stichting Openbaar Onderwijs Wijk bij Duurstede hiervoor niet de (formele) verantwoordelijkheid draagt dan informeert de coördinator datalekken onverwijld de organisatie die wél de verantwoordelijkheid draagt voor het melden van het datalek.

3) De coördinator datalekken heeft de leiding over het onderzoek en kan hierbij zowel de hulp van anderen binnen de organisatie als (in overleg met de bestuurder) buiten de organisatie inschakelen (‘Datalek Onderzoeksteam’). De coördinator datalekken rapporteert over de voortgang en (voorlopige) uitkomst van het onderzoek aan de bestuurder.

4) Het Datalek Onderzoeksteam onderzoekt vervolgens het desbetreffende datalek en stelt vast hoe de negatieve gevolgen van het lek zoveel mogelijk beperkt kunnen worden.
Daarbij neemt het Datalek Onderzoeksteam in ieder geval de volgende zaken in overweging:
   - de datum waarop het datalek is ontstaan;
   - hoe het datalek is ontstaan;
   - hoe het datalek is ontdekt;
   - de aard en ernst van het datalek;
   - de omvang van het datalek;
   - of het datalek specifieke (kwetsbare) groepen personen betreft;
   - of de verloren, gestolen of geschonden Persoonsgegevens zijn hersteld;
   - of er aangifte bij de politie is gedaan of gedaan moet worden;
   - of het datalek, althans enige schade die hieruit is voortgevloeid, bij de verzekering gemeld moet worden;
   - of eventueel een advocaat in de arm genomen moet worden[1] ;
   - welke (preventieve) beschermingsmaatregelen genomen zijn/kunnen worden om de gevolgen van het datalek zoveel mogelijk te beperken en welke kosten dit met zich meebrengt;
   - wat er met de persoonsgegevens gebeurd (is) en welke gevolgen dit heeft gehad/zou kunnen hebben;
   - overige consequenties (zoals een risico voor de algemene gezondheid of het verlies van reputatie).

5) Bovenstaande bevindingen worden schriftelijk vastgelegd en door de coördinator datalekken in concept voorgelegd aan de bestuurder. De bestuurder kan vervolgens opdracht geven nader of diepgaander onderzoek te verrichten.

6) Dit onderzoek geniet een hoge prioriteit en dient -indien mogelijk- binnen 3 werkdagen afgerond te zijn, nadat het gerapporteerd is door de melder aan de coördinator datalekken.

7) Nadat de belangrijkste kwesties zijn onderzocht en er eventueel (preventieve) beschermingsmaatregelen zijn getroffen, wordt indien noodzakelijk en op verzoek van de bestuurder, door (een deel van) het Datalek Onderzoeksteam diepgaander onderzoek verricht naar (de oorzaak en de gevolgen van) het datalek.

[1] Een advocaat kan adviseren of een melding aan de AP en betrokkenen noodzakelijk is. Informatie-uitwisseling met een advocaat is vertrouwelijk en kan nadien in beginsel niet worden opgevraagd door de AP.

## 1.4 (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.

## 1.5 Melding aan de AP

Indien (enkele van) bovenstaande maatregelen getroffen zijn, beoordeelt de coördinator datalekken in overleg met de bestuurder of een melding aan de AP noodzakelijk is. Hiervoor dient vastgesteld te worden of het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Hierbij spelen verschillende factoren een rol, zoals:

- de hoeveelheid gelekte persoonsgegevens in totaal en/of per persoon;
- de categorie betrokkenen;
- de aard van de gegevens (betreft het gevoelige gegevens?).

Bij gevoelige persoonsgegevens kan gedacht worden aan:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp (godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag);
- gegevens over de financiële of economische situatie van de betrokkene (schulden, salaris- en betalingsgegevens);
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene ((gok)verslaving, prestaties op school of werk of relatieproblemen);
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude (biometrische gegevens, kopieën van identiteitsbewijzen BSN);
- gegevens waar een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust of die onder het beroepsgeheim vallen.

Indien de gelekte persoonsgegevens van gevoelige aard zijn dan is een melding aan het AP over het algemeen noodzakelijk. Dit is ook het geval wanneer het aanzienlijke aantallen gelekte persoonsgegevens betreft.

Indien de coördinator datalekken, eventueel in overleg met het Datalek Onderzoeksteam, constateert dat een melding aan de AP noodzakelijk is, stelt hij de bestuurder hiervan onverwijld op de hoogte. De bestuurder doet -indien mogelijk binnen een werkweek na de ontdekken van het Datalek- een melding van het Datalek bij de AP[2].

Deze melding moet worden ingediend door het webformulier[3] 'Meldloket Datalekken' in te vullen en omvat in ieder geval de volgende elementen:

- de aard van de inbreuk;
- de instanties waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die zijn getroffen of voorgesteld om deze gevolgen te verhelpen.

Indien de melding later dan na 72 uur geschiedt, wordt (door de AP) aanbevolen om te vermelden waarom de melding niet eerder gedaan is. De melding kan later overigens altijd nog aangevuld of ingetrokken worden.

[2] Wanneer geen melding van het datalek wordt gedaan aan de AP, terwijl dit wel had gemoeten, kan een bestuurlijke boete opgelegd worden.

[3] https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

## 1.6 Melding aan betrokkene

Nadat een melding aan de AP is gedaan onderzoekt de coördinator datalekken - eventueel gesteund door (een deel van) het Datalek Onderzoeksteam- in samenspraak met de bestuurder of het datalek gemeld dient te worden aan de betrokkene(n)[4]. Hiervoor zijn de volgende vragen van belang:

- bieden de technische maatregelen/cryptografie die zijn toegepast voldoende bescherming om de melding achterwege te laten?
  **Ja:** Een melding aan de betrokkene(n) kan achterwege gelaten worden.
  **Nee:** Zie volgende vraag;
- zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene(n) (hierbij kan bijv. gedacht worden aan identiteitsfraude, aantasting van in eer en goede naam, discriminatie of onrechtmatige publicatie)?[5]
  **Nee:** Een melding aan de betrokkene(n) kan achterwege gelaten worden.
  **Ja:** Zie volgende vraag;
- zijn er zwaarwegende redenen om de melding aan de betrokkene(n) achterwege te laten?
  **Ja:** Een melding aan de betrokkene(n) kan achterwege gelaten worden.
  **Nee:** Een melding aan de betrokkene(n) is noodzakelijk.

Indien de bestuurder besluit dat een melding aan de betrokkene(n) noodzakelijk is, bepaalt ze tevens hoe deze kennisgeving[6] dient plaats te vinden. Hierbij kan er afhankelijk van de omstandigheden aan gedacht worden om alle betrokkenen individueel, dan wel gezamenlijk te informeren, dan wel te kiezen voor een combinatie daarvan.

Daarnaast beslist de bestuurder welke communicatiemiddelen voor de kennisgeving ingezet worden (e-mail, post, berichtgeving op de eigen website, kranten etc.) en wordt een tekst voor de kennisgeving vastgesteld welke in elk geval de volgende elementen omvat:

- de aard van de inbreuk;
- de instanties waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

---

[4] Indien het datalek volgens de wet niet aan de AP gemeld hoeft te worden, hoeft dit ook niet aan de betrokkenen(n) te worden gemeld

[5] Hierbij kan gedacht worden aan identiteitsfraude, aantasting van in eer en goede naam, discriminatie of onrechtmatige publicatie. Indien de gegevens van gevoelige aard zijn, dient in beginsel een melding aan betrokkene gedaan te worden.

[6] Volgens de wet dient de kennisgeving aan de betrokkene op zo'n manier gedaan te worden dat, rekening houdend met de aard van de inbreuk, de geconstateerde en feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van de betrokkenen en kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.

## 1.7 Beoordeling en evaluatie

Zodra alle initiële zorgen omtrent het datalek verholpen zijn actualiseert de coördinator datalekken het overzicht met alle datalekken. Dit overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, de melding aan de AP en, indien een melding aan de betrokkene(n) is gedaan, de tekst van de kennisgeving aan de betrokkene(n).

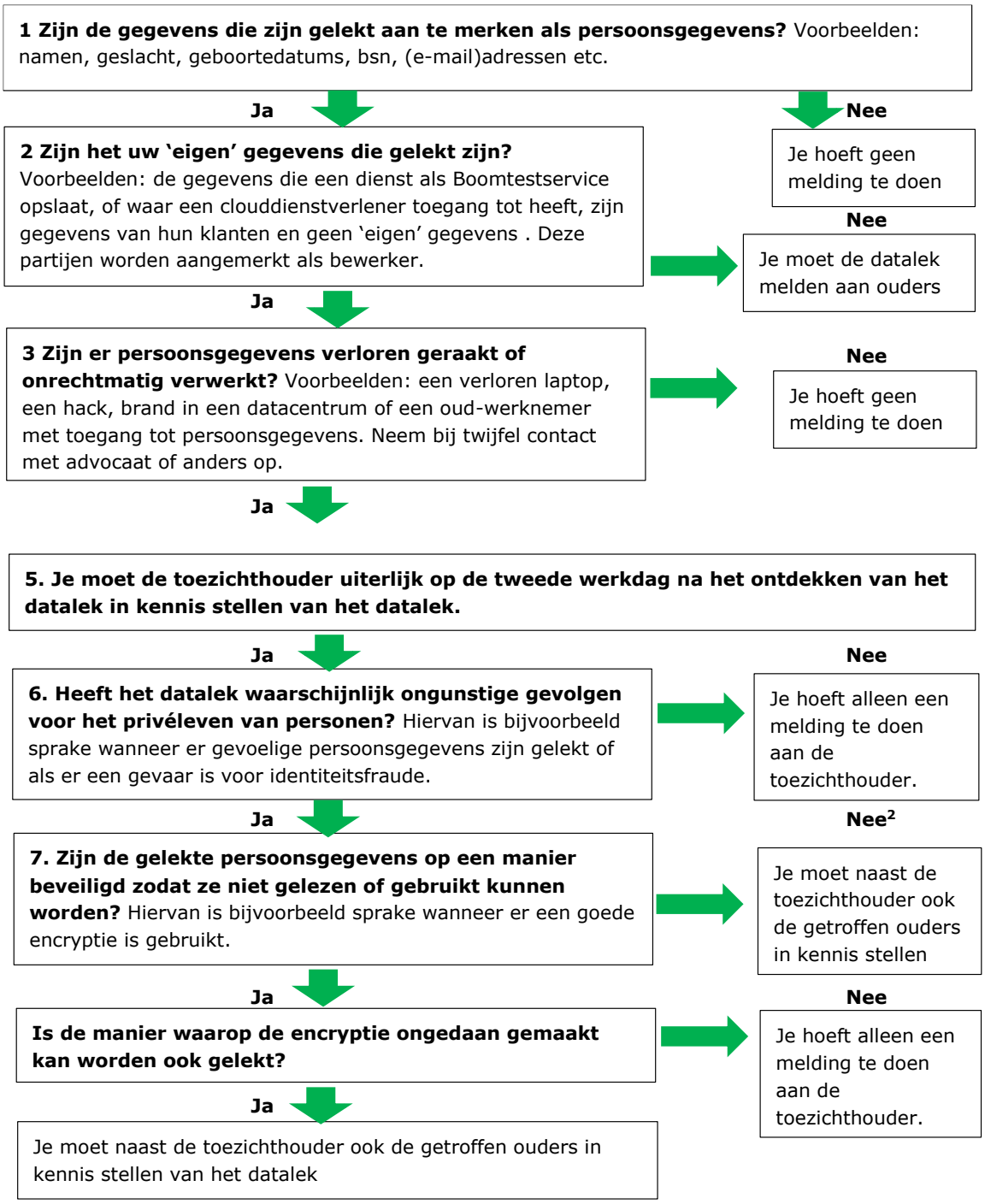
De gegevens worden -behoudens het gestelde in artikel 4.27- gedurende een jaar na het ontstaan van het datalek bewaard (om lering te trekken uit het datalek en antwoord te kunnen geven op vragen van betrokkene(n) of het datalek, indien nodig, later alsnog aan betrokkene(n) te melden). Dit overzicht wordt niet openbaar gemaakt.

In afwijking van artikel 4.26 geldt een bewaartermijn van drie jaar wanneer geen melding van het datalek aan de betrokkene(n) is gedaan omdat a) geoordeeld is dat de technische beschermingsmaatregelen voldoende bescherming boden of b) er sprake was van zwaarwegende omstandigheden. De coördinator datalekken evalueert -in overleg met de bestuurder - eenmaal per jaar of het datalek alsnog aan de betrokkene(n) gemeld moet worden.

De bestuurder neemt aan de hand van de evaluatie in overweging of:

- nog diepgaander onderzoek gedaan moet worden naar (het ontstaan en/of de gevolgen van) het datalek;
- een actieplan/prioriteitenlijst opgesteld moet worden om toekomstige/verwachte problemen systematisch aan te pakken.

## 2 Bijlage 1 : Beslisboom datalek




[1] Ouders: de Ouders/Verzorgers van de getroffen leerlingen

[2] https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

## 3 Bijlage 2 : Intern formulier melding datalek

| | |
|---|---|
| Tijdstip melding: | |
| Inhoud melding: | |
| Impact: | ☐ Klein<br>☐ Middel<br>☐ Groot |
| Welke type gegevens bevat het: | ☐ Naam-, adres- en woonplaatsgegevens<br>☐ Telefoonnummers<br>☐ E-mailadressen of andere adressen voor elektronische communicatie<br>☐ Toegangs- of identificatiegegevens<br>☐ Financiële gegevens<br>☐ Burgerservicenummer (BSN)<br>☐ Paspoortkopieën of kopieën van andere legitimatiebewijzen<br>☐ Geslacht, geboortedatum en/of leeftijd<br>☐ Bijzondere persoonsgegevens<br>☐ Anders nl; |
| Inbreuk voor de persoonlijke levenssfeer van de betrokkenen? | ☐ Stigmatisering of uitsluiting<br>☐ Schade aan de gezondheid<br>☐ Blootstelling aan (identiteits)fraude<br>☐ Blootstelling aan spam of phishing<br>☐ Nog onbekend |
| Wat is de aard van de inbreuk? | ☐ Lezen (vertrouwelijkheid)<br>☐ Kopiëren<br>☐ Veranderen (integriteit)<br>☐ Verwijderen of vernietigen (beschikbaarheid)<br>☐ Diefstal<br>☐ Nog niet bekend |
| Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie? | ☐ Ja<br>☐ Nee |
| Indien Ja, welke organisatie: | |
| Wbp of telecommunicatiewet: | ☐ Wbp<br>☐ Telecommunicatiewet |
| 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**<br><br>**Meldingsnummer:** |
| Indien Nee waarom niet? | |
| **Indien Ja:**<br>Data lek melden aan betrokkenen | ☐ **Ja**<br>☐ **Nee** |
| Indien **Nee** waarom niet? | |
| Zijn er technische maatregelen genomen? | |
| Externe partij ingeschakeld? | ☐ **Ja**<br>☐ **Nee** |
| Zo Ja welke | |
| Indien Nee waarom niet? | |
| Hoe is de lek ontstaan: | ☐ Verlies van papieren data<br>☐ Verlies van data op gegevensdrager (usb, harde schijf etc)<br>☐ Verlies van data d.m.v. verkeerd zenden e-mail<br>☐ Verlies van data<br>☐ Verlies telefoon en of tablet met mailgegevens en of andere gegevens<br>☐ Hacken van een cloudservice<br>☐ Virus / Ransomware<br>☐ anders…… |
| Verdere opmerkingen: | |

Afgerond dd. tijd:

Door:
Functie:

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

# 4 Bijlage 3 : 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.

**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 ICT beheerder, 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
- 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 ICT beheerder en/of bestuurder.

Gelezen d.d. Naam en handtekening medewerker:

# 5 Bijlage 4 : 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,

# 6 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: 24 mei 2018

Namens de Gemeenschappelijke Medezeggenschapsraad

De heer G. van Rijswijk
Voorzitter Gemeenschappelijke Medezeggenschapsraad
Datum: 24 mei 2018