Afbeelding met Lettertype, tekst, schermopname, Graphics

Automatisch gegenereerde beschrijving

Incidentmanagementproces

Voorbeelddocument

Versie: Januari 2025

Afbeelding met Kleurrijkheid, Graphics, blauw, patroon

Automatisch gegenereerde beschrijving

**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen incidentmanagementproces. Elke school en elk schoolbestuur is anders. Pas het proces daarom aan aan jouw eigen situatie.**

**Aanpassen van dit voorbeelddocument**

Let bij het aanpassen van het document op het volgende:

* Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je de procesbeschrijving definitief maakt.
* Deze procesbeschrijving gaat ervan uit dat taken, rollen en functies die nodig zijn om het proces uit te voeren bij de juiste personen belegd zijn. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
* Geel gearceerde teksten moet je vervangen door eigen tekst.

**Totstandkoming**

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.

Afbeelding met biljartbal, symbool, cirkel

Automatisch gegenereerde beschrijving

Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/normenkaderibp.kennisnet.nl/groeipad)of stuur een mail naar [*ibp@kennisnet.nl*](mailto:ibp@kennisnet.nl)*.*

**Documentgeschiedenis**

***Toelichting***

* *Geef hier aan wie het document vaststelt. Dat kan bijvoorbeeld de proceseigenaar zijn, maar ook het bestuur.*
* *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

**Revisies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Review** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentclassificatie**

|  |  |
| --- | --- |
| **Classificatie** | **Beschrijving** |
| Openbaar | Dit document mag zonder beperkingen worden gedeeld |
| Vertrouwelijk | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties> |
| Geheim | Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>. |

**Inhoudsopgave**

[1 Inleiding 5](#_Toc189242111)

[1.1 Wat is een beveiligingsincident en een datalek 5](#_Toc189242112)

[1.2 Reikwijdte 5](#_Toc189242113)

[2 Processtappen 6](#_Toc189242114)

[2.1 Melding ontvangen en registeren 6](#_Toc189242115)

[2.2 Incident classificeren en beoordelen 7](#_Toc189242116)

[2.3 Vervolgstappen bepalen 8](#_Toc189242117)

[2.4 Incident oplossen 9](#_Toc189242118)

[2.5 Incident vastleggen en afsluiten 9](#_Toc189242119)

[2.6 Periodieke rapportage 10](#_Toc189242120)

[2.7 Evaluatie en preventie 10](#_Toc189242121)

[Bijlage A 11](#_Toc189242122)

[Soorten datalekken 11](#_Toc189242123)

[Bijlage B 12](#_Toc189242124)

[Beoordelen van een datalek 12](#_Toc189242125)

[Bijlage C 14](#_Toc189242126)

[Template melding datalek aan betrokkene(n) 14](#_Toc189242127)

# Inleiding

Een incidentmanagementproces zorgt ervoor dat we snel en effectief reageren op incidenten om schade te beperken en problemen te voorkomen. Dat doen we door incidenten te melden, herkennen en registreren, de impact te bepalen en het probleem zo snel mogelijk op te lossen. Daarna bekijken we wat er is gebeurd en leren ervan om herhaling te voorkomen. Dit document beschrijft hoe het incidentmanagementproces wordt uitgevoerd binnen <vul naam organisatie in>. Het is bedoeld voor alle medewerkers, inclusief de privacy officer en/of de functionaris gegevensbescherming en de IBP’er.

## Wat is een beveiligingsincident en een datalek

Bij een beveiligingsincident is de normale werking van de ICT-omgeving verstoort. Het is dus niet alleen een dreiging of een zwakke plek in de beveiliging, maar er is daadwerkelijk een probleem ontstaan. Zijn er door een beveiligingsincident ongewenst persoonsgegevens verloren gegaan? Of heeft iemand door een beveiligingsincident ongewenst toegang gekregen tot persoonsgegevens? Dan is er sprake van een datalek.

## Reikwijdte

Binnen het incidentmanagementproces vallen alle problemen die de beschikbaarheid, integriteit en vertrouwelijkheid van informatie verstoren. Er kunnen veel oorzaken zijn voor zulke problemen. Denk bijvoorbeeld aan:

* Stroomstoringen
* Geen back-up hebben of een fout in de back-up
* Verlies van een USB-stick, harde schijf of andere gegevensdrager
* Een vertrouwelijk document bij de printer laten liggen
* Cyberaanvallen zoals phishing, virussen of DDoS-aanvallen

# Processtappen

Het incidentmanagementproces bestaat uit 7 stappen.

Afbeelding met tekst, schermopname, Lettertype, ontwerp

Door AI gegenereerde inhoud is mogelijk onjuist.

## Melding ontvangen en registeren

***Toelichting***

*Je geeft bij deze stap aan op welke manier meldingen opgenomen worden in het incidentmanagementproces van de organisatie en wie hiervoor verantwoordelijk is.*

Het ontvangen van meldingen van incidenten en het registreren ervan valt uiteen in een aantal taken:

A. Ontvang de melding en verzamel de juiste informatie

Incidenten kunnen worden gemeld door medewerkers, leerlingen, ouders, leveranciers of mensen van buiten de organisatie. Het indienen en registreren van een melding vindt plaats door:

* Melding per E-mail naar: <vul het e-mailadres in waar incidenten kunnen worden gemeld>
* Telefonische of mondelinge melding naar <naam> <telefoonnummer>

Van elk incident wordt ten minste de volgende informatie verzameld:

* Contactgegevens melder
* Beschrijving incident
* Datum/tijdstip van constatering incident

B. Registreer de melding

De incidentmanager of proceseigenaar registreert de melding in <naam systeem of incidentregister>.

## Incident classificeren en beoordelen

***Toelichting:****Bij deze stap wordt het incident geclassificeerd op basis van ernst en impact. Daarna wordt geïnventariseerd hoe groot de schade is en hoe snel er actie nodig is aan de hand van de doorlooptijden voor het oplossen van het incident.*

A. Beoordeel of het incident ook een datalek is

Afbeelding met tekst, schermopname, diagram, lijn

Door AI gegenereerde inhoud is mogelijk onjuist.

Niet elk incident is een datalek, maar elk datalek is wel een incident. De privacy officer of functionaris gegevensbescherming beoordeelt of er sprake is van een datalek en bepaalt wat er moet gebeuren

B. Bepaal de impact en urgentie van het incident  
Bepaal de impact en de urgentie van het incident volgens de criteria in onderstaand schema. Dit bepaalt de prioriteit.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Prioritering** | | | **Urgentie** | | |
| **Hoog** | **Midden** | **Laag** |
| Kan niet werken | Kan deels werken | Kan werken |
| **Impact** | **Hoog** | Hele organisatie/ school/primair onderwijsproces | 1 - Calamiteit | 2 - Hoog | 3 - Midden |
| **Midden** | Team/afdeling | 2 - Hoog | 3 - Midden | 4 - Laag |
| **Laag** | Eén of een  beperkt aantal eindgebruikers | 3 - Midden | 3 - Laag | 4 - Laag |

Binnen <naam schoolbestuur> gelden de volgende doorlooptijden voor het afhandelen van incidenten:

* **Calamiteit**: Zo snel mogelijk. Te bepalen door crisismanagementteam.
* **Hoog**: <bijvoorbeeld, 8 uur>
* **Midden** <bijvoorbeeld, 3 werkdagen>
* **Laag**: <bijvoorbeeld, 5 werkdagen>

De doorlooptijden van openstaande incidenten worden bewaakt door de incidentmanager of proceseigenaar en bij overschrijding geëscaleerd naar behandelaren en/of leveranciers of het schoolbestuur. Overschrijding van de doorlooptijden kan leiden tot aanpassing van de prioriteit en daarmee tot escalatie naar het schoolbestuur of het crisismanagementteam.

|  |
| --- |
| **Let op**: de doorlooptijden gelden niet voor datalekken waar melding van gemaakt moet worden bij de Autoriteit Persoonsgegevens. Vanaf het moment van ontdekking heb je daarvoor **72 uur** de tijd. |

C. Hoe bepaal je de ernst van en kans op een datalek?

Hoe groot de gevolgen van een datalek zijn, wordt bepaald door twee belangrijke factoren:

1. De ernst van de gevolgen:
   * Kan het lek bijvoorbeeld leiden tot identiteitsdiefstal, fraude, reputatieschade, discriminatie of financiële schade?
   * Zijn gevoelige gegevens betrokken, zoals medische informatie, strafrechtelijke gegevens of persoonsgegevens van kwetsbare groepen zoals leerlingen?
2. De kans schade optreedt:
   * Zijn de gegevens al in verkeerde handen gevallen of is dat waarschijnlijk?
   * Zijn de gegevens versleuteld of beschermd of kunnen ze eenvoudig worden misbruikt?

Snelle actie is nodig als de ernst van de gevolgen groot is, de kans op misbruik hoog is of bij twijfel om verdere schade te voorkomen.

## Vervolgstappen bepalen

***Toelichting:****Bij deze stap ga je de vervolgstappen bepalen voor het incident. Wie gaat het oplossen en wie moet er worden geïnformeerd of betrokken bij de oplossing?*

A. Wijs een behandelaar toe  
De incidentmanager wijst het incident toe aan een behandelaar of aan de relevante leverancier. Is er sprake van een datalek? Dan zijn ook de privacy officer en/of functionaris gegevensbescherming betrokken.

B. Melden van een datalek

Een datalek moet worden gemeld als het grote gevolgen kan hebben voor de mensen van wie de gegevens zijn gelekt. Wat die gevolgen kunnen zijn en welke soorten datalekken er zijn, wordt uitgelegd in bijlage A. Een datalek moet soms aan de Autoriteit Persoonsgegevens gemeld worden en/of soms aan betrokkenen.

* **Autoriteit Persoonsgegevens**: Is er sprake van een risico voor de rechten en vrijheden van betrokkenen? Dan moet er een melding worden gedaan bij de Autoriteit Persoonsgegevens. Bij het beoordelen hiervan wegen veel factoren mee. Zie bijlage B voor een toelichting. Beschik je nog niet over alle informatie voor het datalek? Dan kun je een eerste melding doen en later een vervolgmelding
* **Melden aan betrokkenen**. Een datalek moet gemeld worden aan de betrokkene(n) als het voor hen een hoog risico inhoudt. Deze afweging wordt gemaakt door de functionaris gegevensbescherming in overleg met de privacy officer. Een datalek moet altijd aan betrokken worden gemeld als persoonsgegevens van gevoelige of bijzondere aard zijn gelegd (medisch of financieel) of als het gaat om grote hoeveelheden persoonsgegevens.
* **Niet melden**. Zijn er beschermingsmaatregelen genomen (preventief of reactief) en is daardoor het risico weggenomen? Dan hoeft het datalek niet aan betrokkenen te worden gemeld. Denk hierbij aan versleuteling van gegevens als preventieve maatregel of het op afstand wissen van een verloren laptop als reactieve maatregel.

Moet het datalek worden gemeld aan betrokkenen? Dan moet de school bepaalde informatie verzamelen en opnemen. Je kunt gebruikmaken van het template in bijlage C voor deze melding.

## Incident oplossen

A. Oorzaak analyseren en wegnemenOntwikkel een plan om het incident aan te pakken en verdere schade te voorkomen. Dit kan inhouden het herstellen van systemen, het informeren van betrokkenen en het nemen van juridische stappen indien nodig. Analyseer daarnaast de oorzaak van het incident en neem de oorzaak van het incident onmiddellijk weg of bepaal een work-around om het incident te beëindigen of de schade te beperken. Heeft de oplossing een change nodig? Dan dien je een wijzigingsverzoek in volgens het proces changemanagement.

B. Maatregelen nemen

Het is belangrijk bij incidenten om snel te handelen en bij datalekken te onderzoeken wat er met de persoonsgegevens is gebeurd om verdere problemen te voorkomen. Je moet weten waar de verloren, gestolen of ongewenst geziene gegevens nu zijn en wie ze mogelijk in handen heeft. Dit bepaalt hoe groot het risico is en welke maatregelen je moet nemen. Heb je de gegevens teruggekregen? Vraag dan ook meteen de schriftelijke bevestiging dat de gegevens volledig zijn verwijderd van alle apparaten en back-ups.

Bedenk goed wat je aan herstelacties kunt doen en welke maatregelen je moet nemen om herhaling te voorkomen. Als het om een ernstig probleem gaat, kan het crisismanagementteam worden ingeschakeld om de schade te beperken en verdere problemen te voorkomen.

## Incident vastleggen en afsluiten

Elk incident wordt geregistreerd in <naam systeem of incidentregister>. Is het incident correct opgelost? Dan leg je dit vast in het incidentregister. Datalekken moeten verplicht worden geregistreerd in het incidentenregister, ook als het datalek niet wordt gemeld aan de AP. De school slaat incidentdocumentatie op voor toekomstige audits, analyses en als interne verantwoording onder de AVG Het incident is hiermee afgesloten.

## Periodieke rapportage

***Toelichting***

*In deze stap beschrijf je hoe er gerapporteerd wordt aan het management over incidenten. Geef aan met welke frequentie dit gebeurt en over welke zaken wordt gerapporteerd.*

Met het incidentenregister als bron wordt <frequentie> gerapporteerd aan de directie. Er wordt gerapporteerd over het aantal gemelde incidenten, het aantal datalekken, het aantal openstaande incidenten en de incidenten met grote impact.

## Evaluatie en preventie

Na afsluiting van een incident bekijken we hoe een incident is opgelost en of dit goed is gegaan. Terugkerende incidenten kunnen verder worden onderzocht in het problemmanagementproces. Elk incident met persoonsgegevens moet worden geëvalueerd, zodat de functionaris gegevensbescherming patronen kan herkennen.

In de evaluatie wordt gekeken naar de oorzaak van incidenten, maatregelen om incidenten in de toekomst te voorkomen en noodzakelijke aanpassingen in werkwijzen en regels. Ook kunnen medewerkers extra getraind worden, en kunnen lessen uit incidenten intern worden gedeeld.

# Bijlage A

## Soorten datalekken

|  |  |  |
| --- | --- | --- |
| **Inbreuk op de beschikbaarheid** | **Inbreuk op de integriteit** | **Inbreuk op de vertrouwelijkheid** |
| Er is onbedoeld geen toegang tot persoonsgegevens, terwijl dat wel nodig is. Denk aan de onbedoelde vernietiging van persoonsgegevens. | De juistheid van de persoonsgegevens is in het geding, bijvoorbeeld door een onbevoegde of onbedoelde wijziging van deze persoonsgegevens. Nu is niet bekend welke gegevens nu wel of niet kloppend zijn. | Er is sprake van onbevoegde inzage in persoonsgegevens of een onbedoelde openbaring van of toegang tot persoonsgegevens |
| **Voorbeelden** | | |
| * Door een besmetting van gijzelsoftware (ransomware) is een deel van de data in het leerlingvolgsysteem vernietigd * Storing/ uitval systemen (technische storing en menselijke fout) * Wateroverlast/ brand in datacenter * Verlies/diefstal devices/datadragers * DDOS aanval * Malware (virussen, wormen, Trojaanse paarden etc.) | * Er is een verkeerde backup terug gezet waardoor gegevens van de laatste week terug zijn gezet * Technische/menselijke fout bij data-uitwisseling * Malware * Hacking | * Persoonsgegevens die aan een verkeerde geadresseerde zijn verstuurd * Geen, slecht of verkeerd toegepast autorisatiebeleid * Gebruik standaard inloggevens of zwakke wachtwoorden |
| **Voorbeelden passende maatregelen** | | |
| * Redundant * Software updates en patches tijdig installeren * Monitoring * Disaster Recovery Plan * Backups * Beleid hoe om te gaan met persoonsgegevens * Monitorings software * Awareness | * Versiebeheer * Datavalidatie * Standaarden voor data uitwisseling * Logging en monitoring voor schrijfacties | * Autorisatiematrix * Controle op toegekende autorisaties * Versleutelde verbindingen * MFA * Versleutelde opslag van informatie * Antivirus & end point protection |

# Bijlage B

## Beoordelen van een datalek

Melden aan de Autoriteit Persoonsgegevens

Bij de beoordeling gaat het er om of het datalek een risico oplevert voor ‘de rechten en vrijheden van betrokkenen. De functionaris gegevensbescherming of privacy officer van de school beantwoorden onderstaande vragen wanneer ze moeten beoordelen of het datalek aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) gemeld moet worden.

1. Wat is er precies gebeurd (is er sprake van een intern of extern datalek)?
2. Welke gegevens zijn betrokken bij het datalek?
3. Waarom is het wel / geen datalek dat gemeld moet worden?
4. Wat zijn de (mogelijke) gevolgen van het datalek?
5. Wie zijn er al geïnformeerd?
6. Wat zijn de te nemen vervolgstappen (melding aan de Autoriteit Persoonsgegevens en/of betrokkene(n))

Melden aan betrokkenen

De betrokkenen moeten worden geïnformeerd als een datalek waarschijnlijk een hoog risico voor hen oplevert. De volgende factoren helpen je bij het maken van de overweging of een datalek waarschijnlijk een hoog risico voor betrokkenen is:

**1.De aard van de inbreuk (gewist, gewijzigd of gelekt). Wat voor soort datalek is het?**

Het type datalek bepaalt hoe groot het risico is voor de mensen die betrokken zijn. Bijvoorbeeld: Als vertrouwelijke informatie in verkeerde handen komt doordat een papieren gespreksverslag over een leerling van de schoolpsycholoog per ongeluk in een klaslokaal achterblijft na een overlegt. En in het volgend lesuur alle leerlingen het verslag kunnen inzien.

**2. De soort, gevoeligheid en hoeveelheid persoonsgegevens.**

* Een gespreksverslag over een leerling van schoolpsycholoog bevat waarschijnlijk gezondheidsgegevens en is gevoeliger dan een normale persoonsgegevens, zoals een postcode van een leerling.
* Sommige gegevens zijn niet meteen schadelijk als ze uitlekken, maar als deze informatie in een bepaalde situatie wordt gedeeld, kan het grote gevolgen hebben. Bijvoorbeeld, identiteitsbewijzen of bankgegevens kunnen gebruikt worden voor identiteits / financiële fraude.
* Combinatie van gegevens. Eén los gegeven kan misschien onschuldig lijken, maar als meerdere gegevens samen worden gelekt, kan dit misbruikt worden.
* Het maakt ook uit of de gegevens van 1 leerling worden gelekt of de gegevens van alle leerlingen van een school.

**3. Hoe makkelijk kunnen personen worden herkend bij een datalek?**

Bij een datalek is het belangrijk om te kijken hoe eenvoudig iemand geïdentificeerd kan worden. Dit betekent: kan iemand de gegevens gebruiken om een specifieke persoon te herkennen of te koppelen aan andere informatie?

Soms is het direct duidelijk van wie de gegevens zijn, zonder extra onderzoek. In andere gevallen lijkt het moeilijker, maar kan een combinatie van gegevens alsnog een persoon herkenbaar maken. Identificatie kun je moeilijker maken door gegevens te versleutelen of pseudonimiseren.

**4. Hoe erg zijn de gevolgen van een datalek?**

Bij een datalek kan de impact voor de betrokken personen verschillen. Dit hangt af van welke gegevens zijn gelekt en wie hierdoor getroffen is. Sommige datalekken kunnen zeer ernstige schade veroorzaken, vooral als gevoelige persoonsgegevens betrokken zijn.

Mogelijke gevolgen van een datalek

* Identiteitsdiefstal of fraude – Iemand kan zich voordoen als een ander en misbruik maken van de gegevens.
* Lichamelijk of psychisch leed – Bijvoorbeeld als vertrouwelijke medische gegevens uitlekken.
* Schade aan reputatie – Persoonlijke informatie die openbaar wordt, kan iemand in problemen brengen.

**5. Wat als de gegevens per ongeluk bij de verkeerde persoon terechtkomen?**

Soms worden persoonsgegevens per ongeluk naar de verkeerde ontvanger gestuurd, bijvoorbeeld naar een andere afdeling op school. In zo’n geval kan de ontvanger gevraagd worden om de gegevens terug te sturen of te verwijderen en dit schriftelijk te bevestigen. Als de school erop kan vertrouwen dat de ontvanger hier correct mee omgaat, is de schade meestal kleiner.

**6. Wie loopt extra risico bij een datalek?**

Sommige mensen zijn kwetsbaarder als hun persoonsgegevens uitlekken. Dit geldt vooral voor kinderen en andere kwetsbare groepen. Voor hen kan een datalek grotere gevolgen hebben, zoals misbruik van gegevens of problemen op school en thuis.

**7. Wie is verantwoordelijk voor de gegevens en waarom is dat belangrijk?**

De organisatie die het doel en de middelen bepaalt bij een verweking, heet de verwerkingsverantwoordelijke. Hoe groot het risico van een datalek is, hangt af van het soort gegevens dat deze organisatie bewaart. Bijvoorbeeld:

* Een school bewaart leerling gegevens. Als deze uitlekken, kan dat ernstige gevolgen hebben voor de leerlingen.
* Een krant heeft misschien alleen een mailinglijst met namen en e-mailadressen. Dit is minder gevoelig dan leerling informatie.

**8. Hoeveel mensen zijn getroffen door een datalek?**

Een datalek kan één persoon raken, maar ook honderden of zelfs duizenden mensen. Hoe meer personen betrokken zijn, hoe groter het probleem vaak wordt. Toch kan zelfs een datalek dat maar één persoon treft, ernstige gevolgen hebben. Dit hangt af van het soort gegevens en de situatie. Bijvoorbeeld:

* Als gevoelige informatie zoals medische gegevens uitlekt, kan dat grote impact hebben, zelfs voor één persoon.
* Als het om algemene gegevens gaat, zoals een naam en e-mailadres, is de schade meestal kleiner.

# Bijlage C

## Template melding datalek aan betrokkene(n)

Moet het datalek worden gemeld aan betrokkenen? Dan nemen we daarin de volgende informatie op:

* De aard van de inbreuk. Geef duidelijke, eenvoudige uitleg over het datalek.
* De waarschijnlijke gevolgen van het datalek voor de betrokkene(n).
* De getroffen en voorgestelde maatregelen die onze school heeft genomen om de gevolgen voor de betrokkene(n) te beperken.
* De acties die de betrokkene(n) zelf kan ondernemen om de gevolgen voor zichzelf te beperken, denk aan het wijzigen van een wachtwoord.
* De naam- en contactgegevens van de privacy officer en/of functionaris gegevensbescherming of een ander contactpunt binnen onze school.

|  |  |
| --- | --- |
| **Melding datalek aan betrokken** | |
| Inleidend bericht | Beste <naam>, |
| Omschrijving + maatregelen + excuses | Op <datum> heeft er bij onze school een datalek plaatsgevonden waarbij uw gegevens betrokken zijn. <uitgebreide omschrijving + getroffen maatregelen>.  We betreuren dat dit datalek heeft plaatsgevonden. Dit had natuurlijk niet moeten gebeuren. Wij bieden dan ook onze excuses aan. |
| Wat zijn de gevolgen voor u? | Het datalek kan voor u de volgende gevolgen hebben: <omschrijving gevolgen>. |
| Wat kunt u doen? | Om de gevolgen van dit datalek te beperken raden wij u aan om de volgende maatregelen te treffen:  <MAATREGELEN>. |
| Vragen? | Voor vragen kunt u contact opnemen met onze <privacy officer/Functionaris Gegevensbescherming>, via <e-mailadres> of <telefoonnummer>. |