Stichting De Hoeksche School, openbaar primair en voortgezet onderwijs Hoeksche Waard

Protocol beveiligingsincidenten en datalekken

Biezenvijver 5
3297 GK Puttershoek

Telefoon: (078) 629 59 99
E-mail: secretariaat@dehoekscheschool.nl
Website: www.dehoekscheschool.nl

Inhoudsopgave

Inleiding

Stichting De Hoeksche School verzorgt het openbaar primair en voortgezet onderwijs in de Hoeksche Waard. De Hoeksche School ontstond op 1 augustus 2019, na een statutenwijziging van Stichting Acis voor openbaar primair onderwijs Hoeksche Waard en de daaropvolgende fusie met Stichting Openbaar Voortgezet Onderwijs Hoeksche Waard (OVO).

Op 19 september 2018 is het Protocol beveiligingsincidenten en datalekken van Stichting Acis vastgesteld; op 2 november 2018 is hetzelfde protocol vastgesteld voor Stichting OVO. De tekst van beide protocollen is gelijkluidend en is hieronder samengevoegd. De vermeldingen ‘Acis’ en ‘OVO’ zijn echter vervangen door ‘De Hoeksche School’.

Dit protocol biedt een handleiding voor de melding, beoordeling en afhandeling van Beveiligingsincidenten en Datalekken binnen onze organisatie. In het protocol is vastgelegd hoe en naar wie de meldingen intern doorgezet dienen te worden, wie verantwoordelijk is voor welke melding en hoe en in welke vorm de melding aan de Autoriteit Persoonsgegevens en eventueel ook aan de Betrokkenen wordt gedaan.

Toepassingsgebied

Dit Protocol wordt gehanteerd bij het melden en afhandelen van (mogelijke) Beveiligingsincidenten binnen onze organisatie, dan wel (mogelijke) Beveiligingsincidenten die buiten onze organisatie hebben plaatsgevonden, maar waarvoor wij als Verwerkingsverantwoordelijke verantwoordelijkheid dragen (bijvoorbeeld als een Beveiligingsincident zich bij een Verwerker van ons voordoet).

Om te zorgen voor een eenduidig beleid binnen onze organisatie en om te voorkomen dat (mogelijke) Beveiligingsincidenten niet (tijdig) worden opgemerkt en eventueel niet (tijdig) worden gemeld, hebben wij er voor gekozen om de meldingen van Beveiligingsincidenten centraal te laten verlopen. Om die reden is het van belang dat iedereen weet hoe er gehandeld dient te worden zodra hij of zij een Beveiligingsincident ontdekt of hem of haar dit ter ore komt. Dit Protocol voorziet daar in en is van toepassing op de hele organisatie en al haar (externe) medewerkers.

In dit Protocol worden onder meer de volgende termen gebruikt:

- **Persoonsgegeven:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. In ons geval gaat het dan om leerlinggegevens, gegevens van ouders, leerkrachten en van de personen die voor ons werkzaam zijn;
- **Betrokkene:** de persoon op wie de Persoonsgegevens betrekking hebben;
- **Beveiligingsincident:** een gebeurtenis (niet uitsluitend digitaal!) die er voor 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 organisatie;
- **Datalek:** een Beveiligingsincident (niet uitsluitend digitaal!) waarbij Persoonsgegevens verloren raken of onrechtmatig worden verwerkt (denk aan: opgeslagen, aangepast, verzonden, et cetera) of als dit niet uit te sluiten is.
  Alle Datalekken zijn dus Beveiligingsincidenten, maar niet alle Beveiligingsincidenten zijn Datalekken.
  Bij ieder Beveiligingsincident zal moeten worden vastgesteld of er sprake is van een Datalek. 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 het eindverslag van de ondersteuningscommissie, is ook een datalek.

Wat te doen

Er zijn tenminste vier rollen die onderscheiden moeten worden om een (mogelijk) Beveiligings-incident succesvol af te handelen:

1. Het begint bij de **Ontdekker.** Dit is degene die een (mogelijk) Beveiligingsincident op het spoor komt en het proces in werking stelt. Dat kan dus iedere (externe) medewerker zijn. Indien een ouder, leerkracht, relatie of andere derde een (mogelijk) Beveiligingsincident opmerkt, is het zaak dat hij/zij dit onmiddellijk meldt bij de directie van de school. De directie wordt dan voor de uitvoering van de te volgen stappen in het kader van dit protocol aangemerkt als Ontdekker.
2. Het **Meldpunt.** Dit is een centrale locatie/persoon binnen de organisatie waar alle (mogelijke) Beveiligingsincidenten door de Ontdekker dienen te worden gemeld. In ons geval is dit de Functionaris Gegevensbescherming (FG)/het college van bestuur. Het Meldpunt is hiervoor bereikbaar via het e-mailadres **FG@dehoekscheschool.nl** (cc naar l.vanheeren@dehoekscheschool.nl) of telefonisch (078-6295999).

3. De **Melder** wordt geïnformeerd door het Meldpunt. De Melder is degene die verantwoordelijk is voor het beoordelen van het Beveiligingsincident en het eventueel melden van een Datalek bij de Autoriteit Persoonsgegevens en (indien van toepassing) de Betrokkene(n). In ons geval is dat de Functionaris Gegevensbescherming. Eveneens bereikbaar via bovenstaand e-mailadres.
4. De **Technicus** ondersteunt het Meldpunt en de Melder bij het onderzoek naar de oorzaak van het Beveiligingsincident en het (laten) repareren van het Beveiligingsincident, althans het beperken van de gevolgen daarvan.

Hieronder, bij de beschrijving van alle stappen die worden doorlopen, is het bovenstaande nader uitgewerkt.

De stappen die worden doorlopen bij een (mogelijk) Beveiligingsincident:

1. **Ontdekken:** ***door alle (externe) medewerkers***
   - De Ontdekker merkt een (mogelijk) Beveiligingsincident op.
     Dit kan via eigen waarneming of via waarneming van een derde. Een derde kan een van onze Verwerkers zijn, maar dit kan ook een ouder, leerkracht, relatie of andere derde zijn.
     Indien een ouder, leerkracht, relatie of andere derde een (mogelijk) Beveiligingsincident opmerkt, is het zaak dat hij/zij dit onmiddellijk meldt bij de directie van de school. De directie wordt dan voor de uitvoering van de te volgen stappen in het kader van dit protocol aangemerkt als Ontdekker.

   - De Ontdekker meldt het door hem of haar opgemerkte (mogelijke) Beveiligingsincident per ommegaande bij het Meldpunt via **FG@dehoekscheschool.nl** (met CC naar l.vanheeren@dehoekscheschool.nl) of eventueel telefonisch via telefoonnummer 078-6295999. Een e-mail heeft de voorkeur. Bij het onderwerp van de e-mail moet "(mogelijk) Beveiligingsincident" worden vermeld, zodat voor het Meldpunt direct duidelijk is waar het om gaat. Bovendien moet de e-mail als "urgent" worden verzonden.

   - Voor de melding bij het Meldpunt maakt de Ontdekker gebruik van het als **Bijlage 1** aangehechte meldingsformulier. De Ontdekker vult dit formulier zoveel als mogelijk in.

2. **Inventariseren en vastleggen:** ***door het Meldpunt***
   - Het Meldpunt gaat zo spoedig mogelijk alle relevante informatie met betrekking tot het (mogelijke) Beveiligingsincident verzamelen en vastleggen.
     Het Meldpunt kan daarvoor aanvullende vragen uitzetten bij de Ontdekker en/of de Technicus.

   - De volgende informatie wordt door het Meldpunt verzameld en vastgelegd:
     - een samenvatting van het Beveiligingsincident;
       waar heeft het incident plaats gevonden en wat is er met de gegevens gebeurd?;
     - aard van de inbreuk;
     - datum/periode van het Beveiligingsincident;
     - vond het Beveiligingsincident plaats in een verwerking die is uitbesteed aan een andere organisatie (een Verwerker), zo ja, wat is de naam van de Verwerker;
     - een nadere omschrijving van:
       - de categorieën van Betrokkenen (leerlingen, ouders, leerkrachten etc.);
       - (bij benadering) het aantal Betrokkenen;

- type persoonsgegevens in kwestie;
- worden de gegevens binnen een keten gedeeld;
- de vooralsnog bekende en/of te verwachten gevolgen die het Beveiligingsincident voor de persoonlijke levenssfeer van de Betrokkenen kan hebben;
- de mogelijke technische beschermingsmaatregelen die zijn genomen (denk aan versleuteling, encryptie, hashing etc.);
- of het Beveiligingsincident eventueel betrekking heeft op Betrokkene(n) in andere landen binnen de EER of daarbuiten;
- de technische en organisatorische maatregelen die zijn getroffen om het Beveiligingsincident aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan, uiteraard voor zover de oorzaak daarvan bekend is;
- indien van toepassing, binnen welke keten de Persoonsgegevens in kwestie worden gedeeld.

Alle informatie die wordt verzameld dient schriftelijk te worden **vastgelegd**. Hiervoor kan het eerste tabblad van het "Datalekregister" worden gebruikt.

3. **Beoordelen:** ***door de Melder***

- Wanneer het Meldpunt voldoende informatie heeft verzameld, stuurt het Meldpunt de Melder (in ons geval de Functionaris Gegevensbescherming) een verzoek om de verzamelde informatie te bekijken.

- De Melder beoordeelt de feiten om te bepalen of er sprake is van een Beveiligingsincident en zo ja, of dit Beveiligingsincident is aan te merken als een Datalek. De Melder deelt zijn bevindingen met het college van bestuur.

- Indien er sprake is van een Datalek, beoordeelt de Melder vervolgens of het Datalek moeten worden gemeld aan de Autoriteit Persoonsgegevens. Immers niet alle Datalekken hoeven te worden gemeld aan de Autoriteit Persoonsgegevens. Volgens de wet moet een "ernstig" Datalek worden gemeld aan de Autoriteit Persoonsgegevens.

  Een Datalek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig). Daarnaast kan een Datalek ook ernstig zijn indien er geen grote hoeveelheden persoonsgegevens gelekt zijn, maar het wel om gevoelige persoonsgegevens gaat (kwalitatief ernstig). Dit laatste is bijvoorbeeld aan de orde als het gaat om bijzondere persoonsgegevens, persoonsgegevens over de financiële of economische situatie van de Betrokkene(n), of als de gegevens kunnen leiden tot stigmatisering van de Betrokkene(n). De aard (het type) en de omvang (de hoeveelheid) van het Datalek spelen dus beide een belangrijke rol bij de beoordeling of melding aan de Autoriteit Persoonsgegevens noodzakelijk is.

  Anders gezegd, indien het Datalek leidt tot ernstige nadelige gevolgen voor de bescherming van Persoonsgegevens, of de kans daarop aanzienlijk is, moet het Datalek gemeld worden aan de Autoriteit Persoonsgegevens.

- Onder stap 5. wordt nader ingegaan op de wijze waarop de melding aan de Autoriteit Persoonsgegevens zal plaatsvinden.

- Indien er sprake is van een Datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens, beoordeelt de Melder vervolgens of het Datalek ook moet worden gemeld aan de Betrokkene(n). Dit is namelijk niet automatisch het geval. Hiervoor moet onder andere worden gekeken of het Datalek kan leiden tot fysieke, materiële of immateriële schade voor de Betrokkene(n). Zoals: discriminatie, (identiteits-)fraude, financiële schade en reputatieschade.

- De melding aan Betrokkene(n) mag achterwege worden gelaten als:
  - er, voordat het Datalek plaats vond, passende maatregelen zijn getroffen waardoor de gelekte Persoonsgegevens onbegrijpelijk zijn voor onbevoegden.
    Let op: deze uitzondering geldt alleen maar als:
    (1) de gegevens nog volledig intact zijn;
    (2) er nog steeds volledige controle is over de gegevens;
    (3) de sleutel die voor de encryptie of voor de hashing is gebruikt bij de inbreuk geen gevaar heeft gelopen en voor onbevoegden met de beschikbare technologische middelen niet te vinden is;
  - er, onmiddellijk nadat het Datalek heeft plaatsgevonden, maatregelen zijn getroffen waardoor het hoge risico voor de rechten en vrijheden van Betrokkene(n) zich waarschijnlijk niet meer zal voordoen (bijvoorbeeld doordat de gelekte Persoonsgegevens onmiddellijk na het Datalek zijn gewist, nog voordat de onbevoegde ontvanger iets met de gegevens kon doen);
  - wanneer het niet melden noodzakelijk en evenredig is ter waarborging van: a. de nationale veiligheid; b. landsverdediging; c. de openbare veiligheid; d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

- Onder stap 5. wordt nader ingegaan op de wijze waarop de melding aan de Betrokkene(n) zal plaatsvinden.

- **Kortom**, door de Melder (de Functionaris Gegevensbescherming) moeten de volgende vragen worden beantwoord:
  - is er sprake van een Datalek?;
  - heeft dit Datalek mogelijke gevolgen voor de persoonlijke levenssfeer van de Betrokkene(n);
  - wordt het Datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
  - wordt het Datalek aan betrokkene(n) gemeld? Waarom niet?
  - hoe worden meldingen gedaan? Wat is de inhoud van de melding?

- Bij ieder Beveiligingsincident wordt beoordeeld of er aanwijzingen zijn voor of vermoedens van strafbaar handelen (zoals bijvoorbeeld hacken). Indien dit het geval is, kan aangifte worden gedaan bij de Politie.

- Als een (externe) medewerker het niet eens is met de beslissing van de Melder om een (vermoedelijk) Datalek wel - of niet te melden aan de Autoriteit Persoonsgegevens en/of de Betrokkene(n), dan richt hij of zij zich tot het college van bestuur teneinde zijn of haar bedenkingen aldaar te bespreken. Het is de (externe) medewerker niet toegestaan om een (vermoedelijk) Datalek zelf aan de Autoriteit Persoonsgegevens en/of de Betrokkene(n) te melden. Zie ook onder punt 5. bij “Communicatie”.

4. **Maatregelen treffen:** ***door de Technicus***
   De Technicus wordt door het Meldpunt en/of de Melder gevraagd (voor zover dat nog niet is gebeurd en voor zover mogelijk) de oorzaak van het Beveiligingsincident vast te stellen en (technische) maatregelen te treffen om het Beveiligingsincident te (laten) verhelpen en de gevolgen van het Beveiligingsincident te beperken. Ook wordt de Technicus gevraagd (technische) maatregelen te treffen om herhaling van het Beveiligingsincident te voorkomen. Deze maatregelen worden zo spoedig mogelijk in gang gezet.

5. **Melden:** ***door de Melder***
   Bij de Autoriteit Persoonsgegevens
   Indien de conclusie bij stap 3. is dat er sprake is van een Datalek dat bij de Autoriteit Persoonsgegevens gemeld dient te worden, dan zal de Melder dit **binnen 72 uur** na het ontdekken van het Datalek melden. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Als nog niet alle informatie over het Datalek bekend is, zal alvast een incomplete melding worden gedaan, zodat de Autoriteit Persoonsgegevens tijdig is geïnformeerd.

   Het Datalek wordt gemeld bij het Meldloket datalekken Autoriteit Persoonsgegevens: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

   Bij de Betrokkenen
   Indien de conclusie bij stap 3. is dat een Datalek ook moet worden gemeld aan de Betrokkene(n), dan dient melding onverwijld plaats te vinden.

   De melding aan Betrokkene(n), dient in ieder geval behoorlijk en zorgvuldig uitgevoerd te worden, en de volgende informatie te bevatten:
   - aard van de inbreuk, waarbij volstaan kan worden met een algemene omschrijving van wat er is gebeurd;
   - waar men terecht kan met vragen, denk hierbij aan het telefoonnummer/e-mailadres van de Functionaris Gegevensbescherming of een speciaal telefoonnummer/e-mailadres voor vragen;
   - aanbevolen maatregelen om negatieve gevolgen te beperken, zoals het veranderen van wachtwoorden.

   De Betrokkene(n) dienen in beginsel individueel te worden geïnformeerd, maar als het individueel informeren van de Betrokkene(n) een onevenredige inspanning vergt, bijvoorbeeld omdat de contactgegevens van de Betrokkene(n) door het Datalek verloren zijn gegaan, dan mogen de Betrokkene(n) ook worden geïnformeerd met een openbare mededeling of een soortgelijke maatregel, waarbij de Betrokkene(n) even doeltreffend worden geïnformeerd.

   Communicatie
   Bij het melden aan de Autoriteit Persoonsgegevens en eventueel de Betrokkene(n) en/of de politie is de communicatie een belangrijk punt van aandacht. Het is van groot belang dat alle communicatie (zowel geschreven pers, social media platform alsmede alle overige communicatieplatforms) uitsluitend via de Melder in overleg met het college van bestuur plaatsvindt. **Ieder ander dient zich te allen tijde te onthouden van enig commentaar** en hiervoor te verwijzen naar de Melder en/of het college van bestuur. **Ook dient ieder ander zich te onthouden van uitlatingen op eigen initiatief in welke vorm dan ook**.

6. **Registratie:** ***door het Meldpunt***
   Alle informatie, die in de voorafgaande stappen met betrekking tot een Beveiligingsincident is ingewonnen of ontstaan, wordt door het Meldpunt (in samenspraak met de Melder) geregistreerd in het “Datalekregister". Met de voornoemde registratie wordt het afhandelen van het Beveiligingsincident afgesloten.

   Nota bene, de registratie hoeft niet openbaar te worden gemaakt.

Voornoemde stappen zijn hieronder in **Bijlage 2** nog eens **schematisch** weergegeven.

Beheer beveiligingsincidenten

Het college van bestuur maakt twee keer per jaar een analyse van alle meldingen van beveiligings-incidenten die zij heeft ontvangen in samenwerking met de Functionaris Gegevensbescherming.
In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om extra maatregelen te nemen om herhaling te voorkomen.

Bijlage 1: Meldingsformulier

Naam Ontdekker:

Contactgegevens Ontdekker:
E-mail:
Telefoon:

Datum / periode van het (mogelijke) Beveiligingsincident:

Heeft het (mogelijke)Beveiligingsincident binnen de organisatie plaatsgevonden:
Ja, vermeld waar / Nee, vermeld waar wel / Weet ik niet:

Omschrijving van de toedracht van het (mogelijke) Beveiligingsincident:

Zijn er persoonsgegevens bij het (mogelijke) Beveiligingsincident betrokken:
Ja / Nee / Weet ik niet

Zo ja, omschrijf welke persoonsgegevens betrokken zijn (type, hoeveelheid, etc.):

Zo ja, welke categorieën van Betrokkenen gaat het om en geef een inschatting van het aantal Betrokkenen per categorie:

Welke technische en/of organisatorische beschermingsmaatregelen zijn genomen (denk aan versleuteling, encryptie, hashing etc):

Welke mogelijke gevolgen heeft het (mogelijke) Beveiligingsincident:

Welke technische en/of organisatorische maatregelen zijn er reeds genomen om het (mogelijke) Beveiligingsincident aan te pakken, om de gevolgen te beperken en/of om in de toekomst te voorkomen:

Bijlage 2: Schematische weergave te nemen stappen

Wie?	Actie	Opmerkingen
	Stap 1: Ontdekken	
Alle (externe) medewerkers (**Ontdekker**)	Ontdekken / ter ore komen (mogelijk) Beveiligingsincident	
Alle (externe) medewerkers (**Ontdekker**)	Melden (mogelijk) Beveiligingsincident bij **Meldpunt**	
	Stap 2: Inventariseren en vastleggen	
Meldpunt / eventueel met ondersteuning **Technicus**	Verzamelen informatie met betrekking tot het Beveiligingsincident en registreren in register	Zie overzicht in protocol bij **Stap 2**
Meldpunt	Verzamelde informatie ter beoordeling voorleggen aan **Melder**	
	Implementeren van maatregelen (**Stap 4**)	
	Stap 3: beoordelen	
Melder (in overleg met college van bestuur)	Vaststellen of er sprake is van een Datalek	
	Ja: ↓ Implementeren van maatregelen (**Stap 4**)	**Nee:** Er is mogelijk wel sprake van een Beveiligingsincident; - implementeren van maat-regelen (**Stap 4**); - sluiting melding en registratie in register (**Stap 6**)
Melder (in overleg met college van bestuur)	Vaststellen of Datalek moet worden gemeld aan de Autoriteit Persoonsgegevens	
Bij **Nee: Meldpunt & Technicus** (in samenspraak met Melder)	**Ja:** ↓ Implementeren van maatregelen (**Stap 4**)	**Nee:** - implementeren van maat-regelen (**Stap 4**); - sluiting melding en registratie in register (**Stap 6**)
Melder / eventueel met ondersteuning **Technicus**	Indien nodig: verzamelen nadere informatie Datalek ten behoeve van melding bij Autoriteit Persoonsgegevens	
Melder (in overleg met college van bestuur)	Melding bij Autoriteit Persoonsgegevens (**Stap 5**)	
Melder	Vaststellen of Datalek moet worden gemeld aan de Betrokkene(n)	
Bij **Nee: Meldpunt & Technicus** (in samenspraak met Melder)	**Ja:** ↓ Implementeren van maatregelen (**Stap 4**)	**Nee:** - Implementeren van maat-regelen (**Stap 4**); - sluiting melding en registratie in register (**Stap 6**)
Melder (in overleg met college van bestuur)	Melding aan Betrokkene(n) (**Stap 5**)	Evt. raadplegen communicatie-deskundige
Technicus	Implementeren eventuele resterende maatregelen (**Stap 4**)	

Meldpunt (in samenspraak met Melder)	Sluiting melding en registratie in register (**Stap 6**)	