

**Protocol
informatiebeveiligingsincidenten en
datalekken**

Inhoud

Inleiding.....	2
Wet- en regelgeving datalekken	2
Afspraken met leveranciers	3
Werkwijze	3
Uitgangssituatie	3
De vier rollen	3
De zeven stappen	3
Monitoring beveiligingsincidenten en datalekken	5
Communicatie.....	5

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van het Staring College.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen en afhandelen van beveiligingsincidenten en datalekken.

Dit protocol is van toepassing op de gehele organisatie van het Staring College, zoals vermeld in het IBP beleid en al haar medewerkers.

Gebruikte termen:

- **Beveiligingsincident;** een beveiligingsincident is een gebeurtenis 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 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.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplichting 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 je leerlingadministratie 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.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens in handen vallen van personen die daartoe geen bevoegdheid hebben. 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 klas 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een verwerker voor de school. Er kan worden afgesproken dat een verwerker 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. Bij stap 5 van het stappenplan is te lezen hoe dit gedaan wordt.

Afspraken met leveranciers

De afspraken met leveranciers staan in de verwerkersovereenkomsten die afgesloten zijn.

Werkwijze

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en/of gedragscode ict en internetgebruik.

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.
2. **Meldpunt (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens. Waar een datalek gemeld dient te worden is terug te lezen in stap 5 van het stappenplan.
4. **Verantwoordelijke voor het proces waar het datalek is ontstaan**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren. Voor digitale zaken is dit bijvoorbeeld netwerkbeheer.
5. **Schoolbestuur**; is de eindverantwoordelijke. De melder heeft een informatieplicht aan het schoolbestuur. Dit betekent dat de melder het schoolbestuur in moet schakelen en op de hoogte moet brengen van eventuele datalekken.

De zeven stappen

1. Ontdekken

De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker zal het incident zo snel mogelijk schriftelijk melden bij privacy@staring.nl. Hierna zal er contact opgenomen worden met de bestuurder en gezamenlijk de verder te ondernemen stappen worden bepaald. Bij het melden van het incident is snelheid gewenst aangezien er binnen 72 uur een melding bij de Autoriteit Persoonsgegevens gedaan moet worden.

2. Inventariseren

Het Meldpunt bepaalt dan 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 daarna vastgelegd:

- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Wanneer van toepassing (bij een datalek):
 - Omschrijving van de groep betrokkenen
 - Aantal betrokkenen
 - Type persoonsgegevens in kwestie
 - Worden de gegevens binnen een keten gedeeld

Bij het verzamelen van deze informatie is wederom snelheid gewenst aangezien er binnen 72 uur een melding bij de Autoriteit Persoonsgegevens gedaan moet worden.

3. Beoordelen

Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt de feiten om, in overleg met de bestuurder, te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is. Tevens adviseert de melder de bestuurder over de vervolgstappen.

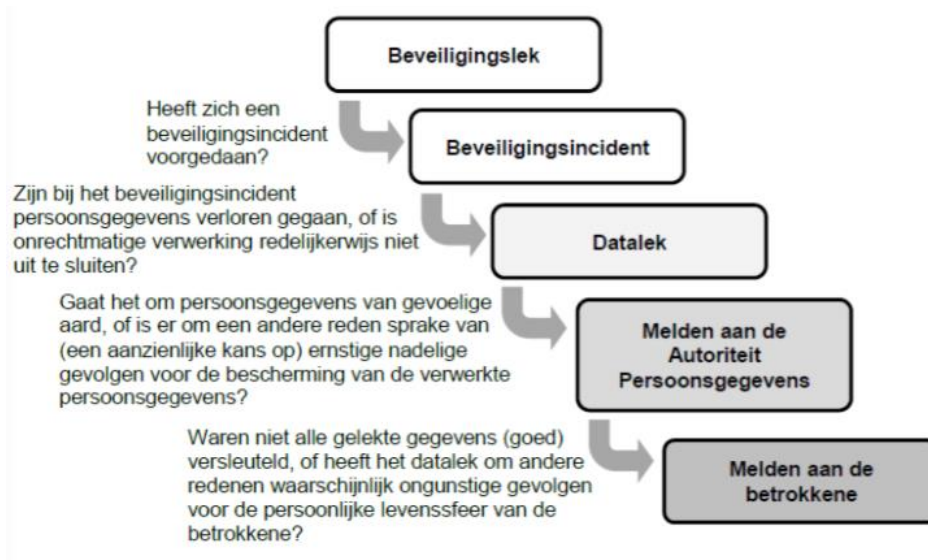
De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', hou je rekening 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 (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom kan gebruikt worden



4. Procedures

De Technicus (intern of extern) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van het Staring College legt onderstaande vast:

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.

- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

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 Melder dit binnen twee werkdagen 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>.

6. Vastleggen

Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident juridisch is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker. Daarnaast zullen de melder en bestuurder samen beslissen over eventuele nazorg en herhalingsacties.

7. Informeren betrokkene: leerling en/of zijn ouders

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan er van worden uitgegaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van het Staring College maakt een keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de functionaris gegevensbescherming. In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen. Het schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse om eventueel maatregelen te nemen en zich te kunnen verantwoorden.

Communicatie

Met alle betrokkenen van het Staring College zal gecommuniceerd worden doormiddel van internet, intranet, Staring Contact nieuwsbrief en mail. Via deze kanalen zal de benodigde informatie worden verstrekt. Wanneer betrokkenen zelf signalen opmerken over een mogelijk datalek dienen ze dit te melden door te mailen naar privacy@staring.nl.

Om te zorgen dat de juiste informatie gecommuniceerd kan worden schakelt het Staring College de hulp in van een Functionaris gegevens bescherming en van de expertise van Kennisnet.

onderwerp	Protocol informatiebeveiligingsincidenten en datalekken	
datum	oktober 2018	
kenmerk	4076.1819	vervangt: n.v.t.
verantwoordelijke	directie	
vastgesteld	d.d.: 11 oktober 2018	door: DV
MR	n.v.t.	d.d. n.v.t.