PROTOCOL BEVEILIGINGSINCIDENTEN EN DATALEKKEN

Stichting Vrije Scholen Zuidwest Nederland

Versie: januari 2020

INHOUDSOPGAVE

Inleiding 3

1 Wet- en regelgeving 4

2 Afspraken met leveranciers 5

3 Werkwijze 6

3.1 De vier rollen 6

3.2 De zeven stappen 7

4 Communicatie 12

4.1 Communicatie betrokkenen en pers bij datalekken 12

4.2 Signalen van derden over mogelijk datalek 12

5 Controle en rapportage 13

Inleiding

Voor u ligt het protocol beveiligingsincidenten en datalekken. Dit protocol dient als verlengstuk van het Informatiebeveiligings- en privacybeleid.

Door middel van dit protocol kan er professioneel en adequaat worden gehandeld wanneer er sprake is van een beveiligingsincident en/of een datalek. Door het doorlopen van de juiste procedures worden incidenten op een correcte juridische wijze afgehandeld. Tevens dient dit protocol als ondersteuning voor het verminderen en voorkomen van beveiligingsincidenten en datalekken.

Dit protocol informatiebeveiliging en datalekken is van toepassing voor alle medewerkers, externen, ouders en leerlingen van De Stichting Vrije Scholen Zuidwest Nederland (Stichting ZWN).

In dit protocol wordt er gebruikt gemaakt van een aantal 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 verwerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- ***Betrokkene;***
  de persoon van wie de persoonsgegevens zijn gelekt.

1 Wet- en regelgeving

Sinds de invoering van de Wet meldplicht datalekken op 1 januari 2016 zijn ook scholen verplicht om melding te maken bij de Autoriteit Persoonsgegevens wanneer er sprake is van een (ernstig) datalek. Scholen riskeren een boete wanneer zij dit verzaken.

Een voorbeeld van een datalek is als er bij een inbraak servers worden ontvreemd waarop persoonsgegevens zijn opgeslagen. Dit kan gaan om (gevoelige) leerling informatie, maar ook gegevens van medewerkers. Ook het verlies van een smartphone van een leerkracht met daarop de informatie van een klas kan worden aangemerkt als een datalek. Bij een datalek 'is' of 'kan niet worden uitgesloten dat' er persoonsgegevens verloren zijn gegaan.

De meldplicht voor datalekken geldt alleen bij het lekken van persoonsgegevens. De meldplicht geldt voor de verantwoordelijke van de persoonsgegevens, het schoolbestuur. In veel gevallen kan de school het verwerken van persoonsgegevens uitbesteden aan derden. Deze leveranciers zoals uitgevers of distributeurs treden op als verwerkers van de persoonsgegevens namens de school. Met verwerkers moet een school ook afspraken maken over het melden van datalekken. Dit kan worden opgenomen in de verwerkersovereenkomst.

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

2 Afspraken met leveranciers

In een verwerkersovereenkomst worden afspraken gemaakt met betrekking tot de verwerking van de persoonsgegevens namens de school. Afspraken over datalekken worden daarin ook geregeld. Onderwerpen die in deze overeenkomst moeten worden opgenomen zijn:

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatie gegevens de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

De afspraken – waaronder de afspraken over datalekken- met de verwerker(s) dienen schriftelijk te worden gemaakt.

3 Werkwijze

Om een goed en correct databeveiligingsprotocol te kunnen uitvoeren zijn er een aantal randvoorwaarden. Deze randvoorwaarden betreffen het informatiebeveiligings- en privacy beleid. Deze moet actueel zijn, regelmatig geëvalueerd en zo nodig worden bijgestuurd.

Daarnaast is het van belang dat er een actuele gedragscode over het aanvaardbaar gebruik van bedrijfsmiddelen van toepassing is. En een zgn. 'online protocol' met daarin gedragsregels voor het gebruik van ICT, internet en social media.

3.1 De vier rollen

Er zijn ten minste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

Ontdekker; degene die het beveiligsingsincident of datalek op het spoor komt en het proces in werking stelt.

Meldpunt; een centraal person en locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt in het incidentenregister.

Melder (Functionaris Gegevensbescherming); degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.

Technicus (security officer/ict coördinator); degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

3.2 De zeven stappen

3.2.1 Ontdekken

De ontdekker merkt een beveiligingsincident of datalek op. Via eigen waarneming of via waarneming van een derde. Bij twijfel of sprake is van een datalek kan worden afgestemd met de bestuurssecretaris van de Stichting ZWN, Anna Italianer (a.italianer@vszh.nl). De ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het meldpunt via de Functionaris Gegevensbescherming van de Stichting ZWN: Arnelieke de Bondt (a.debondt@goc-consultants.nl). Daarnaast wordt het incident gemeld bij de schoolleiding (hoofd bedrijfsvoering).

3.2.2 Inventariseren

Het meldpunt bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de ontdekker en/of de technicus (systeembeheerder)van de Stichting ZWN Maarten de Keizer (m.de.keizer@markei.nl 088 – 747 1000)

De volgende informatie wordt vastgelegd in incidentenregister:

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

3.2.3 Beoordelen

Wanneer het meldpunt voldoende informatie heeft verzameld, stuurt deze de melder een verzoek om de verzamelde informatie te bekijken. De melder beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkenen vereist is.

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?

Om te kunnen inschatten of er sprake is van ernstige nadelige gevolgen moet de melder rekening houden met diverse factoren. Bijvoorbeeld met informatie over het type persoonsgegevens, de hoeveelheid en de mogelijkheid voor ernstige nadelige gevolgen voor de betrokkene.

Van die ernstige nadelige gevolgen, of de kans daarom, 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 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:

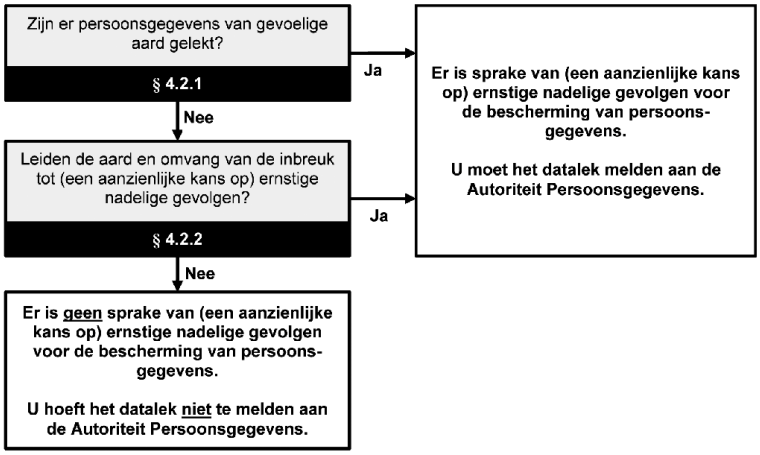
3.2.4 Repareren

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

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voor zover de oorzaak bekend is.
- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Zijn gegevens gepseudonimiseerd? Hoe zijn de gegevens versleuteld?

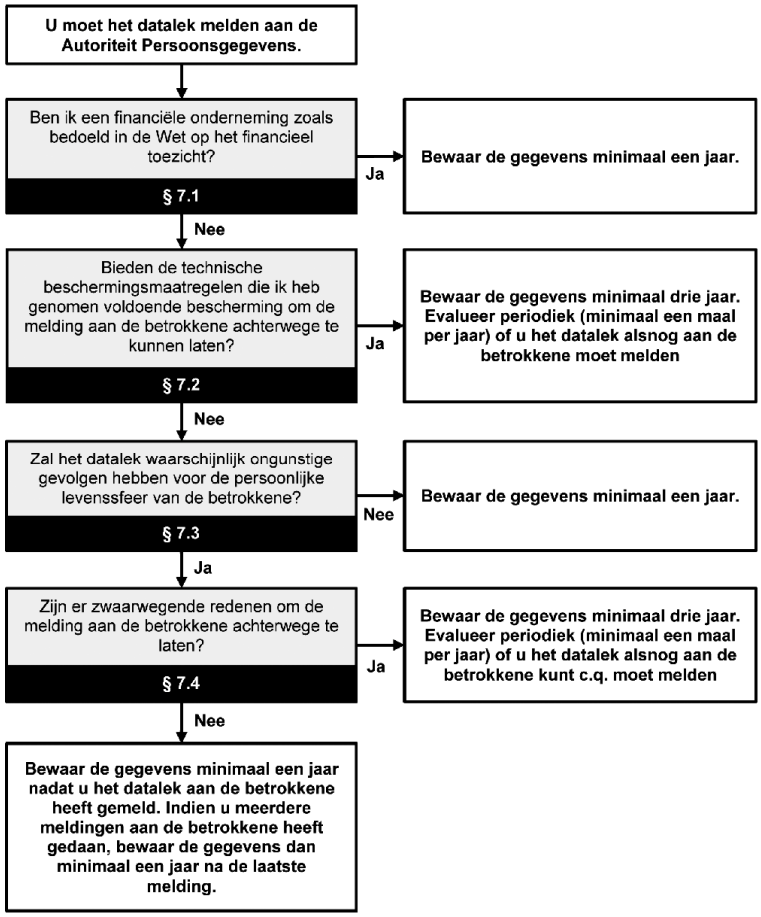
3.2.5 Melden

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 72 uur** doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij de Autoriteit Persoonsgegevens.



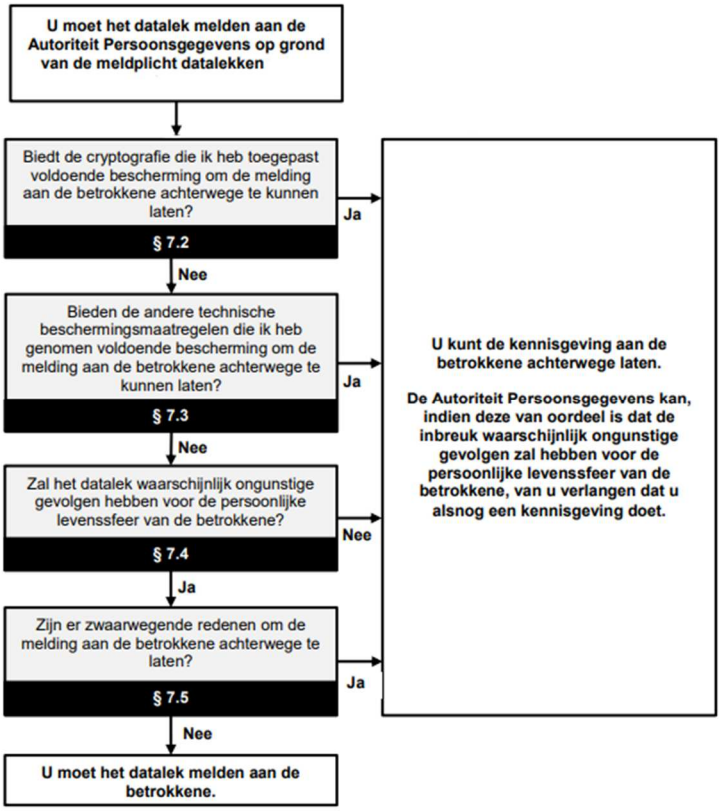
3.2.6 Vastleggen

Het meldpunt is verantwoordelijk voor de juiste afwikkeling van alle verworven informatie en documentatie over het incident. Onder afwikkeling wordt mede verstaan, het informeren van de ontdekker en archiveren van alle documentatie en bewaren volgens onderstaand schema.



3.2.7 Informeren betrokkene: leerling en/of de 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 uitgaan dat het lekken van gevoelige aard 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.



4 COMMUNICATIE

4.1 COMMUNICATIE BETROKKENEN EN PERS BIJ DATALEKKEN

Wanneer er sprake is van een ernstig datalek met gevolgen voor betrokkene, dan moet de betrokkene ook worden geïnformeerd over het datalek. Daarna is het vaak een kwestie van tijd voordat de pers berichtgeving daarover naar buiten brengt. Om dit te monitoren zijn er een aantal vuistregels opgesteld.

- **Stel een woordvoerder aan**
  Door een centraal persoon aan te stellen als woordvoerder blijft de communicatie met betrokkenen en/of pers beheersbaar. Dit kan een verantwoordelijke zijn binnen het MT of de directie van de betreffende school.
- **Hou geen informatie binnen 'vier muren'**
  Het is onmogelijk om te verwachten dat de communicatie over een datalek binnen vier muren blijft. Wees open in de informatieverstrekking, op die manier is berichtgeving helder en overzichtelijk. Deel daarom de naar buiten gebrachte informatie ook via de website of andere communicatiekanalen.
- **Meld informatie zodra dit mogelijk is**
  Update berichtgeving regelmatig. Voorkom dat er speculaties uit de hand lopen. Meld het ook als er géén nieuwe informatie is.
- **Social Media**
  Blijf zelf actief op social media. Voorkom speculaties door te reageren op onjuistheden en verwijs naar de officiële berichtgeving op bijvoorbeeld de website.

4.2 SIGNALEN VAN DERDEN OVER MOGELIJK DATALEK

Signalen van derden over een mogelijk datalek kunnen zeer divers van aard zijn. Zorg dat er altijd adequaat op wordt geregeerd om mogelijke gevolgen te beperken of te voorkomen.

- **In kaart brengen mogelijk datalek**
  Breng het mogelike datalek in kaart. Is er sprake van een datalek? Wat is de omvang van het datalek? Zijn er daadwerkelijk persoonsgegevens verloren gegaan? Inventariseer of er sprake is van verlies van gegevens of dat er sprake is van een onrechtmatige verwerking.
- **Onderzoek mogelijk datalek**
  Onderzoek het mogelijke datalek als zijnde een 'reguliere ontdekking' en werk de procedure af zoals eerder in dit protocol beschreven.
- **Informeren diverse partijen**
  Breng de Autoriteit Persoonsgegevens op de hoogte wanneer de meldplicht op het datalek van toepassing is. Afhankelijk van de ernst van het lek; informeer ook eventueel de betrokkenen en derden over het ontdekken van het datalek. Geef aan of, en welke gegevens daarbij betrokken waren en welke gevolgen dit heeft.

5 Controle en rapportage

Twee maal per jaar analyseert het meldpunt samen met de Functionaris Gegevensbescherming de geregistreerde meldingen van beveiligingsincidenten en datalekken. Hierbij wordt rekening gehouden met:

- eventuele structurele ontwikkelingen
- de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen

Het schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.