PROTOCOL INFORMATIEBEVEILIGINGSINCIDENTEN EN DATALEKKEN

CSG DINGSTEDE

Inhoud

Bron: Dit document is gebaseerd op het Protocol informatiebeveiligingsincidenten en datalekken van Kennisnet, maar op punten door Verus en CSG Dingstede aangepast.

Het originele document is te vinden op: https://maken.wikiwijs.nl/bestanden/614315/Protocol%20beveiligingsincidenten%20en%20datalekken.docx

Inleiding

Het protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten van het informatiebeveiligings- en privacy beleid (IBP) van CSG Dingstede. Dit protocol biedt de richtlijnen voor de melding, beoordeling en afhandeling van zowel beveiligingsincidenten als een datalek. Het protocol is van toepassing op de gehele organisatie van CSG Dingstede, al haar medewerkers en leerlingen.

Gebruikte termen

- **Beveiligingsincident;** een beveiligingsincident is een gebeurtenis die 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, etc.). Alle datalekken zijn beveiligingsincidenten maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene;** de persoon van wie de persoonsgegevens gelekt zijn.

Wet- en regelgeving datalekken

Sinds 1 januari 2016 is de Wet meldplicht datalekken, een wijziging van de Wet bescherming persoonsgegevens ingevoerd. In de plaats van de Wbp is sinds 25 mei 2018 de Algemene Verordening Gegevensbescherming van kracht.

Datalek

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. Onderstaande zijn ook voorbeeld van een datalek:

- Verlies van een USB-stick met adresgegevens van een klas.
- Sturen van een mailing met alle adressen in het CC-veld (in plaats van BCC-veld).
- Diefstal van een laptop/tablet met leerlinggegevens.

Meldplicht

De AVG wijkt inzake de meldplicht op onderdelen af van de Wbp. Door de meldplicht blijft de verwerkingsverantwoordelijke verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een boete van maximaal € 20 miljoen of 4% van de wereldwijde inkomsten.

De meldplicht is van toepassing wanneer persoonsgegevens worden verwerkt, bijvoorbeeld in de leerlingenadministratie of in digitale leermiddelen. Als de verwerkingsverantwoordelijke gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school/scholen, dan moet de school/verwerkingsverantwoordelijke met deze verwerkers aanvullende afspraken over het melden van datalekken (in de verwerkersovereenkomst). Niet van toepassing is de meldplicht als het onwaarschijnlijk is dat de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

De meldplicht geldt voor de verwerkingsverantwoordelijke voor de persoonsgegevens, dat is het schoolbestuur. Een leverancier is een verwerker voor de school/verwerkingsverantwoordelijke. 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 schriftelijk worden afgesproken, anders zal de verwerkingsverantwoordelijke zelf de melding moeten doen.

Indien sprake is van een datalek, moet daar binnen 72 uur na kennisneming door verantwoordelijke van het lek, melding van worden gedaan bij de Autoriteit Persoonsgegevens. Lukt dat niet, dan zal een verklaring moeten worden gegeven voor de vertraging.

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens eveneens direct mee. Zowel de aard van de inbreuk, als de aanbevelingen over hoe de verantwoordelijke mogelijke negatieve gevolgen kan beperken, moeten aan de betrokkene gemeld worden.

Een melding aan betrokkene is niet nodig wanneer er maatregelen conform de AVG zijn getroffen en deze zijn toegepast op de betreffende persoonsgegevens. De gegevens zijn bijvoorbeeld gepseudonimiseerd, zodat degene die de gegevens in handen krijgt niet kan achterhalen welke personen de gegevens betreffen. Een melding kan ook achterwege gelaten worden als achteraf maatregelen zijn genomen door de verwerkingsverantwoordelijke om te zorgen dat de hoge risico's voor de rechten en vrijheden van betrokkene zich waarschijnlijk niet meer voor zullen doen of de mededeling onevenredige inspanning vergt.

Afspraken met leveranciers

CSG Dingstede is verantwoordelijk voor het maken van afspraken met leveranciers indien er sprake is van het ontvangen van persoonsgegevens. De afspraken over hoe te handelen in het geval van een datalek valt hier ook onder. In de verwerkersovereenkomst is vastgelegd welke gegevens zij ontvangen met welk doel en hoe zij handelen in geval van een beveiligingsincident. Hierin is vastgelegd of de leverancier of CSG Dingstede melding maakt bij de Autoriteit Persoonsgegevens, hoe de communicatie verloopt, of er een kopie van de melding wordt gestuurd en wie de communicatie naar de betrokkenen op zich neemt. Voor een model verwerkersovereenkomst kan de meest huidige versie ingezien worden via de website van www.privacyconvenant.nl, leveranciers kunnen zich aansluiten bij het convenant waardoor gemaakte afspraken gebaseerd zijn op de huidige wet- en regelgeving.

Werkwijze

Hieronder wordt het protocol rondom beveiligingsincidenten en datalek uiteengezet. De uitgangssituatie omschrijft de stand van zaken binnen CSG Dingstede. In de vier rollen wordt er gekeken naar welke personen in welke hoedanigheid betrokken zijn in het protocol. In de zeven stappen wordt uiteengezet welke handelingen ondernomen moeten worden voor een adequate afhandeling.

Uitganssituatie

Als uitgangssituatie wordt gehanteerd dat alle medewerkers binnen CSG Dingstede op de hoogte zijn van de gedragscode personeel. Hierin zitten het ICT- en internetgebruik verwerkt. Ook is er vanuit CSG Dingstede een actueel beleid op informatiebeveiliging en privacy. Minimaal tweejaarlijks worden het beleid en protocol gecontroleerd op overeenstemming. Hierop volgt een beoordeling of het beleid en protocol nog passend zijn of dat het geactualiseerd dient te worden.

De vier rollen

Onderstaande vier rollen zijn te onderscheiden als een beveiligingsincident succesvol afgehandeld dient te worden. Het kan voorkomen dat er meerdere rollen betrokken zijn. In de zeven stappen wordt aangegeven wie de rollen 2, 3 en 4 vervult binnen CSG Dingstede.

1. **De ontdekker;** dit kan iedereen binnen de organisatie zijn. Degene die het beveiligingsincident (of datalek) op het spoort komt en het gehele proces in werking stelt door hier melding van te maken.
2. **Meldpunt;** hier kan de ontdekker de melding doen. Het is een centrale locatie binnen de organisatie. Het meldpunt zorgt voor actie en registratie rondom het beveiligingsincident.
3. **Melder;** degene die namens de verwerkingsverantwoordelijke de melding maakt bij de Autoriteit Persoonsgegevens in geval van een datalek. In de praktijk zal dit de functionaris gegevensbescherming of privacy officer zijn.
4. **Technicus;** degene belast met het achterhalen van de oorzaak van het beveiligingsincident (of datalek). In de praktijk zal dit de privacy officer of afdeling ICT zijn. Zij kunnen na het achterhalen van het beveiligingsincident dit (laten) repareren.

De zeven stappen

Hieronder worden de stappen doorlopen als er een beveiligingsincident zich voordoet. Mocht het gaan om een datalek, dan moet er binnen 72 uur door de verwerkingsverant-woordelijke melding gemaakt worden bij de Autoriteit Persoonsgegevens.

1. **Ontdekken**
   De ontdekker merkt een beveiligingsincident op, dit kan gaan via eigen waarneming of de waarneming van een derde. Met deze informatie en gegevens wordt er door de ontdekker melding gemaakt bij het meldpunt. Dit kan via AVG@dingstede.nl.

2. **Inventariseren**
   Met de gegevens van de ontdekker bepaalt de privacy officer of er voldoende informatie rondom het beveiligingsincident is. Mochten er aanvullende gegevens nodig zijn, dan zal de privacy officer deze opvragen bij de juiste betrokkene. De volgende informatie wordt (op zijn minst) vastgelegd;
   - Samenvatting van het beveiligingsincident, met daarin de gegevens over wat er gebeurd is en om wat voor gegevens het gaat (bijzondere gegevens of gegevens die gevoelig zijn van aard).
   - Datum/periode van het beveiligingsincident.
   - Aard van het beveiligingsincident.
   - Aanvullend als het gaat om een datalek:
     - Omschrijving van de groep betrokkenen;
     - Aantal betrokkenen;
     - Type persoonsgegevens;
     - Worden de gegevens in een keten gedeeld.

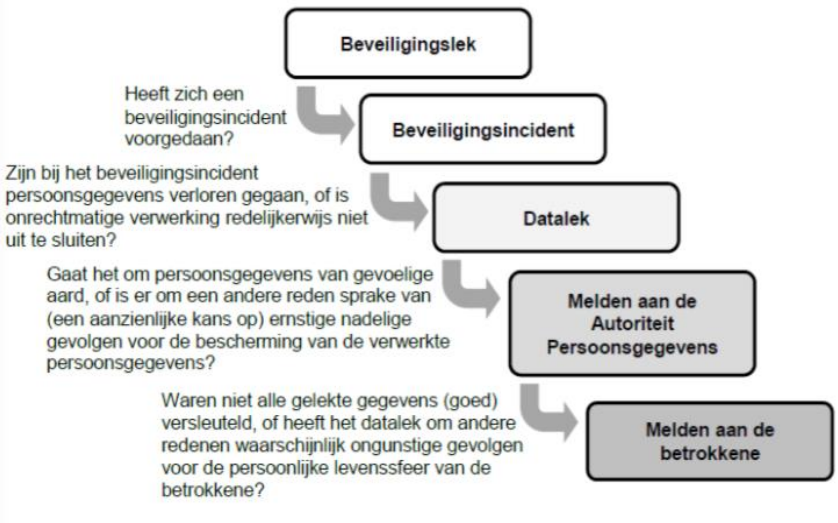
3. **Beoordelen**
   Als er voldoende informatie verzameld is door de privacy officer, en deze vermoedens heeft van een datalek, dan zal hij/zij in overleg met de rector-bestuurder de informatie beoordelen om te bepalen of er een melding gemaakt moet worden bij de Autoriteit Persoonsgegevens en of de betrokkenen ingelicht dienen te worden.

De privacy officer legt de volgende informatie vast over het beoordelingsproces:

- De mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen.
- Wordt het datalek binnen 72 uur gemeld aan de Autoriteit Persoons-gegevens? Indien nee, waarom niet?
- Wordt het datalek aan de betrokkenen gemeld? Indien nee, waarom niet?
- Hoe worden de meldingen gedaan en wat is de inhoud van de meldingen?

Bij de beoordeling of er sprake is van een meldplicht in verband met het datalek dient er rekening gehouden te worden met het type gegevens en de hoeveelheid gelekte gegevens. Als het datalek leidt tot, of de kans heeft tot, nadelige gevolgen voor de bescherming van persoonsgegevens dient er altijd gemeld te worden.

Onderstaande beslisboom kan het bestuur helpen bij het beoordelen van de informatie verschaft door het meldpunt omtrent het beveiligingsincident.



4. Repareren

De technicus wordt gevraagd om te achterhalen wat de oorzaak van het beveiligingsincident is en deze moet de oorzaak (laten) verhelpen. De technicus binnen CSG Dingstede is de ICT-afdeling. Mocht het nodig zijn, dan kunnen zij externe hulp inschakelen. De technicus legt het volgende vast:

- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en herhaling te voorkomen.
- Zijn de gelekte gegevens onbegrijpelijk voor de verkrijger? Op welke manier zijn de gegevens onbegrijpelijk gemaakt (versleuteling)?

De technische en organisatorische maatregelen worden zo gedetailleerd mogelijk vastgelegd, voor zover de oorzaak bekend is.

5. Melden

Onder stap 3 wordt door de privacy officer en de rector-bestuurder bepaald of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel de betrokkenen). Mocht er bepaald zijn dat dit het geval is, dan maakt de privacy officer binnen 72 uur de melding bij de Autoriteit Persoonsgegevens.

De melding bevat alle verzamelde gegevens en de getroffen maatregelen zoals vastgelegd door de technicus onder stap 4. De melding kan gemaakt worden via het meldloket datalekken van de Autoriteit Persoonsgegevens; https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken.
Het meldingsformulier is openbaar dus er kan gekeken worden om welke gegevens wordt gevraagd. Het kan mogelijk zijn dat niet alle informatie in één keer is te verstrekken, dan mag dit ook in stappen aangeleverd worden via een vervolgmelding.

6. **Vastleggen**
   Alle informatie die in voorafgaande stappen is ingewonnen of ontstaan wordt gearchiveerd door de privacy officer. Deze verstuurt een samenvatting van de genomen maatregelen aan de ontdekker. Hiermee wordt het beveiligingsincident afgerond.
   Een verwerkingsverantwoordelijke is, onder de AVG, verplicht om alle inbreuken vast te leggen, ook als er geen melding gemaakt is bij de Autoriteit Persoons-gegevens. Het is van belang dat er dan vastgelegd wordt wat de reden is van het niet melden.

7. **Informeren betrokkene**
   Als het datalek een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene, dan wordt het datalek direct door de verwerkingsverantwoordelijke aan de betrokkene meegedeeld. Mocht er met een verwerker een andere afspraak gemaakt zijn in een verwerkersovereenkomst, dan wordt deze gehanteerd.
   Als de gelekte gegevens onbegrijpelijk of ontoegankelijk zijn (pseudoniemen, encryptie), dan hoeft het datalek niet gemeld te worden aan de betrokkenen.

Monitoring beveiligingsincidenten en datalekken

De privacy officer van CSG Dingstede maakt jaarlijkse een analyse van de beveiligingsincidenten die zich voor hebben gedaan. Deze analyse zal, indien nodig, worden besproken met de functionaris gegevensbescherming. In de analyse wordt uiteengezet of er structurele ontwikkelingen zijn waargenomen en of er de noodzaak bestaat om maatregelen te nemen om risico's en kans op herhaling te verkleinen.

Het schoolbestuur en de (P)MR worden geïnformeerd over de uitkomsten.

Mocht er een jaar voorbijgaan zonder beveiligingsincident, dan wordt dit ook vastgelegd.