PROTOCOL INFORMATIEBEVEILIGINGSINCIDENTEN EN DATALEKKEN

Tabor College

Inhoudsopgave

Bron: Dit document is gebaseerd op het Protocol informatiebeveiligingsincidenten en datalekken van Kennisnet, maar op punten door Verus 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-beleid) van het Tabor College.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken.
Dit protocol is van toepassing op de gehele organisatie van het Tabor College, zoals vermeld in het IBP-beleid, al haar medewerkers en soms ook leerlingen.

Gebruikte termen:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die ervoor 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

Sinds 1 januari 2016 is de Wet meldplicht datalekken, een wijziging van de Wet bescherming persoonsgegevens ingevoerd. De privacyreglementen van het Tabor College zijn hier op aangepast. In de plaats van de Wbp is vanaf 25 mei 2018 de Algemene Verordening Gegevensbescherming van kracht. 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 (AP). Het nalaten van deze melding kan leiden tot een boete. Van deze datalekken dient ook de Functionaris Gegevensbescherming (FG) in kennis gesteld worden, aangezien hij voor de AP gesprekspartner in deze zaken is. Tevens kan de FG het Tabor College met raad en daad terzijde staan.

De meldplicht is van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in de leerlingenadministratie of in digitale leermiddelen. Als de school dan wel de verwerkingsverantwoordelijke gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de scholen, dan moet de 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.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is 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. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

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 van de vertraging. De FG wordt bij iedere melding betrokken. 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 aanbevelingen over hoe de verantwoordelijke mogelijke negatieve gevolgen kan beperken, moet 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

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers indien sprake is van het ontvangen van persoonsgegevens. Afspraken over datalekken vallen daar ook onder. In de verwerkingsovereenkomsten is opgenomen:

- 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 informatiegegevens de verwerker 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 verwerkers de gegevens moet aanleveren.
- Wie de communicatie met de betrokkenen voor haar rekening neemt als dat nodig is.

Werkwijze

1. Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacy beleid;
- Er is een actueel document over het ICT en internetgebruik.

2. 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/leerling)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt. Dit kan ook de verwerker zijn.
2. **Meldpunt (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. Aangeven op welke wijze het meldpunt te bereiken is. Dit meldpunt treedt op in de plaats van het schoolbestuur.
3. **Melder (functionaris gegevensbescherming** of **privacy officer)**; degene die namens de verwerkingsverantwoordelijke verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (security officer/ict coördinator)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

3. De zeven stappen

LET OP: een datalek moet wel na kennisneming door verwerkingsverantwoordelijke binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens.

1. Ontdekken

De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij de privacy officer via privacy@tabor.nl.

2. Inventariseren

Het Meldpunt (Emergency Team[1], dat handelt conform het schema ET en het onderstaande schema) 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.

[1] Het Emergency Team bestaat uit de deelnemers van het ICT-overleg (Picta). Het voorzitterschap valt bij de bestuurder van het Tabor College

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

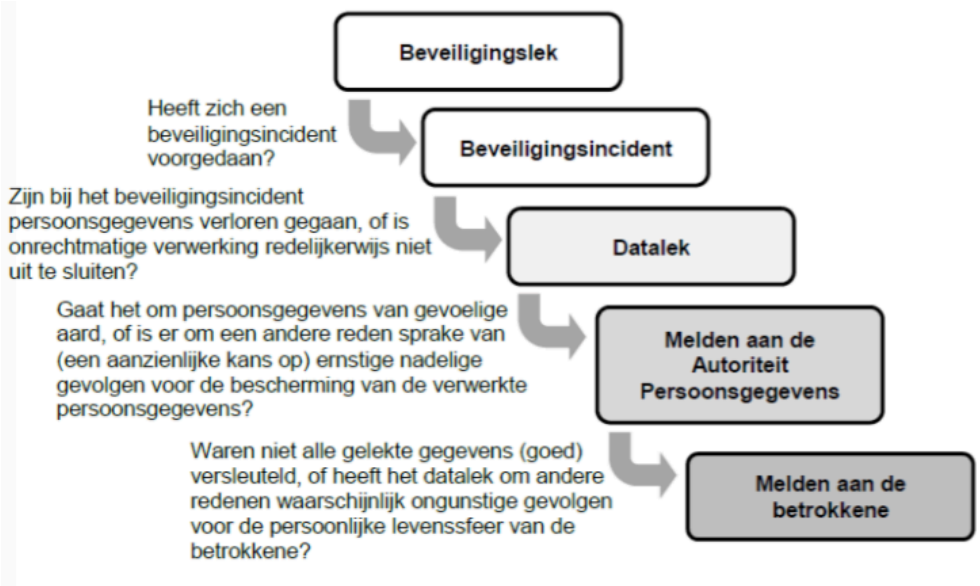
3. Beoordelen

Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoedt, 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 binnen 72 uur 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.

De onderstaande beslisboom kan gebruikt worden:



4. **Repareren**
   De Technicus (hoofd ICT van het Tabor College) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van het Tabor 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 gegevensverantwoordelijke dit binnen 72 uur doen, in samenspraak met de FG. 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/melding/aanmaken?2.

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.
   - Een verwerkingsverantwoordelijke is onder de AVG verplicht alle inbreuken te documenteren, met inbegrip van de feiten over de inbreuk, de gevolgen en de genomen corrigerende maatregelen (artikel 33, vijfde lid AVG). Hierdoor is de Autoriteit Persoonsgegevens in staat naleving van de AVG te controleren.

   NB: dit moet ook gebeuren als het incident niet hoeft gemeld te worden aan de Autoriteit Persoonsgegevens. De AVG schrijft in dat geval voor dat er beargumenteerd en gedocumenteerd moet zijn vastgelegd waarom er niet gemeld is.

7. **Informeren betrokkene: leerling en/of zijn ouders**
   Houdt het datalek een hoog risico in voor de rechten en vrijheden van natuurlijke personen, dan deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens direct mee.
   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 niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen, pseudoniemen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken

De privacy officer van het Tabor College maakt tenminste een keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met de gegevensverantwoordelijke. Deze analyse wordt besproken met de GF.

In de analyse wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

De Raad van Toezicht en de MR worden geïnformeerd over de uitkomsten van de analyse.