Protocol Informatiebeveiligingsincidenten en datalekken Winkler Prins 2019

Versie februari 2019

Winkler Prins
openbare school voor voortgezet onderwijs

Inhoudsopgave

1. Inleiding

Geregeld lezen we in de media dat gegevens van werknemers of leerlingen letterlijk op straat liggen: dossiers liggen bij het oud papier, examenwerk van leerlingen ligt in de trein, onbeveiligde usb-sticks belanden bij mensen buiten de organisatie. Wanneer persoonsgegevens in de handen vallen van derden die geen toegang tot die gegevens mogen hebben, spreken we van een datalek. Omdat we steeds meer persoonsgegevens gaan vastleggen, is er ook steeds vaker de kans dat deze gegevens bij personen terecht komen die geen recht hebben op deze gegevens.

Een datalek kan nadelige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkenen doordat de gelekte gegevens oneigenlijk gebruikt kunnen worden. Identiteitsfraude is hiervan een voorbeeld maar ook kan gedacht worden aan ongewenste profilering of doorbreking van bewust gekozen anonimiteit.
Op 1 januari 2016 is de Wet meldplicht datalekken in werking getreden. Het doel van deze wet is '*het voorkomen van datalekken ten gevolge van doorbreking van beveiligingsmaatregelen als deze zich toch voordoen, de gevolgen ervan voor betrokkenen zoveel mogelijk te beperken'.*
De Algemene Verordening Gegevensbescherming (AVG, ingegaan op 25 mei 2018) heeft deze privacywetgeving verder aangescherpt.

Dit Protocol Informatiebeveiligingsincidenten en datalekken sluit aan op deze wettelijke verplichting en bij de uitgangspunten van het informatiebeveiligings- en privacy beleid (IBP beleid) van Stichting Winkler Prins.

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

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

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 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.

2. 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 (AP). Het nalaten van deze melding kan leiden tot het opleggen van boetes door de AP.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in de leerlingadministratie of bij de 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 maken over het melden van datalekken. Dit gebeurt dan middels het afsluiten van een verwerkersovereenkomst.

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. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

De meldplicht geldt voor de eindverantwoordelijke voor de persoonsgegevens, dat is dus bestuurder. Een leverancier is een verwerker voor de school. Er kan worden afgesproken dat een verwerker **namens** de eindverantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van de eindverantwoordelijke. Dat moet wel worden afgesproken, anders zal de eindverantwoordelijke 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.

3. Afspraken met leveranciers

De bestuurder maakt als eindverantwoordelijke voor de persoonsgegevens afspraken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Daarbij wordt o.a. afgesproken:

- Hoe je elkaar informeert over datalekken, en ook zorgt voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie de melding doet 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
- De tijd waarbinnen de verwerkers de gegevens moeten aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.

Er worden schriftelijke afspraken gemaakt tussen de eindverantwoordelijke en de gebruikers over datalekken. Hiervoor wordt gebruik gemaakt van het meest recente model verwerkersovereenkomst die hoort bij het convenant “Digitale onderwijsmiddelen en privacy” (medio 2018: versie 3.0; www.privacyconvenant.nl).

4. 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:** degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt; veelal zal dat een medewerker, leerling of ouder zijn.
2. **Meldpunt:** de functionaris waar alle beveiligingsincidenten kunnen worden gemeld voor verdere verwerking; in dit geval is het de functionaris IBP.
3. **Melder:** degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens; het betreft de functionaris gegevensbescherming.
4. **Technicus:** degene die de oorzaak van het datalek kan vinden en kan (laten) repareren; het betreft de stafdirecteur ICT of iemand namens hem.

De zeven stappen

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 het meldpunt via security@winklerprins.nl.
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.

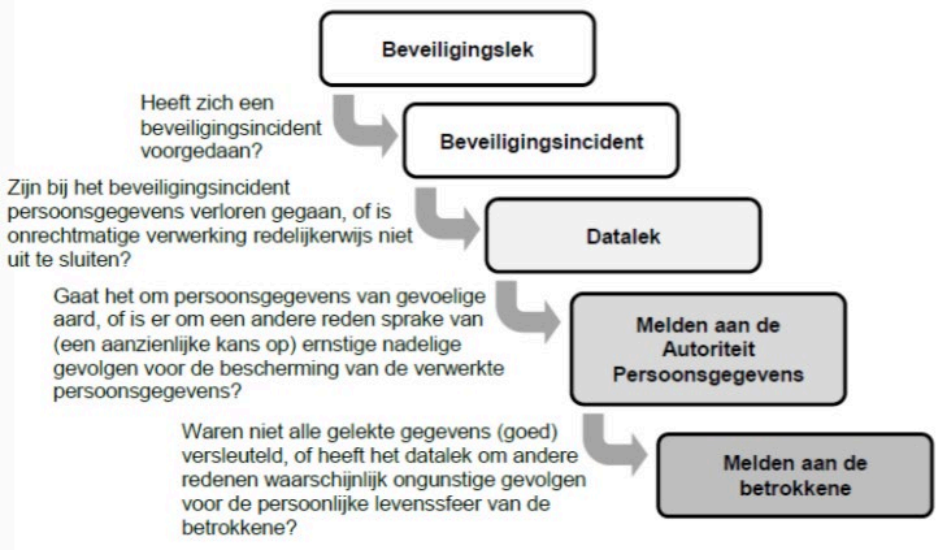
3. Beoordelen

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 gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe wordt de melding gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een meldingsplichtig datalek, wordt rekening gehouden 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 informatie over een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom kan gebruikt worden



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. 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 moeten 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 is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

7. ***Informeren betrokkene: medewerker, 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 ervan worden uitgaan dat het lekken van informatie 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. Bijvoorbeeld in het geval van het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

   De melding aan de betrokkenen bevat, in duidelijke en eenvoudige taal, ten minste:
   - een omschrijving van de aard van de inbreuk;
   - de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
   - de waarschijnlijke gevolgen van de inbreuk voor betrokkenen;
   - de maatregelen die zijn voorgesteld of genomen om de inbreuk aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

5. Monitoring beveiligingsincidenten en datalekken

Het Meldpunt maakt twee 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. De bestuurder wordt geïnformeerd over de uitkomsten van de analyse.

6. Tot slot

1. Het ‘Protocol Informatiebeveiligingsincidenten en datalekken Winkler Prins 2019’ is vastgesteld door het bevoegd gezag van Winkler Prins op 17 april 2019 nadat de medezeggenschapsraad van Winkler Prins heeft ingestemd met het beleid in de vergadering van 16 april 2019.
2. Het bevoegd gezag stelt alle belanghebbenden op de hoogte van dit beleid.
3. Het beleid is via www.winklerprins.nl te downloaden of op verzoek bij een lid van het managementteam van de school op te vragen.
4. Het beleid kan door het bevoegd gezag worden gewijzigd of ingetrokken, met inachtneming van de geldende bepalingen.