ORANJE NASSAUSCHOOL
christelijk basisonderwijs

Datalekprotocol

Protocol informatiebeveiligings-incidenten en datalekken

			Ondertekening
Vaststelling	Goedgekeurd door bestuur d.d. 23-04-2019 (20)	Ondertekend door:	A. Verburg - den Boer
Instemming MR	Goedgekeurd door MR d.d. __-__-2019 22 04 2020	Ondertekend door:	J. Voets

Inhoud

Inleiding

Op 1 januari 2016 is de **meldplicht datalekken** ingevoerd. Door deze meldplicht zijn we ook als school verplicht om melding te maken van ernstige datalekken bij de **Autoriteit Persoonsgegevens (AP)**.

Het protocol **informatiebeveiligingsincidenten en datalekken** sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacybeleid van de Oranje-Nassauschool (ONS) te Stolwijk.

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 onze hele schoolorganisatie en al onze medewerkers.

A.C. van Zaanen,

namens het schoolbestuur

Begrippen

In dit document staan een aantal begrippen, die we hieronder toelichten.

Bijzondere persoonsgegevens :	Een persoonsgegeven dat iets zegt over iemands ras, godsdienst of levensovertuiging, etnische afkomst, politieke opvattingen, seksuele voorkeur of gerichtheid, lidmaatschap van een vakbond, genetische of biometrische gegevens, en gezondheid;
Beveiligingsincident :	Een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit of vertrouwelijkheid van de informatievoorziening wordt aangetast;
Betrokkene:	De betrokkene in de zin van de wet over wie de persoonsgegevens iets zeggen;
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;
Ouder :	U als wettelijk vertegenwoordiger van uw kind, of u als verzorger of voogd.
Persoonsgegevens :	Alle informatie die een natuurlijke persoon direct of indirect kan identificeren, zoals naam, geboortedatum, geslacht etc.
Privacy :	Privacy wordt in de Nederlandse grondwet 'eerbiediging van de persoonlijke levenssfeer' genoemd;
Verwerker :	Een bedrijf, organisatie of leverancier die in opdracht van het schoolbestuur de persoonsgegevens verwerkt;
Verwerkingsverantwoordelijke :	Het bestuur van de ONS, het bestuur is eindverantwoordelijk voor de privacy van de leerlingen.
Verwerking :	Alles wat met persoonsgegevens gedaan wordt, zoals het verzamelen, vastleggen, bewaren, wijzigen, doorsturen etc.

Wet- en regelgeving datalekken

Op 1 januari 2016 is de **meldplicht datalekken** ingevoerd. Door deze meldplicht zijn we ook als school verplicht om melding te maken van ernstige datalekken bij de **Autoriteit Persoonsgegevens (AP)**.

De meldplicht is alleen van toepassing wanneer er **persoonsgegevens** worden verwerkt. Bijvoorbeeld in de leerlingadministratie of digitale leermiddelen. Als wel als school gebruik maken van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moeten we met deze bewerkers aanvullende afspraken over het melden van datalekken.

Er is sprake van een **datalek** als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan of waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. De wettelijke definitie is:

> *Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.*

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 groep 3 is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een **bewerker** voor de school. Er kan worden afgesproken dat een bewerker namens de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Als hierover geen afspraken zijn, zullen we als school zelf de melding doen.

Als er een datalek is moeten we daar **binnen 72 uur** na ontdekking van het lek een melding maken bij de Autoriteit Persoonsgegevens.

Afspraken met leveranciers

We hebben bewerkersovereenkomsten met afspraken rond privacy met de leveranciers die persoonsgegevens van ons ontvangen. In deze overeenkomsten staan ook afspraken over datalekken:

- Hoe we elkaar informeren over datalekken;
- Wie de melding bij de Autoriteit Persoonsgegevens doet;
- Welke informatiegegevens de bewerker moet geven bij een datalek;
- Welke informatie nodig is voor het doen van een melding en hoe we elkaar informeren over de melding (afspraken over een kopie van de melding);
- De tijd waarbinnen de bewerker de gegevens moet aanleveren;
- Wie de communicatie met de gebruikers voor haar rekening neemt, als dat nodig is.

Werkwijze

Uitgangssituatie

- Er is een actueel informatiebeveiligings- en privacybeleid;
- Er is een actueel document gedragscode ict- en internetgebruik.

Rollen

We hanteren vier rollen om een beveiligingsincident of datalek succesvol af te handelen:

1. **Ontdekker** – Degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt. Dit kan een personeelslid zijn of u als ouder.
2. **Meldpunt** – Een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt. Op onze school zijn dit J. Korevaar en M. van Zijl. Zijn zijn te bereiken via **privacy@ons-stolwijk.nl**.
3. **Melder** – Degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens. Op onze school is dit M. van Zijl als functionaris gegevensbescherming (FG).
4. **Technicus** – Degene die de oorzaak van het datalek kan vinden en kan (laten) repareren. Op onze school is dit J. Korevaar als security officer en ict-coördinator.

Stappen

We nemen zeven stappen bij een beveiligingsincident of datalek:

1. Ontdekken;
2. Inventariseren;
3. Beoordelen;
4. Repareren;
5. Melden;
6. Vastleggen;
7. Informeren.

Lees het volgende hoofdstuk voor een uitwerking van deze stappen.

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 privacy@ons-stolwijk.nl.

2. Inventariseren

Het *meldpunt* bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet deze aanvullende vragen uit bij de *ontdekker* of de *technicus*. De volgende informatie leggen we daarna vast:

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

Wettekst:

a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpuntwaar meer informatie kan worden verkregen;

c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;

d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken

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 betrokkenen vereist is.

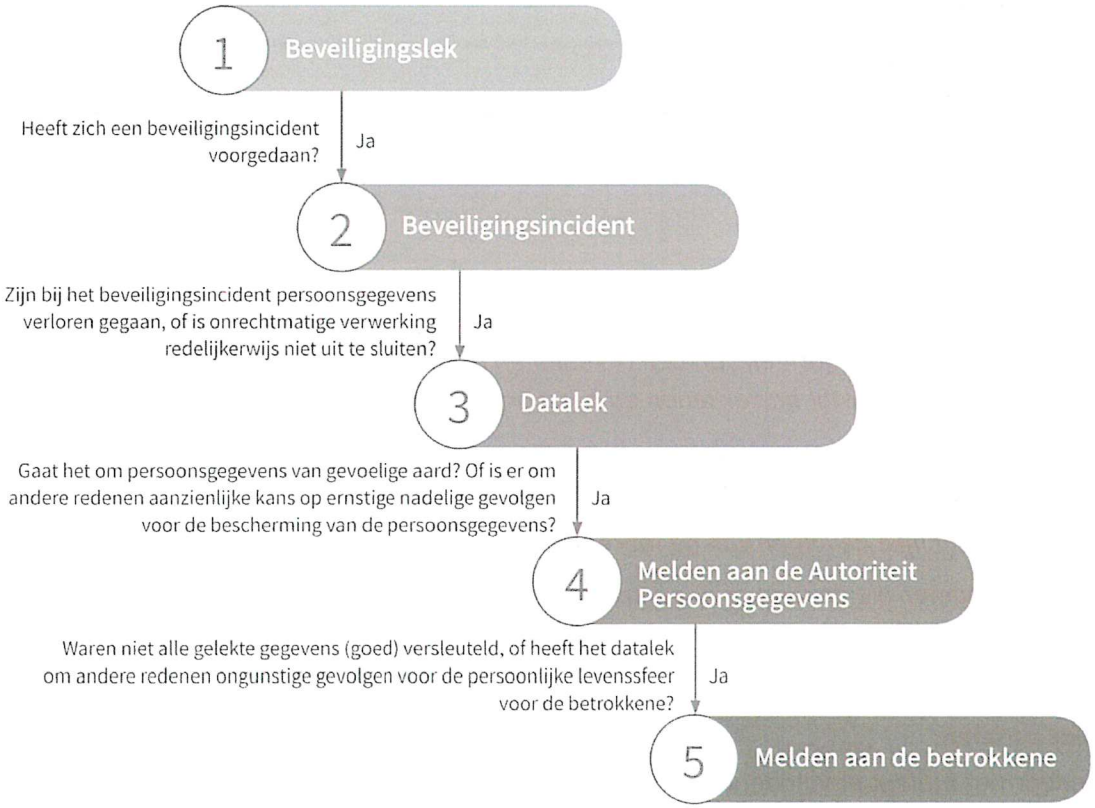
De melder legt de volgende informatie vast:

- Wat zijn de mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen?
- Melden we het datalek aan de Autoriteit Persoonsgegevens? Zo nee, waarom niet?
- Melden we het datalek aan betrokkenen? Zo nee, waarom niet?
- Hoe doen we de melding en wat is de inhoud?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek' houden we rekening met het type gegevens en met de hoeveelheid gegevens. We doen een melding als 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.

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. Dat geldt ook wanneer de gelekte gegevens 'gevoelig' zijn. Dat is het geval bij ***bijzondere persoonsgegevens*** over gezondheid, over de financiële of economische situatie van de betrokkene. Of als de gegevens kunnen leiden tot stigmatisering van de betrokkene, denken daarbij bijvoorbeeld aan het lekken van de gegevens over een leerling, die vaak kinderen pest en daarmee gezien kan worden als notoire pester.

We volgen de onderstaande beslisboom:



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? Zo ja, hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

5. Melden

Als bij stap 3 de conclusie is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens en eventueel ook bij de betrokkenen, dan zal de *melder* dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de incidentele en structurele technische en organisatorische maatregelen die er zijn genomen.

De melder meldt het bij het meldloket datalekken via http://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

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 bent u bent u als ouder (als wettelijk vertegenwoordiger van uw kind) of u als medewerker van onze school.

In principe gaan we ervan uit dat we het lekken van gevoelige aard moeten melden bij de betrokkenen. Als er echter persoonsgegevens zijn gelekt, die zijn beveiligd of versleuteld en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeven we dat niet melden aan de betrokkenen. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken

Het *meldpunt* van onze school maakt minimaal jaarlijks een analyse van de meldingen van beveiligingsincidenten en datalekken in samenwerking met onze functionaris gegevensbescherming.

In de analyse gaan we in op eventuele structurele ontwikkelingen en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

We informeren het schoolbestuur over de uitkomsten van de analyse.

Communicatie

Hiervoor heeft u al veel kunnen lezen over hoe we over datalekken en beveiligingsincidenten communiceren. Als er vanwege menselijk handelen een kans op herhaling is informeren en instrueren we onze medewerkers. Per melding kan gekozen worden om het bestuur te informeren. Bij signalen van buitenaf over een mogelijk datalek kan de *functionaris gegevensbescherming* of de *security officer* actief nagaan waar de signalen vandaan komen en of ze terecht zijn. Zij kunnen dan de melding volgens dit protocol verder afhandelen. Indien nodig schakelen we externe deskundigen in.