Procedure Beveiligingsincidenten en datalekken

MARTINUSSTICHTING VOOR (V)SO

Mattheusschool/Rotterdamcollege

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	06-03-2021	R. Veltman	Concept Privacy-Officers
0.2	Vastgesteld	26-05-2021	Bestuur Martinusstichting	
0.3	MR	01-06-2021		
0.4	Gepubliceerd	09-09-2021		
0.5	Gewijzigd			

INHOUDSOPGAVE

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiligings- en privacy beleid van de Mattheusschool voor ZMLK (inclusief het Rotterdamcollege) ressorterend onder de Martinusstichting voor speciaal onderwijs en voortgezet speciaal onderwijs te Rotterdam hieronder verder genoemd als Mattheusschool voor ZMLK)

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 de Mattheusschool voor ZMLK zoals vermeld in het IBP-beleid (Informatiebeveiliging en privacy) en al haar medewerkers.

Gebruikte 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 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

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. Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in je leerlingadministratie of 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 bewerkers aanvullende afspraken over het melden van datalekken.

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 een specifieke klas, 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. Dat moet wel worden afgesproken, anders zal de verantwoordelijke 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.

Afspraken met leveranciers

Het schoolbestuur moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Deze verantwoordelijkheden zijn ondergebracht in de verwerkingsovereenkomsten met de leveranciers.

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 (medewerker)*; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. *Meldpunt (mailbox datalekmeldingen - privacy officers + registratiesysteem IBP)*; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. *Melder (functionaris gegevensbescherming (FG-er) of privacy-officer)*; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. *Technicus (privacy officer i.s.m. ict-medewerker)*; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

Voor de Mattheusschool/Rotterdamcollege draagt het bestuur van de Martinusstichting voor speciaal onderwijs en voortgezet speciaal onderwijs de eindverantwoordelijkheid voor het beleid IBP (Informatiebeveiliging en privacy). De algemeen directeur G. Reinalda is op school inhoudelijk verantwoordelijk voor IBP.

Dhr. R. Veltman en mw. P. Dekker zijn als privacy-officers aangesteld en zijn hoofdbeheerders van de mailbox voor datalekken.
Dhr. Reinalda heeft als medebeheerder van de mailbox permanent inzicht en toegang tot de mailbox en ondersteunt de hoofdbeheerders bij het bewaken en behandelen van de mailbox datalekmeldingen, vragen en aandachtspunten. De directeur vervangt als beide hoofdbeheerders bij arbeidsongeschiktheid, verlof, vakantie of andere reden afwezigheid zijn.

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 datalek@zmlk.nl
   Dit adres wordt beheerd door de Privacy-officers van de Mattheusschool/ Rotterdamcollege.
   Direct na de melding wordt meteen het (vermeende) datalek doorgegeven aan de Functionaris Gegevensbescherming (ronald.van.rooijen@dyade.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

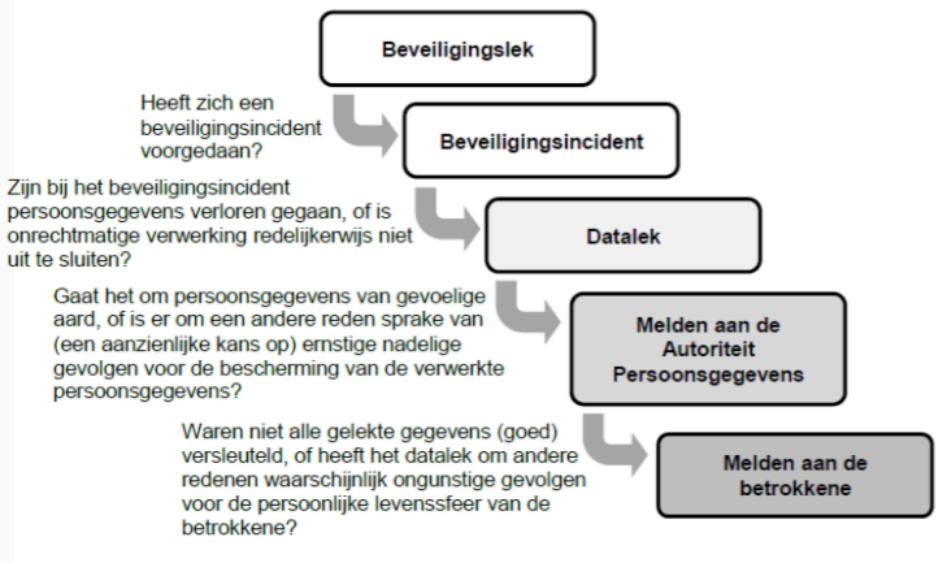
3. *Beoordelen*
   Wanneer het *meldpunt* voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de *melder*, de Functionaris Gegevensbescherming, een verzoek om de verzamelde informatie te bekijken. De FG-er beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.
   De volgende informatie wordt vastgelegd door de FG-er:
   - 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?

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.

De onderstaande beslisboom wordt gehanteerd



4. *Repareren*

De *technicus* (privacy-officer i.s.m. ICT-afdeling) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen.
De *technicus* van de Mattheusschool voor ZMLK 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* (FG-er) dit binnen twee werkdagen 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 van de Autoriteit Persoonsgegevens**.
Klik hier voor een link naar dit meldloket.

6. *Vastleggen*
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het *meldpunt* (privacy-officers) waarmee het incident is afgesloten. Het *meldpunt* verstuurt een samenvatting van de genomen maatregelen aan de *ontdekker* van het datalek.

7. *Informeren betrokkene: leerling en/of zijn ouders*
   Wanneer het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene(n) heeft, dan wordt het datalek ook aan de betrokkene(n) zelf gemeld. Dat kunnen medewerkers, leerlingen of hun ouders (als zij jonger zijn dan 16 jaar) zijn. In principe kan er van worden uitgaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkene(n). Overigens: als de persoonsgegevens die zijn gelekt, beveiligd of versleuteld zijn, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan is melding aan betrokkene(n) niet noodzakelijk.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van de Mattheusschool voor ZMLK 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.

Het schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.

Communicatie

Betrokkenen zullen steeds geïnformeerd worden via e-mail door de privacy-officers. Eventueel zal, wanneer nodig, in samenspraak met de functionaris gegevensbescherming, contact worden opgenomen met externe deskundigen.