Protocol informatiebeveiligingsincidenten en datalekken Stichting Keizer Karel

Gewijzigd protocol vastgesteld GMR d.d. 24 november 2021

Inleiding

Het Protocol informatiebeveiligingsincidenten en datalekken sluit aan bij de uitgangspunten in het informatiebeveiliging en privacy beleid van de Stichting Keizer Karel.
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 alsmede het beperken van de gevolgen daarvan.

Dit protocol is van toepassing op de Stichting Keizer Karel en het daaraan verbonden Alkwin Kollege en het Keizer Karel College.

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, etc.). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene**; de persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken

Krachtens de Wet meldplicht datalekken, zijn ook scholen verplicht 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 de leerling administratie 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 in onbevoegde handen zijn gekomen, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens in onbevoegde handen zijn gekomen. 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 leerlingen of het onzorgvuldig omgaan met een geprinte lijst met leerlinggegevens, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een gegevensverwerker voor de school. Het schoolbestuur heeft afspraken gemaakt met externen ten aanzien van het melden van datalekken. Deze afspraken zijn vastgelegd in verwerkersovereenkomsten.

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 datalekken (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (meestal afdeling ICT)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

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@alkwin.nl of datalek@keizerkarelcollege.nl. Hierbij kan gebruik gemaakt worden van het incidentenmeldingsformulier datalek zoals opgenomen in de bijlage van dit protocol.

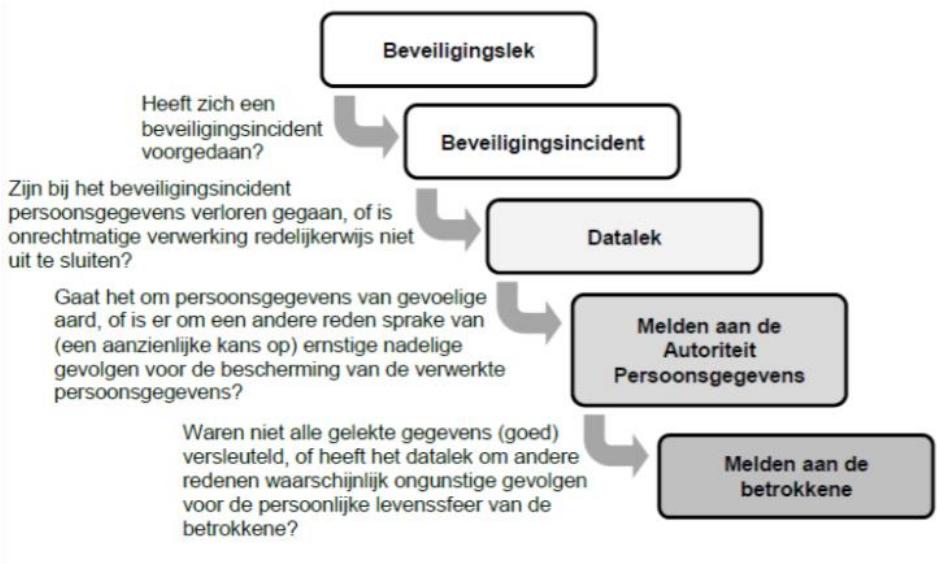
2. *Inventariseren*
   Het Meldpunt datalekken bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:
   - Samenvatting van het beveiligingsincident, 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 datalekken voldoende informatie heeft verzameld, en een datalek vermoed, 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 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 bij de Autoriteit 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 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 een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom kan gebruikt worden



4. *Repareren*
   De Technicus (Bij het Alkwin Kollege intern, bij het Keizer Karel College extern) wordt, indien noodzakelijk, 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 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.

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: 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 er van worden uitgegaan 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 toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken

Het Meldpunt van Stichting Keizer Karel maakt één 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 College van Bestuur wordt geïnformeerd over de uitkomsten van de analyse.

Communicatie

Het College van Bestuur is verantwoordelijk voor de verwerking van persoonsgegevens en doet er alles aan dat passende beveiligingsmaatregelen zijn genomen. Dit neemt niet weg dat een datalek nooit helemaal kan worden voorkomen. Het is daarom verstandig om goed voorbereid te zijn op het "op straat liggen" van persoonsgegevens en het daarmee mogelijk negatief in het nieuws komen van de school. Het is daarom verstandig om goed na te denken over.

- ✓ De manier van communiceren met betrokkenen en de pers.
- ✓ Hoe kan worden omgegaan met signalen van buitenaf over een mogelijk datalek.
- ✓ Het inschakelen van een externe (communicatie)deskundige.

Bijlage: Incidentenregistratieformulier Datalek en Register

INCIDENTENREGISTRATIEFORMULIER

DATALEKKEN

Incidentmelding

Naam van de melder: _____ Datum van de melding: _____

Gegevens over het incident

Wanneer (indien bekend)

Datum waarop het incident plaatsvond: _____

Tijdstip waarop het incident plaatsvond: _____

Wie (indien bekend)

Naam betrokken medewerker/leerling: _____
Klas: _____

Eventueel andere betrokken medewerker/leerling: _____
Klas: _____

Waar

Plaats van ontdekking van het incident (zo nauwkeurig mogelijk omschrijven)
Zo mogelijk: foto of schermafdruk bijvoegen.
_____

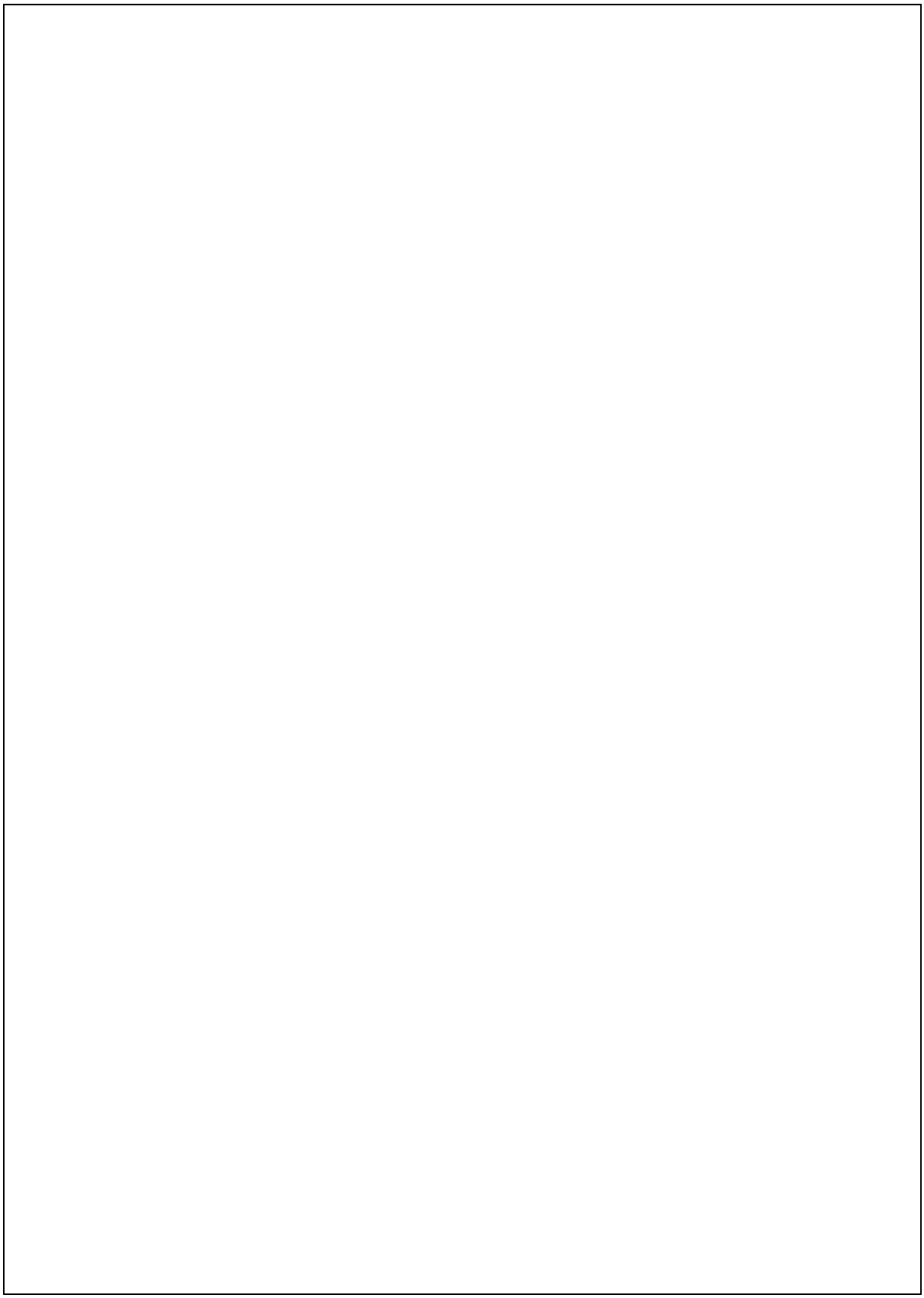
Om welke data gaat het?

Soort incident: (aankruisen wat van toepassing is)

1, chromebook / laptop verdwenen/gestolen		
2. usb stick / externe drive verdwenen/gestolen		
3. Onbevoegd persoon achter ingelogde pc aangetroffen		
4. Opgemerkt op internet		
5. Opgemerkt via social media		

6. Papieren met persoonsgegevens aangetroffen		
7. Anders, namelijk:		

Ruimte voor nauwkeurige omschrijving, indien nodig aanvullen met bijlage



AFHANDELING VAN HET INCIDENT DATALEK

Deze incidentmelding is verwerkt op: _____

Deze incidentmelding is verwerkt door:_____

Inschatting van de risico factor: 1 2 3 4 5

De volgende perso(o)n(en)/instantie(s) is/zijn ingelicht over het incident:

- ☐ schoolleiding
- ☐ mentor
- ☐ docent(en)
- ☐ ouders/verzorgers
- ☐ partner
- ☐ politie
- ☐ anders, namelijk

Naar aanleiding van het incident zijn de volgende acties ondernomen:

Hieronder, indien nodig, een korte toelichting op de afhandeling:

Register Datalekken voorblad

Datum	Naam melder	Omschrijving [1]	Melding AP [2]	Gereed

1) Omschrijving incident:

1. chromebook / laptop verdwenen/gestolen
2. usb stick / externe drive verdwenen/gestolen
3. Onbevoegd persoon achter ingelogde pc aangetroffen
4. Opgemerkt op internet
5. Opgemerkt via social media
6. Papieren met persoonsgegevens aangetroffen
7. Anders, namelijk

2) Datalekken met ernstige nadelige gevolgen voor de bescherming van persoonsgegevens dienen gemeld te worden bij de AP. Zie verder het protocol datalekken.