Protocol datalekken

Periodieke review:

Jaarlijks, in het eerste kwartaal

Definitief besluit

Instemming is verkregen van de GMR d.d. 19 maart 2019.

Aldus vastgesteld door het bevoegd gezag van SKOzoK d.d. 19 maart 2019.

Mevrouw drs. I.C.A.N. Sluiter
Voorzitter College van Bestuur SKOzoK
Pastoor Jansenplein 21
5504 BS Veldhoven
www.skozok.nl

Inhoud

1. Inleiding en begripsbepaling

Op 1 januari 2016 is de meldplicht datalekken in werking getreden via de Wet bescherming persoonsgegevens (Wbp). Iedere organisatie die persoonsgegevens verwerkt, is verplicht om sommige datalekken te melden bij de Autoriteit Persoonsgegevens.

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wet bescherming persoonsgegevens (Wbp) geldt vanaf dat moment niet meer. De AVG geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van organisaties geen persoonsgegevens zijn.

Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens zoals bijvoorbeeld ras, godsdienst, seksuele voorkeur en medische gegevens worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd. Van een datalek is sprake in geval van een inbreuk op de beveiliging die leidt tot verlies van persoonsgegevens of tot de mogelijkheid dat er als gevolg van de inbreuk op de beveiliging persoonsgegevens onrechtmatig worden verwerkt.

Dit protocol heeft ten doel het voor onze medewerkers, leerlingen en ouders, en daarmee voor onze Stichting, het zo veel mogelijk voorkomen en inperken van de risico's van datalekken door heldere afspraken en procedures vast te leggen.

2. Hoe gaat wij om met datalekken

We volgen bij SKOzoK bij het optreden van (mogelijke) datalekken een protocol waarin we onderstaande zaken vastleggen:

- Wie beoordeelt of er sprake is van een datalek?
- Wie registreert een datalek?
- Wie meldt een datalek bij de Autoriteit Persoonsgegevens?
- Wie verzorgt de communicatie richting interne en externe betrokkenen bij een datalek?
- Hoe worden onze medewerkers op de hoogte gehouden van de nieuwe wetgeving betreffende de meldplicht datalekken?

2.1 Wie beoordeelt een beveiligingsincident/datalek?

Elke medewerker binnen de organisatie, die een datalek vermoedt, geeft dit aan bij zijn of haar leidinggevende. Deze neemt vervolgens contact op met de beleidsadviseur IBP. Deze bepaalt vervolgens samen met de functionaris gegevensbescherming of er sprake is van een datalek en zo ja, of het een datalek betreft dat gemeld dient te worden met behulp van het meldingsformulier datalek dat op een speciale AVG pagina op Intranet staat (bijlage A). Indien geconcludeerd wordt dat er gemeld moet worden, wordt het meldingsformulier ingevuld.

De meldingen vanuit de scholen worden op gemeenschappelijk niveau vastgelegd bij de beleidsadviseur IBP. De leidinggevende doet, indien nodig, nader onderzoek. Dit onderzoek wordt bij voorkeur vastgelegd in een rapportage (bijlage B). Bevindingen hiervan worden doorgesproken met de beleidsadviseur IBP. Daarna wordt in samenspraak met de functionaris gegevensbescherming beslist of melding bij de AP gedaan moet worden.

2.2 Wie meldt een datalek bij de Autoriteit Persoonsgegevens?

De melding bij de AP wordt namens de Stichting gedaan door de functionaris gegevensbescherming.

2.3 Wie verzorgt de communicatie richting interne en externe betrokkenen bij een datalek?

De directie van de school is verantwoordelijk voor de juiste interne en externe communicatie bij een datalek. Binnen de organisatie wordt overleg gevoerd met de beleidsadviseur IBP en de functionaris gegevensbescherming en voordat berichten 'naar buiten' gecommuniceerd worden.

2.4 Medewerkers op de hoogte betreffende de meldplicht datalekken en privacy?

De medewerkers worden geïnformeerd over de meldplicht bij datalekken en privacy. Hierbij dient voor medewerkers helder gemaakt te worden welke vormen van datalekken kunnen voorkomen. De focus ligt daarbij op de volgende facetten:

- Vermoeden van onterecht uitwisselen van gegevens van leerling en medewerkers (bijvoorbeeld het ontvangen van aanbiedingen van commerciële bedrijven die rechtstreeks op leerresultaten van een groep of individuele leerlingen terug te voeren zijn).
- Datalek door verlies/diefstal van apparatuur en/of inloggegevens. De apparatuur die een medewerker gebruikt bij zijn werkzaamheden kan gegevens bevatten, die niet toegankelijk mogen zijn voor anderen. Denk hierbij bijvoorbeeld aan het gebruik van apps op een tablet of smartphone. Diefstal of verlies van deze apparatuur kan leiden tot datalek, als de apparaten of de apps niet goed beveiligd zijn.

Standaard maatregelen bij verlies of diefstal:

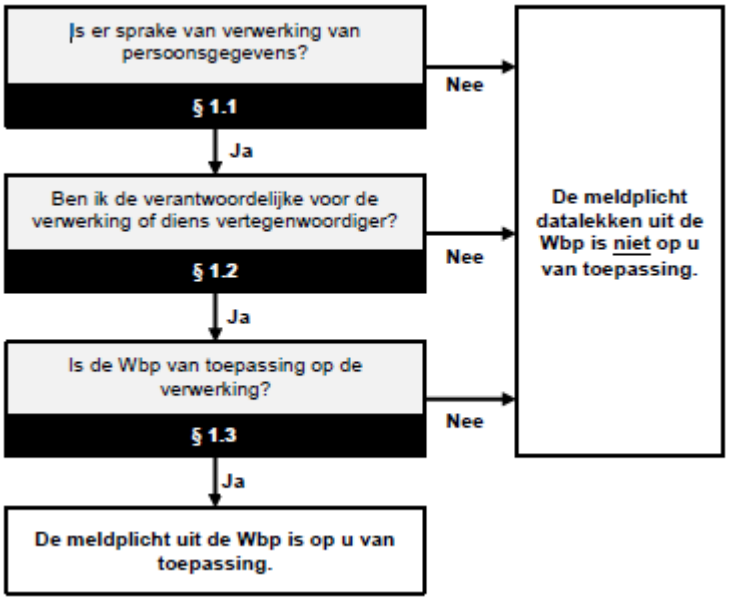
Indien er sprake is van verlies of diefstal van apparatuur zoals laptops, tablets en/of smartphones is het risico aanwezig dat door bijvoorbeeld opgeslagen wachtwoorden op deze apparaten er toegang verkregen kan worden tot omgevingen waar zich privacygevoelige data bevindt. Per incident zal worden beoordeeld of en welke maatregelen er genomen worden. Voor enkele cruciale omgevingen Intranet/Office365, Google G suite for Education en onze administratiesystemen Parnassys (schoolniveau) en Afas (gemeenschappelijk niveau) zullen standaard de wachtwoorden van de gebruiker worden vervangen.

3. Stappenplan meldplicht datalekken

Dit stappenplan wordt door de beleidsadviseur IBP en functionaris gegevensbescherming gehanteerd om te bepalen of een beveiligingsincident onder de meldplicht datalekken valt en wat de te nemen maatregelen zijn.

Stap 1: Bepalen of de meldplicht datalekken van toepassing is

Om vast te stellen of de meldplicht datalekken in een specifieke situatie van toepassing is, wordt eerst vastgesteld of binnen de eigen organisatie persoonsgegevens worden verwerkt en of de eigen organisatie in dat kader als 'verantwoordelijke' is aan te merken. Zie ook onderstaand stroomschema dat afkomstig is uit de beleidsregels:



Indien de meldplicht datalekken van toepassing is, volgt stap 2. Indien de meldplicht niet van toepassing is, hoeft er niet gemeld te worden op grond van de Wbp.

Stap 2: Bepalen of er sprake is van een datalek

Van een datalek is sprake in geval van een inbreuk op de beveiliging die leidt tot verlies van persoonsgegevens of tot de mogelijkheid dat er als gevolg van de inbreuk op de beveiliging persoonsgegevens onrechtmatig worden verwerkt.

Bij een inbreuk op de beveiliging heeft zich een beveiligingsincident voorgedaan. Daarbij kan bijvoorbeeld gedacht worden aan een kwijtgeraakt extern opslag apparaat zoals bv een USB-stick, een gestolen laptop of telefoon, een inbraak door een hacker of een malwarebesmetting.

Van verlies van gegevens is alleen sprake als de gegevens definitief verloren zijn gegaan. Als een medewerker zijn of haar notebook in de trein laat liggen, levert dat dus geen verlies van gegevens op als van de gegevens op het notebook elders een kopie beschikbaar is.

Indien het notebook niet goed beveiligd is, levert dit echter wel de mogelijkheid op dat er persoonsgegevens onrechtmatig worden verwerkt. Van onrechtmatige verwerking is namelijk sprake als persoonsgegevens worden aangetast, of als daar onbevoegd kennis van genomen kan worden. Als die mogelijkheid niet kan worden uitgesloten, is er sprake van datalek.

Indien geconcludeerd wordt dat er sprake is van een datalek, volgt stap 3.

Stap 3: Bepalen of het datalek gemeld moet worden aan de AP

Niet elk datalek hoeft gemeld te worden. Alleen als het datalek leidt tot (de kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, is melden vereist. In dat kader is van belang welk type gegevens het datalek betreft. Ten aanzien van persoonsgegevens van gevoelige aard heeft de AP zich op het standpunt gesteld dat een datalek per definitie leidt tot een aanzienlijke kans op ernstige nadelige gevolgen. Een datalek met betrekking tot gegevens van gevoelige aard moet dus altijd worden gemeld bij de AP.

Betreft het datalek geen gegevens van gevoelige aard, dan moet de afweging gemaakt worden of het datalek leidt tot (de kans op) ernstige nadelige gevolgen. Daarbij wordt gekeken naar de aard en de omvang van de getroffen verwerking en naar de kwetsbaarheid van de betrokkenen. Kwetsbare groepen zijn bijvoorbeeld kinderen.

Stap 4: Melden aan de AP (autoriteit Persoonsgegevens)

Indien de conclusie getrokken wordt dat het datalek gemeld moet worden, moet die melding binnen 72 uur na ontdekking door de Functionaris Gegevensbescherming van SKOzoK of een ingeschakelde bewerker bij de AP gedaan worden. De functionaris Gegevensbescherming meldt het datalek met behulp van een formulier op de website van de AP. Zorg dat er een ontvangstbevestiging van de melding komt, zodat later aangetoond kan worden op welk moment de melding gedaan is.

De beleidsregels meldplicht datalekken hebben een bijlage waarin is uitgewerkt welke gegevens aan de AP gemeld moeten worden. Het betreft onder meer informatie over: de aard van de melding, algemene gegevens van de eigen organisatie, het datalek, door de eigen organisatie getroffen maatregelen, het inlichten van betrokkenen.

Stap 5: Bepalen of het datalek gemeld moet worden aan de betrokkenen

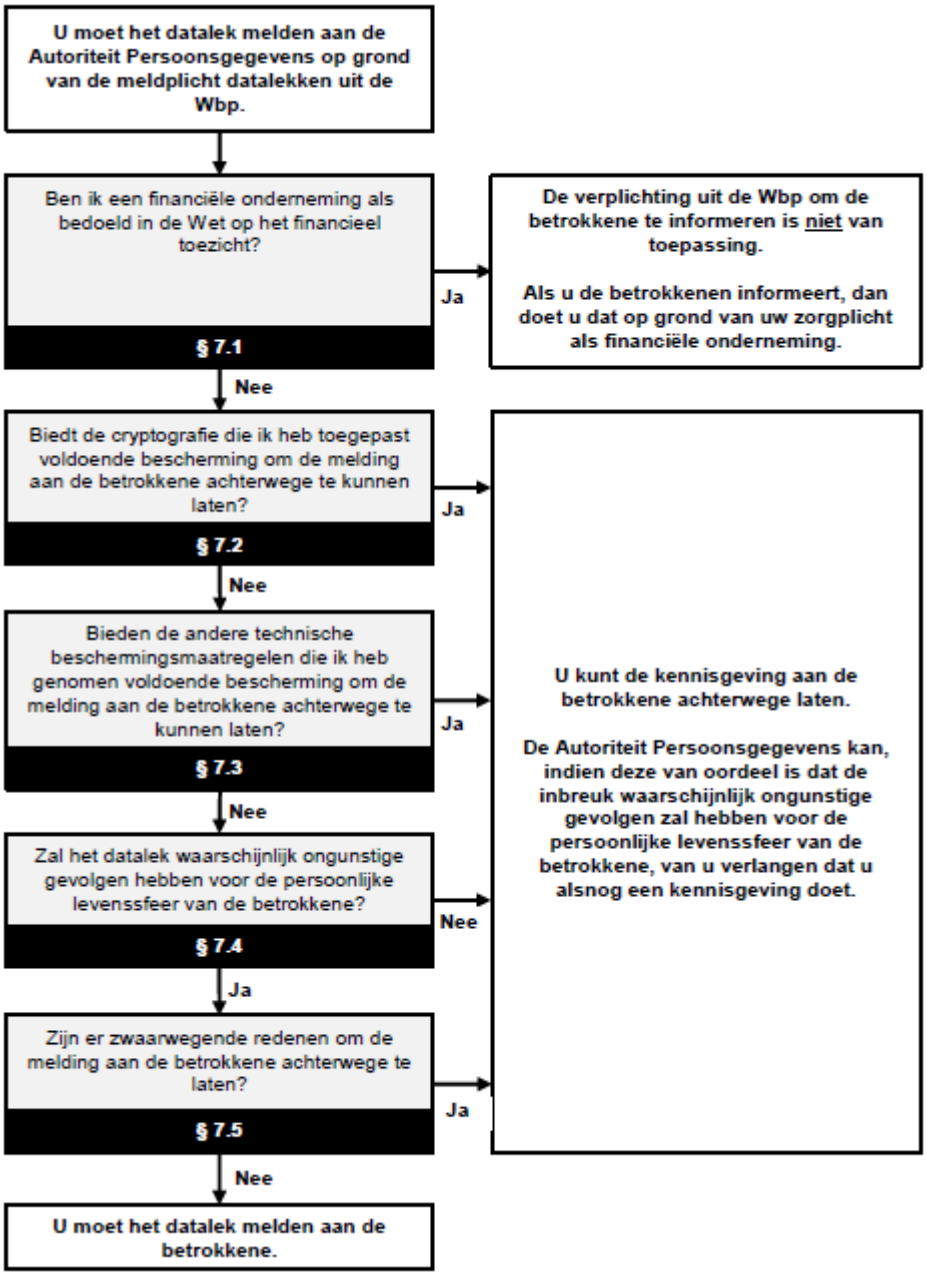
Sommige datalekken dienen niet alleen aan de AP gemeld te worden, maar ook aan de betrokkenen zelf. Dat is het geval indien het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkenen. Om te bepalen of daar sprake van is, heeft de AP in de beleidsregels een stroomschema opgenomen. Gemakshalve is een kopie van dat stroomschema hieronder opgenomen.

Allereerst dient bepaald te worden of de persoonsgegevens ontoegankelijk of onbegrijpelijk zijn voor derden als gevolg van technische beveiligingsmaatregelen en of daardoor in het concrete geval voldoende bescherming wordt geboden tegen onrechtmatige verwerking. Indien dat het geval is, is melden aan de betrokkenen niet nodig. In dat geval zal er overigens in veel gevallen ook geen sprake zijn van een datalek (zie hiervoor). De beleidsregels zijn op dit punt overigens niet helemaal consistent: Elders in de beleidsregels stelt de AP namelijk dat als er persoonsgegevens van gevoelige aard zijn gelekt, de verantwoordelijke er van uit kan gaan dat het datalek aan de betrokkenen moet worden gemeld.

Als de beveiligingsmaatregelen onvoldoende bescherming bieden, is het mogelijk dat er andere beveiligings-maatregelen genomen zijn die afdoende zijn, zoals het op afstand wissen van een apparaat of het anonimiseren van de gegevens, zodat ze niet tot natuurlijke personen herleidbaar zijn. Als dat het geval is, is melden aan de betrokkenen niet noodzakelijk. Het kan zijn dat geconcludeerd wordt dat niet gemeld hoeft te worden aan de betrokkenen, maar dat de Autoriteit Persoonsgegevens (waaraan wel gemeld is) tot de conclusie komt dat wel gemeld moet worden. In dat geval kan de AP verlangen dat het datalek alsnog wordt gemeld aan de betrokkenen.

Tot slot kan het zijn dat op grond van de afwegingen zoals hierboven vermeld geconcludeerd wordt dat aan de betrokkenen gemeld dient te worden, maar dat er zwaarwegende redenen (als bedoeld in artikel 43 Wbp) zijn om niet te melden. De beleidsregels noemen als voorbeeld van een zwaarwegende reden de situatie waarbij er gegevens gelekt zijn over medische hulpvragen die kinderen buiten medeweten van hun ouders hebben gedaan. Het melden van het datalek aan de betrokkenen zou tot gevolg kunnen hebben dat de ouders onbedoeld op de hoogte raken van de hulpvraag van hun kind. In dergelijke gevallen hoeft er niet gemeld te worden.

Stroomschema stap 5:



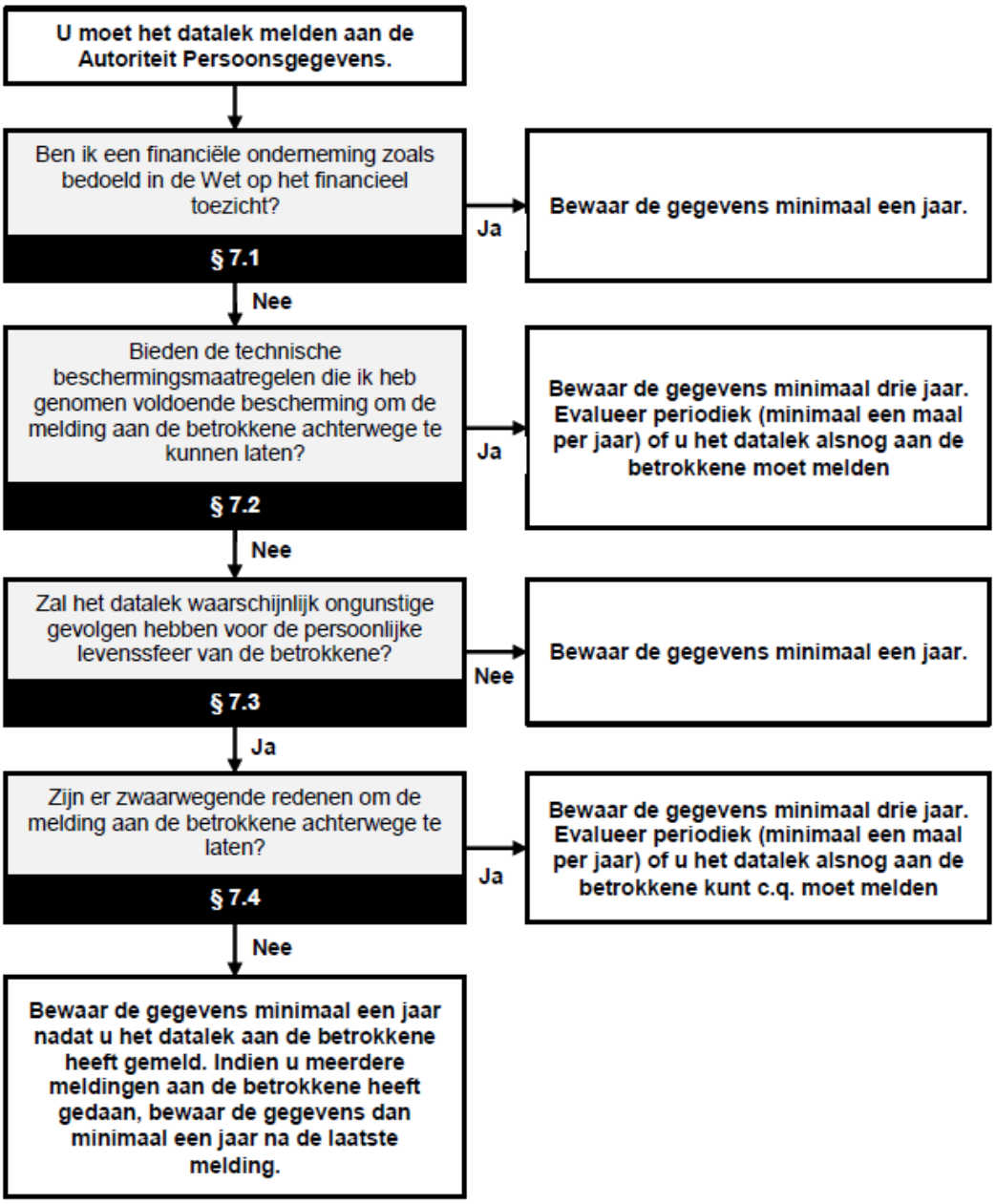
Stap 6: Melden aan de betrokkenen

Wanneer geconcludeerd wordt dat er gemeld moet worden aan de betrokkenen, dan dient de betrokkenen onverwijld geïnformeerd te worden over de aard van het datalek, de instantie waar meer informatie over het datalek kan worden verkregen en de maatregelen die aan de betrokkenen aangeraden zijn om de negatieve gevolgen van de inbreuk zoveel mogelijk te beperken. Indien mogelijk wordt de betrokkene individueel geïnformeerd, dat wil zeggen niet alleen met een bericht in de media, maar bijvoorbeeld per email. Anders dan bij de melding aan de Autoriteit Persoonsgegevens (binnen 72 uur) wordt het begrip ‘onverwijld’ niet nader ingevuld door een concrete termijn waarbinnen gemeld moet worden. Wel moet bij de melding aan de Autoriteit Persoonsgegevens aangegeven worden of aan de betrokkenen gemeld gaat worden en zo ja, wanneer. Deze termijn is bindend.

Stap 7: Gegevens over datalek vastleggen

Er moet een overzicht bijgehouden worden van alle datalekken die onder de meldplicht vallen. In het overzicht moet per datalek de feiten aangegeven worden en gegevens omtrent de aard van de inbreuk worden vastgelegd. Indien het een datalek betreft dat ook aan de betrokkenen gemeld is, dan dient het overzicht ook de tekst van de kennisgeving aan de betrokkenen te bevatten.

De wet schrijft niet voor hoe lang het overzicht bewaard moet worden. De Autoriteit Persoonsgegevens heeft in haar beleidsregels een stroomschema opgenomen met bewaartermijnen. SKOzoK volgt deze richtlijnen:



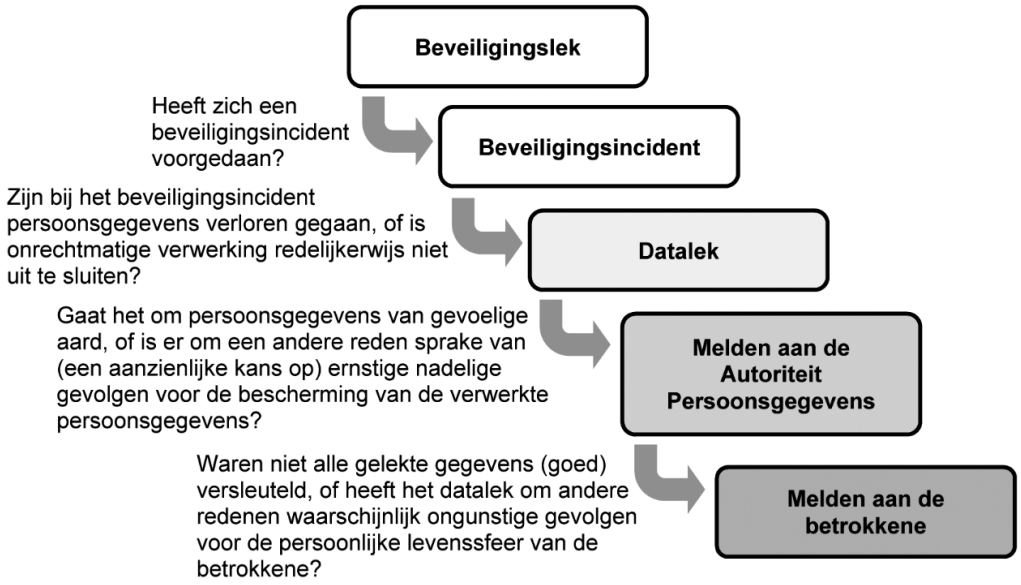
Bijlage A Formulier voor melding datalek bij SKOzoK

Deze bijlage bevat het instructie- en het meldingsformulier dat gebruikt wordt binnen de organisatie om een datalek intern te melden. Dezelfde gegevens worden gebruikt t.b.v. de melding bij de Autoriteit Persoonsgegevens en interne afhandeling door SKOzoK van hetzelfde datalek.

Instructieformulier melding datalek

- Voor het melden van een datalek vul je onderstaand formulier in.
- Wanneer het formulier is ingevuld stuurt je dit z.s.m. door naar de Functionaris Gegevensbescherming van SKOzoK, Karin Wagt, datalek@SKOzoK.nl
- LET OP: Na het ontdekken van een datalek moet dit formulier dezelfde dag (dag van ontdekken) worden ingevuld en doorgestuurd naar de Functionaris Gegevensbescherming via bovenstaand e-mailadres.
- Als je vragen hebt over het datalek of over het invullen van dit formulier, kan je contact opnemen met de AVG-verantwoordelijke medewerker.

Stappenplan



Begrippenlijst

- **Datalek:** Bij een datalek gaat het om toegang tot of vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is van de organisatie.
- **Persoonsgegevens:** Er zijn veel soorten persoonsgegevens. Voor de hand liggende persoonsgegevens zijn iemands naam, adres, woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, gezondheid of levensovertuiging worden bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd. Zie punt 4 in dit formulier met meer voorbeelden van persoonsgegevens.
- **Betrokkene:** Degene op wie de persoonsgegevens betrekking heeft.

Formulier intern melden datalek

1. Naam melder (volledige voor en achternaam)

2. Contactgegevens melder (e-mailadres en telefoonnummer)

3. Datum van ontdekken (Wanneer heb je het datalek ontdekt?)

Exacte datum van ontstaan (Kies een van de volgende opties en vul waar nodig aan) ☐ Op (datum) ☐ Tussen (begindatum periode) en (einddatum periode) ☐ Nog niet bekend

4. Type persoonsgegevens
☐ NAW-gegevens (Naam, Adres, Woonplaats)
☐ Telefoonnummers
☐ E-mailadressen en/of andere elektronische gegevens
☐ Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord)
☐ Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
☐ BSN (Burger Service Nummers)
☐ Kopie legitimatiebewijzen
☐ Geslacht/Geboortedatum/Leeftijd
☐ Godsdienst en/of levensovertuiging
☐ Gegevens over iemands ras
☐ Politieke gezindheid
☐ Gegevens over iemands seksuele leven
☐ Lidmaatschap van een vakvereniging
☐ Strafrechtelijke persoonsgegevens
☐ Gedragingen van betrokkenen
☐ Overige gegevens, namelijk (vul aan)

5. Aard van het incident
☐ Apparaat en/of gegevensdrager (Bijv. USB-stick) en/of papier met persoonsgegevens
☐ Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen
☐ Hacking, malware (bijvoorbeeld ransomware) en/of phishing
☐ Persoonsgegevens bij oud papier gezet
☐ Persoonsgegevens mondeling gedeeld met onbevoegde ontvanger
☐ Persoonsgegevens nog aanwezig op afgedankt apparaat of afgedankte gegevensdrager
☐ Persoonsgegevens per ongeluk gepubliceerd
☐ Anders, te weten…….

6. De groep mensen van wie de persoonsgegevens betrokken zijn bij het datalek
☐ Medewerker ☐ Leerlingen ☐ Ouders ☐ Personen uit kwetsbaren groepen ☐ Overig, te weten…..

7. Geef een samenvatting van het datalek (graag zo nauwkeurig mogelijk omschrijven)

8. Van hoeveel personen (betrokkenen) zijn de persoonsgegevens gelekt? Indien onbekend dan een schatting doen of een minimaal en maximaal aantal personen benoemen.

9. Was er een andere organisatie (of organisaties) betrokken bij het datalek en zo ja: om welke organisatie(s) gaat het en welke rol had(den) deze organisatie(s) m.b.t. dit datalek?

10. Moet het datalek worden doorgezet aan de Autoriteit Persoonsgegevens? *LET OP: laat datalekken altijd door een AVG verantwoordelijke medewerker van SKOzoK naar de Autoriteit Persoonsgegevens doorzetten.*

11. Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? *LET OP: Overleg altijd eerst met een AVG verantwoordelijke medewerker van SKOzoK of de betrokkenen geïnformeerd moet worden en wat de juiste werkwijze hiervoor is.*

12. Welke (mogelijke) gevolgen heeft het datalek voor de betrokkene(n)?

13. Ruimte voor aanvullende informatie rondom het datalek (bijv. i.v.m. een vervolgonderzoek)

Interne vervolgacties Functionaris Gegevensbescherming n.a.v. het datalek

1) Welke technische en organisatorische maatregelenzijn er getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Inlichten van de betrokkenen

2) Is het datalek gemeld aan de betrokkenen of gaat dit nog gebeuren? (Kies een van de volgende opties.)

☐ Ja

☐ Nee

☐ Nog niet bekend

3) Wanneer is het datalek gemeld aan de betrokkenen, of wanneer gaat dit gebeuren?
Beantwoord deze vraag als u vraag 2 met ja hebt beantwoord. Kies een van de volgende opties en vul waar nodig aan:

☐ Ik heb het datalek aan de betrokkenen gemeld op (datum)

☐ Ik ga het datalek aan de betrokkenen melden op (datum)

☐ Nog niet bekend

4) Wat is de inhoud van de melding aan de betrokkenen? (Letterlijke weergave, beantwoord deze vraag als u vraag 2 met ja hebt beantwoord.)

5) Hoeveel betrokkenen zijn er in kennis gesteld of gaat u in kennis gesteld worden? (Beantwoord deze vraag als u vraag 2met ja hebt beantwoord.)

6) Welk communicatiemiddel of welke communicatiemiddelen worden gebruikt of gaan gebruikt worden bij het in kennis stellen van de betrokkenen? *(Beantwoord deze vraag als u vraag 2 met ja hebt beantwoord)*

7) Waarom wordt afgezien van het melden van het datalek aan de betrokkenen? *Beantwoord deze vraag als u vraag 2 met nee hebt beantwoord*. Kies een van de onderstaande opties en vul waar nodig aan:

☐ De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten.

☐ Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (vul aan)

☐ Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten (artikel 43, Wbp), namelijk: (vul aan)

☐ Anders, namelijk (artikel 34a, lid 6, Wbp): (vul aan)

Technische beschermingsmaatregelen

8) Zijn de persoonsgegevens versleuteld, gehackt of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? Kies een van de volgende opties en vul waar nodig aan:

a) Ja
b) Nee
c) Deels, namelijk: (vul aan)

9) Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd? Beantwoord deze vraag als u bij vraag 8 gekozen heeft voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.

Internationale aspecten

10) Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)

☐ Ja

☐ Nee

☐ Nog niet bekend

11) Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?

☐ Ja, namelijk: (vul aan)

☐ Nee

Vervolgmelding

12) Is naar uw mening deze melding compleet? Selecteer een van de onderstaande opties:

☐ Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig.

☐ Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk.

Bijlage B: Rapportageformulier datalekken

Datum concept: <invullen>
Datum bespreking: <invullen>
Datum definitief: <invullen>

Datalekken Beoordelaar(s):
- <naam invullen>
- <naam invullen>

1. **Opdracht en taakstelling**
Hieronder wordt een korte toelichting gegeven bij het schrijven van de rapportage:
Schrijf een korte en bondige rapportage. In de opbouw is met name van belang dat de omschrijving van het incident, de beschrijving van de oorzaken, de beoordeling daarvan en de geadviseerde verbeter-maatregelen een logisch gevolg van elkaar zijn. Maak het incident visueel waar mogelijk, denk aan een foto of tekening.

Datum incident

Geef hier aan gedurende welke periode het datalek heeft plaatsgevonden en wanneer het datalek is opgemerkt. Vermeld hier ook op welke datum de melding door SKOzoK is gedaan bij de Autoriteit Persoonsgegevens.

Volledige beschrijving van incident

Geef hier een omschrijving van het incident. Omschrijf helder wat er heeft plaatsgevonden, waarbij je de gebeurtenissen en data omschrijft. Ga nog niet in op eventuele oorzaken, dit komt later aan bod.

2. Algemene informatie
2.1 Persoonsgegevens

-Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van Persoonsgegevens zich heeft voorgedaan.
-Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
-Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.
-Wanneer vond de inbreuk plaats?
-Om welk type persoonsgegevens gaat het?

Noot: bij de beantwoording kunt u gebruik maken van de bijlage 1 “Formulier voor melding datalek”, met name vraag 10 t/m 13 en vraag 15.

2.2 Aard van inbreuk

Omschrijf de aard van de inbreuk, bij de beantwoording kunt u gebruik maken van de bijlage A “Formulier voor melding datalek” met name vraag 14.

2.3 Gevolgen voor de betrokkene(n)

Met betrokkene(n) is bedoeld degene(n) op wie de persoonsgegeven(s) betrekking heeft (hebben), conform de definitie volgens Wet bescherming persoonsgegevens.
Omschrijf welke gevolgen de inbreuk kan hebben voor de persoonlijke levenssfeer van de betrokkene(n).
Bij de beantwoording kunt u gebruik maken van de bijlage A “Formulier voor melding datalek”, met name vraag 16.

2.4 Informeren betrokkenen

Zijn de betrokkene(n) of diens wettelijk vertegenwoordiger(s) geïnformeerd over het datalek incident en de melding aan de AP? Zo ja, door wie en wanneer is dit besproken.

2.5 **Volledig overzicht intern en extern betrokken medewerkers**

Geef in onderstaand overzicht aan welke medewerkers allemaal intern en extern (bij derden) betrokken zijn. De echte beginletters van de achternamen mogen niet terugkomen in het rapport, geef iedereen een letter op alfabetische volgorde.

Naam	Functie
Mevrouw A.	
De heer B.	
Etc.	

2.6 **Interviews met intern en extern betrokken medewerkers**

Voor dit datalekken onderzoek zijn de volgende interviews gehouden:
Mevrouw A. (functie)
De heer B. (functie)
Etc.

Indien betrokkene conform definitie Wbp (de persoon wiens gegevens het betreft) en/of diens wettelijk vertegenwoordiger niet gehoord zijn, geef een toelichting waarom niet.

3. **Het onderzoek**

3.1 **Focus onderzoek**

Omschrijf naar aanleiding van het verloop van het datalek waar de focus van het incidentonderzoek is komen te liggen. Gebruik hierbij de volgende hulpvragen:

- Wat waren de belangrijkste gebeurtenissen waardoor het incident ontstond?
- Welk kritiek moment of gebeurtenis mag nooit meer plaatsvinden? Hiermee wordt niet de schade voor de betrokkene bedoeld, maar het moment (oorzaak) waardoor de schade (vervolg) kon ontstaan.
- Wat moet dit onderzoek in de toekomst voorkomen?

Beantwoording van deze vragen hoeven niet letterlijk terug te komen in het rapport, maar zijn bedoeld te helpen bij het schrijven van het rapport en het onderzoek.

4. **Basisoorzaken incident**

4.1 **Oorzakenboom**

Maak een oorzakenboom behorend bij de casus en voeg deze toe als bijlage.
Bespreking oorzaak-en-gevolg factoren en veiligheidsbarrières

In deze paragraaf worden de diverse factoren besproken die hebben geleid tot het incident. Dit kan gezien worden als een verhalende toelichting op de oorzakenboom. Hierbij wordt nadrukkelijk gekeken naar oorzaak-gevolg en veiligheidsbarrières (fysieke beveiliging toegang, inlogprocedure, versleutelde data,..).
Schade voor de betrokkene(n) of de organisatie, regresrecht bewerker

Geef weer wat de schade is die de betrokkene(n) heeft opgelopen door het incident.
Nevenbevindingen

Licht hier overige bevindingen toe die nog niet naar voren zijn gekomen in dit hoofdstuk, maar wel onderdeel moeten zijn van het rapport. Zijn er geen overige bevindingen? Dan kan deze paragraaf verwijderd worden.
Vermijdbaarheid

Licht hier toe of er sprake is van vermijdbaarheid (het incident had door bepaalde maatregelen voorkomen kunnen worden).

5. **Professionaliteit**

5.1 **Professionele standaarden en protocollen**

Werd er volgens de professionele normen gewerkt? Werd er protocollair volgens afspraak gewerkt en zo niet, wat was de motivatie om af te wijken? Voeg aangehaalde normen of protocollen toe als bijlage.

5.2 **Andere bevindingen rondom professionaliteit**

Indien een van de onderstaande vragen van belangrijke invloed was op het incident, neem dat dan op onder deze paragraaf. Zijn er geen andere bevindingen op het vlak van professionaliteit? Dan kun je deze paragraaf weghalen.

- Wat was de rol en verantwoordelijkheid van de betrokken professionals en medewerkers? Heeft eenieder zijn rol en verantwoordelijkheid genomen of kunnen nemen? Geef hier een toelichting op.
- Was de bevoegdheid en bekwaamheid van de betrokkenen op niveau?
- Was er adequate overdracht van informatie?

6. **Organisatorische aspecten**

Indien een van de onderstaande vragen van belangrijke invloed was op het incident en eerder in dit rapport nog onvoldoende besproken zijn, neem dat dan op onder dit hoofdstuk. Maak paragrafen indien er meerdere 'losse' punten besproken worden.

6.1 **Bevindingen rondom organisatorische aspecten**

Zijn er geen andere bevindingen op het vlak van organisatorische aspecten? Dan kun je deze paragraaf weghalen.

- Waren er organisatorische tekortkomingen en zo ja welke?
- Heeft het gedrag van de medewerker(s) een rol gespeeld?
- Heeft het kennisniveau van de medewerker(s) een rol gespeeld?

6.2 **Bevindingen rondom technische aspecten**

Zijn er geen andere bevindingen op het vlak van technische aspecten? Dan kun je deze paragraaf weghalen.
Waren er technische tekortkomingen en zo ja welke?

7. **Conclusie**

Herhaal de onderzoeksvraag die gesteld is in paragraaf 1.4 en geef hier antwoord op. Om grote lappen tekst te voorkomen, kan het handig zijn de verschillende basisoorzaken te nummeren in dit hoofdstuk. Draag er zorg voor dat niet het hele rapport wordt herhaald, het gaat om een samenvattende conclusie.

8. **Adviezen en verbetermaatregelen**

In dit hoofdstuk worden de verbetermaatregelen weergegeven die uit het onderzoek zijn voortgekomen. Doe de aanbevelingen op hoofdlijnen en houd hierbij rekening met de volgende zaken:

- Zijn de verbetermaatregelen SMART (Specifiek/ Meetbaat/ Appelerend / Realistisch/ Tijdgebonden)?
- Is duidelijk voor wie de verbetermaatregelen zijn bestemd en hoe ze worden geborgd?
- Op welke tijdstermijn moeten deze maatregelen worden opgepakt?

Gebruik onderstaande tabel om de verbetermaatregelen weer te geven.

Verbetermaatregel	Verantwoordelijke	Termijn afgerond
Het protocol moet worden…	Directie [naam school] …	Binnen 3 maanden