PROCEDURE MELDING DATALEK

DE BRUG
School voor Praktijkonderwijs

Bron
Dyade

Bewerkt door:
Ronald van Rooijen en Emely de Louw

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	24-01-2019 14-02-2021	Dyade Emely de Louw	Concept ter goedkeuring MR
0.2	Vastgesteld	03-06-2021 13-07-2012	Emely de Louw	Vastgesteld door MR Vastgesteld door bestuur
0.3	Informeren/advies MR	03-06-2021	Emely de Louw	
0.4	Gepubliceerd in- en extern	14-06-2021	Emely de Louw	Op website geplaatst en team geïnformeerd (mail).
0.5	Gewijzigd			

Procedure Melden datalek De Brug School voor Praktijkonderwijs

Datum/versie: januari 2021 (conceptversie: 0.01)

In de Algemene verordening gegevensbescherming (AVG) is geregeld wanneer we een datalek (inbreuk in verband met persoonsgegevens) aan de Autoriteit Persoonsgegevens (AP) moeten melden. In deze procedure staat hoe intern te handelen bij een (mogelijk) datalek.

Definitie datalek

Een datalek is een inbreuk op de beveiliging, zoals bedoeld in artikel 4 lid 12 AVG, 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, waaronder begrepen, doch niet beperkt tot, verlies van een USB-stick of computer, inbraak door een hacker, verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden, een malwarebesmetting of een calamiteit zoals een brand in een datacentrum.

Tekst artikel 4 lid 12 AVG: "Inbreuk in verband met persoonsgegevens: 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"

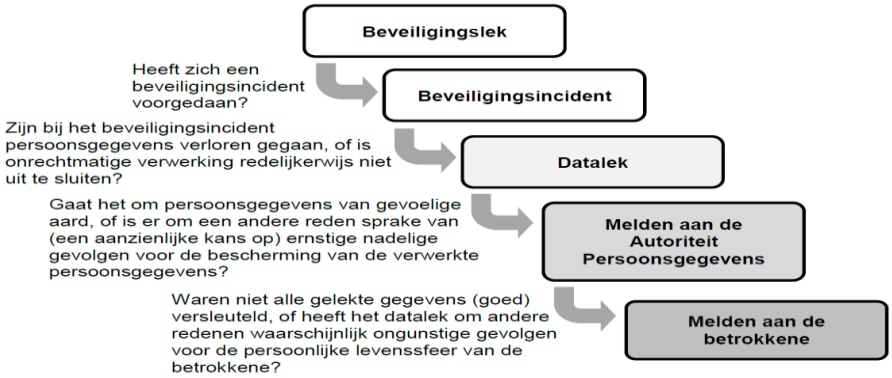
Melden datalek - Externe Functionaris Gegevensbescherming

Een (vermoeden van een) datalek wordt direct gemeld bij de Privacy Officer (adjunct-directeur) en Externe Functionaris Gegevensbescherming (EFG) van De Brug School voor Praktijkonderwijs via de mailbox privacyincidenten@prodebrug.nl. Dit is het meldpunt van De Brug School voor Praktijkonderwijs voor medewerkers, ouders, leveranciers, andere betrokkene(n).
Het bestuur is eindverantwoordelijk en de directeur, de heer Hans van Gent, is op school inhoudelijk verantwoordelijk voor IPB. Adjunct-directeur, mevrouw Emely de Louw, IBP Manager tevens Privacy Officer, is hoofdbeheerder van voornoemde mailbox.
De directeur, heer Hans van Gent, heeft als mede beheerder ook permanente toegang tot de mailbox en ondersteunt de hoofdbeheerder bij het bewaken en behandelen van de mailbox datalekmeldingen, vragen en aandachtspunten. De directeur vervangt de hoofdbeheerder bij arbeidsongeschiktheid, verlof, vakantie of andere reden van afwezigheid.

Afhandeling en registratie datalek in zeven stappen

Stap 1: Schakel direct de eerste externe functionaris gegevensbescherming (EFG) in: Het mailadres van de EFG is: ronald.van.rooijen@dyade.nl
Stap 2: Verzamel relevante informatie en bepaal of sprake is van een datalek
Stap 3: Tref direct maatregelen om het datalek te dichten en de gevolgen te beperken
Stap 4: Bepaal of het datalek gemeld moet worden bij de AP door de EFG
Stap 5: Bepaal of het datalek gemeld moet worden aan een of meer medewerkers, ouders, derden
Stap 6: Indien vereist, meld datalek bij de medewerker(s), ouder(s), derde(n)
Stap 7: Leg incident vast in datalekregister, ook als melden bij AP, ouders en derden niet nodig is

De EFG betrekt bij deze stappen binnen de schoolorganisatie zo nodig het bestuur, directeuren, privacy officer, ICT beheerder, etc.



Achtergrondinformatie om afwegingen te kunnen maken
Om voornoemde zeven stappen zo zorgvuldig mogelijk te kunnen zetten, is het van belang de relevante wettekst ernaast te houden. Zie daarvoor de AVG onder artikel 33 en 34 (bijlage 1) en de Handleiding bij de AVG onderdeel 5.9 (bijlage 2).
Op de website van de AP is eveneens informatie te vinden via de volgende link:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Elk besluit dat we nemen, moeten we altijd kunnen verantwoorden. Dus ook overwegingen die aan een besluit ten grondslag liggen, moeten we vastleggen. Als niet snel helder is te krijgen of we een datalek moeten melden of als achterliggende info ontbreekt, dient mogelijk een voorlopige melding bij de AP plaats te vinden, die later aangevuld of ingetrokken kan worden.

Melden bij de AP en betrokkene(n) - datalekregister
Een verwerkingsverantwoordelijke moet een inbreuk in verband met persoonsgegevens zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, melden aan de AP, tenzij het niet waarschijnlijk is dat deze inbreuk op persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, gaat de melding vergezeld van een motivering voor de vertraging (artikel 33 lid 1 AVG). Als medewerker(s), ouder(s) of derde(n) moet worden geïnformeerd over een incident waarbij sprake is van inbreuk op persoonsgegevens, wordt met betrokken manager(s) afgesproken wie de medewerker(s), ouder(s) of derde(n) informeert.

Melden bij de AP door De Brug School voor Praktijkonderwijs gaat altijd via een meldingsformulier via de website van de AP: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0 De AP heeft De Brug School voor Praktijkonderwijs een EFG-nummer toegekend dat (ook) bekend is bij de EFG en diens vervanger.
De EFG zorgt voor het mede beheren van het wettelijk verplichte register van datalekken voor De Brug, School voor Praktijkonderwijs, en neemt daarin samen met de IBP Manager tevens Privacy Officer de relevante informatie op rond (mogelijke) datalekken. Zoals aangegeven, moeten we elk besluit dat we nemen en de overwegingen die daaraan ten grondslag liggen, kunnen verantwoorden en dus eveneens vastleggen.

Schade beperken en herhaling voorkomen (corrigerende en preventieve maatregelen)
Wanneer een incident heeft plaatsgevonden is het zaak zo snel mogelijk de schade te beperken en herhaling te voorkomen. Denk aan extra beveiligingsmaatregelen, terugplaatsen bestanden, wachtwoorden aanpassen, autorisaties wijzigen. Het kan ook gaan om een indringend gesprek met betrokken medewerker(s), ouder(s) of derde(n). Dat hangt allemaal af van verschillende factoren waarbij feiten, omstandigheden, consequenties etc. een rol spelen. Ook hier is het belangrijk om de getroffen maatregelen vast te leggen. Het maakt bovendien deel uit van een datalekmelding.

Bijlage 1: Tekst Algemene Verordening Gegevensbescherming bij melden datalek

Artikel 33

Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit

1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de overeenkomstig artikel 55 bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

2. De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.

3. In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld:

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 contactpunt waar 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, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.

5. De verwerkingsverantwoordelijke documenteert alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de toezichthoudende autoriteit in staat de naleving van dit artikel te controleren.

Artikel 34

Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

2. De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen.

3. De in lid 1 bedoelde mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

a) de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;

b) de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het in lid 1 bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;

c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

4. Indien de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de toezichthoudende autoriteit, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke daartoe verplichten of besluiten dat aan een van de in lid 3 bedoelde voorwaarden is voldaan.

Bijlage 2: Tekst Algemene Verordening Gegevensbescherming bij melden datalek

5.9 Wat is de verplichting om een inbreuk in verband met persoonsgegevens mede te delen?

De Verordening bevat een verplichting om onder omstandigheden een inbreuk in verband met persoonsgegevens (een datalek) mede te delen aan de Autoriteit Persoonsgegevens en de betrokkene. Deze 'meldplicht datalekken' bestond sinds 1 januari 2016 reeds in Nederland onder de Wbp. Een datalek kan voor betrokkenen grote gevolgen hebben, waaronder verlies van controle over hun persoonsgegevens, de beperking van hun rechten, discriminatie, identiteitsdiefstal of financiële verliezen. Het is dan ook van belang dat een datalek tijdig en op passende wijze wordt aangepakt. De verplichte mededeling aan de Autoriteit Persoonsgegevens en in voorkomende gevallen aan de betrokkene is daar een uitwerking van.

5.9.1 Wanneer is er sprake van een inbreuk in verband met persoonsgegevens?

Een inbreuk in verband met persoonsgegevens, beter bekend als een datalek, is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Het is voor de kwalificatie als 'inbreuk in verband met persoonsgegevens' niet relevant dat er boos opzet in het spel is. Hoewel een *hack* van uw systemen waarbij persoonsgegevens worden buitgemaakt een schoolvoorbeeld is van een datalek, kunnen ook gegevens die op een verloren laptop staan of een afgesloten website met persoonsgegevens die per ongeluk openstaat ook kwalificeren als een datalek.

Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou *kunnen* leiden tot een beveiligingsincident. Er heeft zich *daadwerkelijk* een beveiligingsincident voorgedaan, en de preventieve maatregelen die u eventueel heeft getroffen waren niet toereikend om dit te voorkomen.

5.9.2 Moet ik ieder datalek melden aan de Autoriteit Persoonsgegevens?

Ja. In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht.

5.9.3 Wanneer moet ik aan de betrokkene mededelen dat er een inbreuk heeft plaatsgevonden?

Wanneer u heeft vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor betrokkenen inhoudt, dient u ook aan de betrokkenen mede te delen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens.

U hoeft de betrokkene niet te informeren wanneer:

- u passende technische en organisatorische beschermingsmaatregelen heeft genomen, bijvoorbeeld in de vorm van versleuteling van de gegevens;
- u achteraf maatregelen heeft genomen waarmee de vastgestelde risico's voor betrokkenen zijn weggenomen;

- de mededeling aan betrokkenen u onevenredig veel inspanning zou kosten. In dat geval kunt u volstaan met een openbare mededeling, bijvoorbeeld door de onder paragraaf 5.9.5 vereiste informatie te publiceren op uw website.

Verder hoeft u het datalek niet te melden bij de betrokkene wanneer het achterwege blijven van die melding noodzakelijk is ter waarborging van:

- de nationale veiligheid;
- de landsverdediging;
- de openbare veiligheid;
- de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, en de tenuitvoerlegging van straffen;
- andere belangrijke doelstellingen van algemeen belang van de Europese Unie of een lidstaat;
- de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
- de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
- een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt met de uitoefening van het openbaar gezag;
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen;
- de inning van civielrechtelijke vorderingen.

Voor de financiële sector geldt de meldplicht aan de betrokkene op grond van de Verordening niet. Voor deze sector geldt op grond van de Wet op het financieel toezicht dat een melding aan de betrokkene moet worden gedaan op grond van de zorgplicht.

Nota bene:
Wanneer u betrokkenen niet heeft geïnformeerd en de Autoriteit Persoonsgegevens is van mening dat dit alsnog moet gebeuren, dan kan zij haar handhavende bevoegdheden inzetten.

5.9.4 Wanneer moet ik het datalek melden?

U dient de Autoriteit Persoonsgegevens binnen 72 uur na ontdekking in kennis te stellen over het datalek. Het is goed mogelijk dat u de onder paragraaf 5.9.5 vermelde informatie niet binnen 72 uur volledig in beeld heeft. In die gevallen dient u zo veel mogelijk informatie binnen 72 uur te verstrekken en kunt u de overige informatie zonder onredelijke verdere vertraging in fasen aanleveren. De eerste kennisgeving dient in die gevallen vergezeld te gaan van een verklaring voor de vertraging.

Daarnaast dient u, wanneer kennisgeving aan betrokkenen vereist is, deze *onverwijld* te informeren. Het onverwijld melden houdt in dat u, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek om vast te stellen of u betrokkenen moet informeren. Wat in een concreet geval als 'onverwijld' moet worden aangemerkt zal afhangen van de omstandigheden van het geval. U moet daarbij rekening houden met het feit dat de betrokkene naar aanleiding van uw melding tijdig in staat moet zijn gesteld mogelijke maatregelen te nemen om de nadelige gevolgen van het datalek zo veel mogelijk te beperken of te voorkomen.

5.9.5 Welke informatie moet ik bij de melding verstrekken?

Welke informatie u moet verstrekken is afhankelijk van de vraag aan wie u de mededeling moet doen: de Autoriteit Persoonsgegevens of de betrokkenen.

Mededeling aan de Autoriteit Persoonsgegevens

U dient de Autoriteit Persoonsgegevens bij het doen van de melding in ieder geval van de volgende informatie te voorzien:

- de aard en omvang van de inbreuk;
- waar mogelijk de categorieën van betrokkenen, de persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die u heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Mededeling aan betrokkenen

Wanneer u betrokkenen moet informeren over de inbreuk, dient die kennisgeving in ieder geval de volgende elementen te bevatten:

- 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 u heeft voorgesteld of genomen om de inbreuk aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

U dient de kennisgeving aan betrokkenen in duidelijke en eenvoudige taal op te stellen.

5.9.6 Wat moet ik verder met de mededeling doen?

U dient het datalek te documenteren in een overzicht van datalekken die zich in uw organisatie hebben voorgedaan. In dit overzicht dient u ten minste de feiten omtrent de inbreuk en de gevolgen ervan te documenteren. Verder is het verstandig met het oog op het verantwoordingsbeginsel en uw bewijspositie om de door u genomen corrigerende maatregelen ook te documenteren.

Lees meer:

Artikel 33 AVG | Overweging 75, 85, 87, 88 (melding van een datalek aan de toezichthoudende autoriteit)
Artikel 34 AVG | Overweging 75, 86, 87, 88 (melding van een datalek aan de betrokkene
Artikel 23 AVG | Overweging 73 (beperkingen)
Artikel 42 UAVG | (Uitzondering op meldplicht datalekken aan de betrokkene)

Groep Gegevensbescherming Artikel 29, *Guidelines on Personal data breach notification under Regulation 2016/679*, aangenomen 3 oktober 2017, 17/EN WP250