Stichting Volare
Procedure meldplicht datalekken

STICHTING VOLARE
SPECIAAL
VOOR ONDERWIJS

Versie november 2024

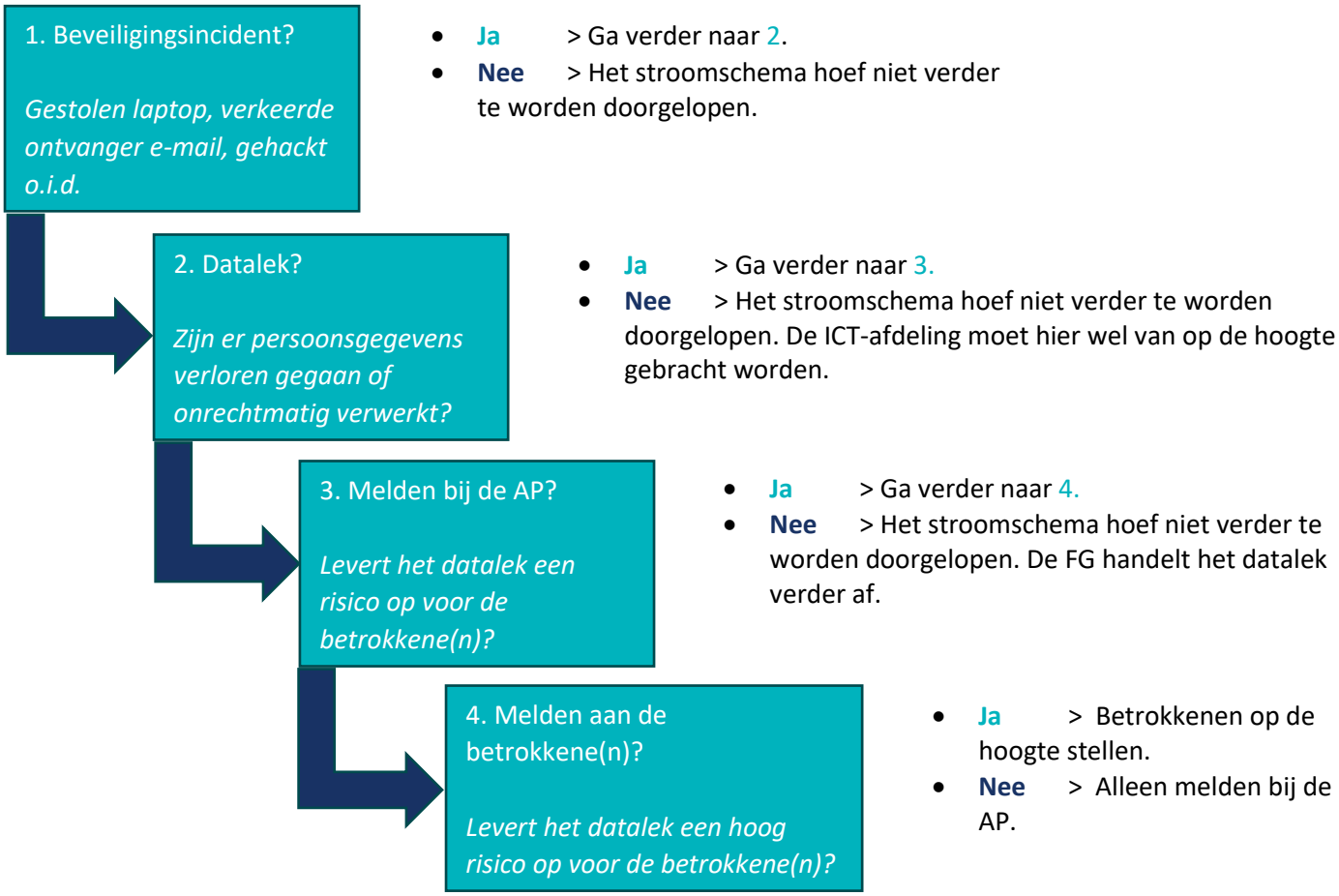
Inleiding

In de privacywetgeving (Algemene verordening gegevensbescherming (verder: **AVG**)) is een meldplicht voor datalekken opgenomen. Deze meldplicht verplicht organisaties om datalekken te melden bij de toezichthouder, namelijk de Autoriteit Persoonsgegevens (verder: **AP**). In sommige gevallen, dient een datalek ook bij de betrokkene(n) te worden gemeld. Betrokkenen zijn de personen wiens gegevens gelekt zijn. Dat zijn bijvoorbeeld de leerlingen (en de ouders/ verzorgers daarvan), maar ook de medewerkers van Stichting Volare.

Het is aan de verwerkingsverantwoordelijke om een datalek te melden aan de AP en eventueel aan de betrokkene(n). In haar rol als verwerkingsverantwoordelijke dient Stichting Volare datalekken daarom zelf te melden. Wanneer een datalek bij een verwerker van Stichting Volare plaatsvindt, dient de verwerker dit zo snel mogelijk aan Stichting Volare te melden, zodat Stichting Volare kan beoordelen of zij dit aan de AP en, in sommige gevallen, aan de betrokkene(n) dient te melden.

In deze procedure over de meldplicht van datalekken wordt omschreven op welke manier Stichting Volare omgaat met eventuele datalekken. Hierbij is uitgegaan van de rol van Stichting Volare als verwerkingsverantwoordelijke. In het plan is vastgelegd hoe en naar wie de meldingen intern worden doorgezet, wie intern verantwoordelijk is voor welke melding, en hoe en in welke vorm de melding aan de toezichthouder en eventueel ook aan de betrokkene(n) wordt gedaan.

De onderstaande beslisboom kan gebruikt worden om te bepalen of er sprake is van een datalek, en zo ja, of een melding gedaan moet worden aan de AP en aan de betrokkene(n):



Wat is een datalek?

De meldplicht is alleen van toepassing wanneer er daadwerkelijk sprake is van een datalek. Er is sprake van een datalek als er persoonsgegevens **inzichtelijk** zijn geworden voor mensen die deze niet mogen zien of wanneer de gegevens **verloren** zijn gegaan, terwijl dat niet de bedoeling was. Ook wanneer persoonsgegevens anderszins onrechtmatig worden verwerkt óf wanneer dit niet valt uit te sluiten, is er sprake van een datalek.[1] Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Andere voorbeelden van datalekken zijn:

- Een kwijtgeraakte USB-stick die persoonsgegevens bevat
- Een gestolen of gehackte laptop
- Het versturen van een e-mail met daarin persoonsgegevens van een huurder naar de verkeerde ontvanger.
- Het plaatsen van e-mailadressen in 'CC' in plaats van in 'BCC', waardoor personen elkaars e-mailadres kunnen inzien.
- Een brief is bij een verkeerde leerling of ouder bezorgd.

Procedure voor het melden van een datalek

Wanneer er binnen Stichting Volare een datalek plaatsvindt, dient iedereen te weten hoe er gehandeld moet worden. Reden hiervoor is dat de melding van het datalek zo snel mogelijk de juiste persoon binnen Stichting Volare moet bereiken. In sommige gevallen moet namelijk een melding worden gedaan bij de AP, en eventueel ook bij de betrokkene(n). Is er sprake van een datalek, dan moet daar binnen 72 uur na ontdekking van het datalek melding van worden gedaan bij de AP.[2] Stichting Volare hanteert daarom het volgende stappenplan:

Stap 1: Melden beveiligingsincident aan de Functionaris Gegevensbescherming

Als er binnen Stichting Volare een beveiligingsincident plaatsvindt, dient de ontdekker van dit beveiligingsincident dit te melden aan de Functionaris Gegevensbescherming (verder: **FG**). Een beveiligingsincident is een **inbreuk op de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens**. De ontdekker van het beveiligingsincident zorgt ervoor dat het datalekkenformulier ingevuld wordt en opgestuurd wordt. Dit formulier is **hier** te vinden.

Stap 2: Inventariseren

De FG dient over voldoende informatie te beschikken over het beveiligingsincident. Deze informatie ontvangt de FG in de vorm van de door de ontdekker online ingevulde formulier. Blijkt de informatie uit het formulier niet voldoende te zijn, dan zal de FG in overleg treden met de ontdekker van het beveiligingsincident en/of de ICT afdeling.

Stap 3: Is het beveiligingsincident een datalek?

Een beveiligingsincident is nog geen datalek. Een beveiligingsincident wordt pas een datalek wanneer de inbreuk gevolgen heeft voor de persoonsgegevens die Stichting Volare verwerkt. Die gevolgen kunnen bijvoorbeeld bestaan uit het verlies van persoonsgegevens, of een onrechtmatige verwerking daarvan, maar ook het inzien door iemand die gegevens niet in had mogen zien.[3] Wanneer de FG voldoende informatie heeft verzameld, beoordeelt deze daarom op basis van de antwoorden op de vragen in online formulier of er sprake is van een datalek.

---

[1] Artikel 4 lid 12 Algemene verordening gegevensbescherming. Een onrechtmatige verwerking van persoonsgegevens kan bestaan uit 1) inbreuk op de vertrouwelijkheid; 2) een inbreuk op de integriteit; en 3) inbreuk op de beschikbaarheid.

[2] Artikel 33 lid 1 Algemene verordening gegevensbescherming.

[3] Artikel 4 lid 12 Algemene verordening gegevensbescherming. Een onrechtmatige verwerking van persoonsgegevens kan bestaan uit 1) inbreuk op de vertrouwelijkheid; 2) een inbreuk op de integriteit; en 3) inbreuk op de beschikbaarheid.

Stap 4: Dient het datalek gemeld te worden aan de AP?

Niet alle datalekken hoeven gemeld te worden aan de AP. Een datalek moet enkel gemeld worden aan de AP indien er sprake is van een risico voor de rechten en vrijheden van de betrokkene(n). Dit risico is aanwezig in twee situaties:

- Bij een kwantitatief ernstig lek (hiervoor kijk je naar de hoeveelheid betrokken persoonsgegevens)
- Bij een kwalitatief ernstig lek (hiervoor kijk je naar de gevoeligheid van de betrokken persoonsgegevens)

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek' dient er daarom rekening gehouden te worden met de hoeveelheid persoonsgegevens en met het type persoonsgegevens. Telkens dient de FG een afweging te maken of een datalek gemeld moet worden aan de AP. Hierbij zijn ook nog andere factoren van belang.[4] Om de afweging te kunnen maken beantwoord FG de volgende vragen:

- Wat is er precies gebeurd (is er sprake van een intern/extern datalek)?
- Welke data (gegevens) zijn betrokken bij het datalek?
- Waarom is het wel/geen datalek dat gemeld moet worden?
- Wat zijn de (mogelijke) gevolgen van het datalek?
- Wie zijn er reeds geïnformeerd?
- Wat zijn de te nemen vervolgstappen (melding aan de AP/betrokkene(n))?

Op basis van de antwoorden op deze vragen, bepaalt de FG of er sprake is van een datalek dat gemeld dient te worden of niet.

Van een datalek dat gemeld dient te worden, is sprake wanneer er gegevens van heel veel leerlingen of andere betrokkenen van Stichting Volare gelekt zijn. Maar van een datalek dat gemeld moet worden is ook sprake wanneer de gelekte gegevens gevoelig of van bijzondere aard zijn. Te denken valt dan bijvoorbeeld aan persoonsgegevens over de gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene.

Stap 5: Melden aan de AP

Brengt het datalek een risico voor de rechten en vrijheden van de betrokkene(n) met zich mee, dan moet er dus een melding worden gedaan bij de AP. Hiervoor geldt als termijn dat het datalek zo snel mogelijk, maar uiterlijk binnen 72 uur na ontdekking, aan de AP gemeld moet worden via de **website van de AP.**

Stap 6: Dient het datalek gemeld te worden aan de betrokkene(n)?

Het is mogelijk dat een datalek niet alleen aan de toezichthouder gemeld moet worden, maar ook aan de betrokkene(n). Dit is het geval wanneer het datalek een **hoog risico** inhoudt voor betrokkene(n). Er is sprake van een datalek met een hoog risico, wanneer het privéleven van de betrokkene(n) waarschijnlijk door het datalek wordt geschaad. Voorbeelden daarvan zijn identiteitsdiefstal of -fraude, financiële verliezen en reputatieschade. Als het gaat om persoonsgegevens van gevoelige aard, zoals financiële gegevens, of om een grote hoeveelheid persoonsgegevens, dan dient er altijd een melding aan de betrokkene(n) gedaan te worden, tenzij de gegevens beveiligd zijn.

Stap 7: Melden aan de betrokken(n)

De melding aan de betrokkene(n) dient zorgvuldig uitgevoerd te worden. De melding dient de volgende informatie te bevatten:

[4] Zie hiervoor Artikel 29-werkgroep, richtsnoeren meldplicht datalekken, herziene versie, 6 februari 2018.

Melding datalek aan betrokkene(n)	
Omschrijving	Op [datum] heeft er bij Stichting Volare een datalek plaatsgevonden waarbij uw gegevens betrokken zijn. [uitgebreide omschrijving].
Vragen?	Voor vragen kunt u contact opnemen met de FG binnen Stichting Volare, via privacy@akorda.nl of [telefoonnummer].
Wat kunt u doen?	Om de gevolgen van dit datalek te beperken raden wij u aan om de volgende maatregelen te treffen: [maatregelen]

Hierbij wordt rekening gehouden met de doelgroep. Wanneer het datalek over leerlingen gaat, dan zal de tekst op een simpele en begrijpbare wijze weergegeven worden. Uiteraard is het verstandig om middels het begeleidend schrijven de betrokkene(n) excuses aan te bieden en duidelijk te maken dat Stichting Volare het datalek inmiddels heeft gedicht (indien dat het geval is) en er alles aan zal doen om dergelijke gevallen in de toekomst te voorkomen.

Stap 8: Datalek registreren in het datalekregister

Heeft de FG geconstateerd dat er sprake is van een datalek, dan dient alle informatie die in de voorafgaande stappen is ingewonnen, intern geregistreerd te worden in het datalekregister. Het datalekregister is een apart register dat bij de FG ter beschikking is. De FG is verantwoordelijk voor het registreren van het datalek.

Let op: ieder datalek dient geregistreerd te worden in het datalekkenregister, ook datalekken die niet gemeld zijn aan de AP en/of betrokkene(n).