Procedure Meldplicht Datalekken

Stichting BOOR

Geactualiseerde versie 0.1.2

Vastgesteld door het college van bestuur van stichting BOOR op 15 juni 2020

Inhoudsopgave

1. Doel

Op grond van artikel 33 en 34 van de Algemene verordening gegevensbescherming (AVG) geldt een meldplicht en registratieplicht voor datalekken. Deze meldplicht houdt in dat stichting BOOR als Verwerkingsverantwoordelijke in beginsel een datalek moet melden aan de Autoriteit Persoonsgegevens (AP), en in bepaalde gevallen ook aan de betrokkene(n).

Deze procedure beschrijft hoe te handelen indien sprake is van een (vermoedelijk) datalek binnen stichting BOOR als buiten haar organisatie, maar waarvoor stichting BOOR als Verwerkingsverantwoordelijke de eindverantwoordelijkheid draagt voor de persoonsverwerkingen.

2. Definities

In deze procedure Meldplicht Datalekken worden de volgende begrippen gehanteerd:

AP	Autoriteit Persoonsgegevens.
AVG	Algemene verordening gegevensbescherming.
Betrokkene(n)	Degene(n) op wie een persoonsgegeven betrekking heeft/ hebben.
Beveiligingsincident	Een inbreuk op de beveiliging.
Datalek	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.
Functionaris voor de Gegevensbescherming	De functionaris die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG.
Persoonsgegeven	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
Privacy Ambassadeur	Een medewerker op een BOOR-school(locatie), die aanspreekpunt is voor leerlingen, ouders en het team als er vragen zijn over privacy en de AVG.

Privacy Officer	Medewerker die verantwoordelijk is voor de uitvoering van het vastgestelde beleid op het terrein van gegevensbescherming en privacy binnen BOOR.
CISO	Medewerker die verantwoordelijk is voor het implementeren van, en toezicht houden op het informatiebeveiligingsbeleid, onder andere door zijn centrale rol in het beheren van de processen die hiermee te maken hebben.

3. Identificeren van een beveiligingsincident

De medewerker die een beveiligingsincident constateert, dient dit per omgaande bij de Privacy Ambassadeur van zijn school te melden (eventueel via zijn leidinggevende). De Privacy Ambassadeur vermeldt het beveiligingsincident in het incidentenregister van zijn school.

4. Is er sprake van een datalek?

Nadat de Privacy Ambassadeur is geïnformeerd over het beveiligingsincident, zal hij zo spoedig mogelijk zorgdragen voor het verzamelen van volledige en juiste informatie. Op basis van de verkregen informatie wordt in overleg met de Privacy Officer en de Chief Information Security Officer (CISO) van stichting BOOR zo spoedig mogelijk een inschatting gemaakt of sprake is van een datalek. Bij de inschatting of er sprake is van een datalek, dient het navolgende in overweging te worden genomen:

Heeft het beveiligingsincident per ongeluk of op onrechtmatige wijze geleid tot:

- Vernietiging van persoonsgegevens?
- Verlies van persoonsgegevens?
- Een wijziging van de persoonsgegevens?
- Een ongeoorloofde verstrekking van persoonsgegevens?
- Een ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens?

Indien één van bovenstaande vragen met “Ja” kan worden beantwoord is er sprake van een datalek. Ook een verwerker kan een datalek constateren en melden aan stichting BOOR.

5. Melden aan de AP

Indien er sprake is van een datalek, dan zal de Privacy Officer in overleg treden met de Functionaris voor de Gegevensbescherming over melding aan de AP, tenzij het onwaarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, een en ander ter beoordeling door de Functionaris voor de Gegevensbescherming.

6. Termijnen voor het doen van een melding bij de AP

De AP dient binnen 72 uur na ontdekking van het datalek in kennis te worden gesteld. Wanneer de in paragraaf 7 vermelde informatie niet binnen 72 uur volledig in beeld is, dient zo veel mogelijk informatie te worden verstrekt. De overige informatie kan zonder onredelijke verdere vertraging in fasen worden aangeleverd. De eerste kennisgeving dient in die gevallen vergezeld te gaan van een verklaring voor de vertraging.

7. Welke informatie moet aan de AP worden verstrekt?

De navolgende informatie wordt door de Privacy Officer of de Functionaris voor de Gegevensbescherming aan de AP verstrekt:

- de aard en omvang van het datalek;
- 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 de Gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die stichting BOOR heeft voorgesteld of genomen om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

8. Hoe te melden bij de AP?

De Privacy Officer of de Functionaris voor de Gegevensbescherming maakt voor het doen melden van het datalek gebruik van het online meldingsformulier van de AP.

9. Melden aan de betrokkene(n)

De Privacy Officer of de Functionaris voor de Gegevensbescherming zal het datalek tevens aan de betrokkene(n) melden indien het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Een melding aan de betrokkene(n) kan achterwege worden gelaten indien is voldaan aan een van de volgende voorwaarden:

- stichting BOOR heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop het datalek betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;

- stichting BOOR heeft achteraf maatregelen genomen om ervoor te zorgen dat het hiervoor bedoelde hoge risico voor de rechten en vrijheden van de betrokkene(n) dat anderen zonder toestemming toegang hebben tot persoonsgegevens, zich waarschijnlijk niet meer zal voordoen;
- de mededeling zou, ter beoordeling door de Functionaris voor de Gegevensbescherming, onevenredige inspanningen vergen. In dat geval zorgt stichting BOOR ervoor dat in de plaats daarvan er een openbare mededeling of een soortgelijke maatregel komt waarbij de betrokkenen even doeltreffend worden geïnformeerd.

Daarnaast hoeft het datalek niet te worden gemeld bij de betrokkene(n) 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(n) of van de rechten en vrijheden van anderen;
- de inning van civielrechtelijke vorderingen.

Indien stichting BOOR heeft besloten om het datalek niet te melden aan de betrokkene(n), kan de AP, na beraad over de kans dat het datalek een hoog risico met zich meebrengt, stichting BOOR verplichten alsnog een melding te maken aan de betrokkene(n). Als deze situatie zich voordoet, coördineert de Privacy Officer de afhandeling.

10. Termijn voor het doen van een melding aan de betrokkene(n)

De Privacy Officer of de Functionaris voor de Gegevensbescherming zal, wanneer kennisgeving aan de betrokkene(n) vereist is, deze onverwijld informeren. Het onverwijld melden houdt in dat de Privacy Officer of de Functionaris voor de Gegevensbescherming, na het ontdekken van een datalek, enige tijd mag nemen voor nader onderzoek om vast te stellen of de betrokkene(n) moet(en) worden geïnformeerd. De Privacy Officer overlegt hierover met de Functionaris voor de Gegevensbescherming. Wat in een concreet geval als ‘onverwijld’ moet worden aangemerkt zal afhangen van de omstandigheden van het geval. De Privacy Officer, moet daarbij rekening houden met het feit dat de betrokkene(n) naar

aanleiding van de melding van een datalek tijdig in staat moet zijn mogelijke maatregelen te nemen om de nadelige gevolgen van het datalek zo veel mogelijk te beperken of te voorkomen.

11. Welke informatie moet aan de Betrokke(n) worden verstrekt?

De navolgende informatie wordt door de Functionaris voor de Gegevensbescherming aan de betrokkene(n) verstrekt:

- een omschrijving van de aard van het datalek;
- de naam en contactgegevens van de Functionaris voor de Gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk voor de betrokkene(n);
- de maatregelen die stichting BOOR heeft voorgesteld of genomen om het datalek aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

De betrokkene(n) worden in duidelijke en eenvoudige taal in kennis gesteld van het datalek.

12. Registratieplicht

De Privacy Officer van stichting BOOR houdt een registratie bij van alle datalekken die zich hebben voorgedaan. In deze registratie worden in ieder geval de details van het datalek, de gevolgen die het datalek had voor de betrokkene(n) en de corrigerende maatregelen die stichting BOOR heeft genomen opgenomen. Deze registratie stelt de AP in staat om na te gaan of aan de AVG is voldaan.