Protocol beveiligingsincidenten en datalekken Stichting Vrije School Amstelveen & Stichting Geert Groote Scholen Amsterdam

De AVG bepaalt dat datalekken direct, binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens (AP), tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Daarnaast moet het datalek ook aan de betrokkenen gemeld worden indien het waarschijnlijk een groot risico voor de persoonlijke levenssfeer van de betrokkenen met zich meebrengt. Hieraan moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelekt zijn van belang. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelekt zijn dan is de melding meestal noodzakelijk.

Dit protocol beveiligingsincidenten en datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of en hoe deze gemeld moet worden.

Het is van belang dat alle medewerkers van de Stichting Vrije School Amstelveen & Stichting Geert Groote Scholen Amsterdam op de hoogte zijn van deze notitie. Het is belangrijk dat er geen datalekken gemist worden. Individuele medewerkers moeten datalekken kunnen herkennen en weten wat de te nemen stappen zijn. Medewerkers binnen de organisatie dienen zich er van bewust te zijn dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de Functionaris voor Gegevensbescherming (FG), zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens. Zij dienen bekend te zijn met het in dit protocol opgenomen stappenplan.

Wat is een datalek?

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de AP persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer. Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:

- kwijtraken van een USB–stick;
- diefstal van een laptop of telefoon;
- het verliezen van gegevens op papier;
- onbevoegde toegang tot een gebouw/locaties/ruimten/kasten;
- inbraak door een hacker;
- persoonsgegevens per ongeluk gepubliceerd;

- hacking, mailware of fishing;
- persoonsgegevens aan verkeerde persoon verstuurd;
- calamiteiten zoals brand in een datacentrum.

Een beveiligingsincident betekent dat inbreuk heeft plaatsgevonden op de beschermingsmaatregelen die de verwerkingsverantwoordelijke heeft genomen of had moeten nemen om persoonsgegevens tegen verlies of tegen enige vorm van onrechtmatige verwerking te beveiligen. Van een beveiligingsincident hoeft geen melding te worden gedaan aan de AP. Beveiligingsincidenten moeten wel altijd bij de FG te worden gemeld.

Melden aan de Autoriteit Persoonsgegevens

Artikel 33 van de AVG bepaalt wanneer en op welke manier een datalek aan de AP moet worden gemeld. De belangrijkste vereisten zijn de volgende:

- Een melding aan de AP moet plaatsvinden bij elk incident met betrekking tot persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico voor de betrokkene(n) inhoudt;
- Het datalek wordt door het schoolbestuur aan de AP gemeld;
- De melding vindt binnen 72 uur plaats. Indien de melding niet binnen 72 uur plaatsvindt, moet de vertraging worden gemotiveerd;
- Indien het datalek door een verwerker wordt geconstateerd, informeert hij het schoolbestuur zonder onredelijke vertraging nadat hij van het datalek heeft kennisgenomen;

De melding aan de AP bevat ten minste de volgende onderdelen:

- de aard van de datalek, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en de contactgegevens van de FG of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die het schoolbestuur 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.

Melding aan de AP kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelekt van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de FG betrokken moeten worden.

Melden aan de betrokkene(n)

Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens. Als er persoonsgegevens van gevoelige aard (bijv. gezondheidsgegevens) gelekt zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de FG betrokken moeten worden.

Indien betrokkenen over het datalek moeten worden geïnformeerd, is het belangrijk dat dit snel en adequaat gebeurd. Dit biedt de betrokkenen de mogelijkheid om maatregelen te nemen om eventuele schade te voorkomen of te beperken. Tevens verkleint dit de kans op reputatieschade, financiële schade en/of andere schade van Stichting Vrije School Amstelveen & Stichting Geert Groote Scholen Amsterdam.

Artikel 34 van de AVG bepaalt wanneer en op welke manier een datalek aan de betrokkene moet worden gemeld. De belangrijkste vereisten zijn de volgende:

- Wanneer het datalek “waarschijnlijk een hoog risico inhoudt” voor de betrokkene, deelt het schoolbestuur de betrokkene de inbreuk in verband met persoonsgegevens mee;
- De melding aan de betrokkene dient “onverwijld” plaats te vinden;
- De melding aan de betrokkene is opgesteld in eenvoudige en duidelijke taal;
- De melding aan de betrokkene bevat ten minste de onderdelen zoals vermeld in onder ‘Melden aan de Autoriteit Persoonsgegevens’ b-d.

Informeren van derden

In geval van (grootschalige) datalekken kan de Stichting Vrije School Amstelveen & Stichting Geert Groote Scholen Amsterdam contact opnemen met de pers om ze te informeren. Het is belangrijk om de volgende aspecten in overweging te nemen:

- Het schoolbestuur is transparant;
- Het schoolbestuur biedt excuses aan en legt uit dat er wordt gewerkt aan een betere beveiliging;
- Het schoolbestuur geeft in heldere taal aan welke stappen de betrokkenen zelf kunnen nemen om de schade te beperken.

Verwerker

Het kan gebeuren dat het datalek optreedt bij de verwerker. Stichting Vrije School Amstelveen & Stichting Geert Groote Scholen Amsterdam is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het datalek bij de verwerker. De verwerker zal in dat geval bij het stappenplan betrokken moeten worden.

Via de verwerkersovereenkomst moet afgedwongen worden dat de verwerker eventuele datalekken terstond (binnen 24 uur) meldt bij de organisatie en de organisatie helpt bij het beoordelen of er

gemeld moet worden en de afwikkeling van het datalek. Belangrijk is dat de verwerker niet buiten de organisatie om een datalek meldt bij de AP. De verwerker moet verder alle redelijke instructies van de Stichting Vrije School Amstelveen & Stichting Geert Groote Scholen Amsterdam opvolgen.

Boete

Bij overtreding van de meldplicht datalekken kan de AP een (hoge) boete opleggen. De kans op een boete is groter bij niet melden dan bij wel melden.

Communicatie

Voor Stichting Vrije School Amstelveen & Stichting Geert Groote Scholen Amsterdam is het heel belangrijk dat ouders, leerlingen en medewerkers erop kunnen vertrouwen dat zijn of haar persoonsgegevens zorgvuldig worden verwerkt. Dat vertrouwen wordt gecreëerd door inzichtelijk te maken op welke wijze gegevens worden verwerkt en beheerd. Hierbij wordt duidelijk:

- welke gegevens worden verzameld;
- waarom deze gegevens worden verzameld;
- wat vervolgens met deze gegevens gebeurt;
- wie toegang heeft tot deze gegevens;
- welke rechten ouders en medewerkers hebben.

Stichting Vrije School Amstelveen & Stichting Geert Groote Scholen Amsterdam heeft daartoe principes en verantwoordingsplicht vastgelegd in het privacyreglement.

Evalueren

Na het afsluiten van het proces van afhandeling van het datalek zal de FG een evaluatie moment initiëren. Doel is om het proces te evalueren en verbeteracties te bepalen. Van deze evaluatie wordt een verslag gemaakt en door de FG bewaard.

Stappenplan beveiligingsincidenten en datalekken

De FG draagt zorg voor de invoering en naleving van het hieronder opgenomen stappenplan . Indien er een datalek optreedt dienen de stappen in het stappenplan doorlopen te worden.

STAPPENPLAN BEVEILIGINGSINCIDENTEN EN DATALEKKEN

Processtappen	Activiteit	Verantwoordelijke persoon
1. Er wordt een beveiligingsincident of mogelijk datalek ontdekt	• Maak direct intern melding van (mogelijke) datalek • Informeer de FG	Medewerker die het ontdekt
2. Beoordeel het beveiligingsincident	• Onderzoek het beveiligingsincident • Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden • Beoordeel wie binnen de organisatie hierbij betrokken zijn • Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden	FG i.s.m.: • Schooldirecteur van de school waar binnen het datalek heeft plaatsgebonden • Uitvoerend bestuurder • ICT-medewerker
3. Als er sprake is van een datalek: bestrijdt het datalek	• Stop het datalek als het nog kan • Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperkten • Leg de acties van de genomen maatregelen vast in het dossier	FG i.s.m.: • Schooldirecteur van de school waar binnen het datalek heeft plaatsgebonden • Uitvoerend bestuurder • ICT-medewerker
4. Vaststellen impact datalek	• Onderzoek het datalek en de gevolgen daarvan • Onderzoek de aard van de gegevens die gelekt zijn (bijvoorbeeld gezondheidsgegevens) • Onderzoek de omvang van de gelekte gegevens • Beoordeel welke impact het lek kan hebben op de betrokken personen • Stel vast wat de nadelige gevolgen kunnen zijn	FG i.s.m.: • Schooldirecteur van de school waar binnen het datalek heeft plaatsgebonden • Uitvoerend bestuurder • ICT-medewerker

5. Vaststellen Meld en Herstelaanpak	• Bepaal aanpak/informeren AP • Bepaal aanpak/informeren betrokkenen • Bepaal acties voor nazorg betrokkenen • Bepaal acties voor belang van de organisatie • Bepaal acties voor verbetering beveiliging	FG i.s.m.: • Schooldirecteur van de school waar binnen het datalek heeft plaatsgebonden • Uitvoerend bestuurder • ICT-medewerker
6. Melden AP	• Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur • Melding via de website van het AP • Het Meldformulier Datalekken kan gebruikt worden	FG i.s.m.: • Uitvoerend bestuurder • ICT-medewerker
7. Melden betrokkenen	• Melding via bijvoorbeeld brief • Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. • Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	FG i.s.m.: • Uitvoerend bestuurder • Bestuur (afhankelijk van de ernst van de situatie)
8. Uitvoeren herstelwerkzaamheden	• Herstel het datalek • Verbeteren van de beveiliging • Lever nazorg aan de betrokkenen	FG i.s.m.: • Uitvoerend bestuurder • ICT-medewerker
9. Optimaliseer het beveiligings- en het datalek proces	• Registreer, evalueer en verbeter de beveiliging en het proces inzake melding beveiligingsincidenten en datalekken	FG i.s.m.: • Uitvoerend bestuurder • Bestuur

BESLISBOOM

Onderstaande beslisboom kan bij het beoordelen van een beveiligingsincident / datalek gebruikt worden: