VRIJE UNIVERSITEIT AMSTERDAM

WERKPROCES MELDPLICHT DATALEKKEN

Versie 1.1

VRIJE UNIVERSITEIT AMSTERDAM

IS VERDER KIJKEN

Werkproces meldplicht datalekken

Inhoudsopgave

1. Inleiding

Sinds 25 mei 2018 is onder de Algemene Verordening Gegevensbescherming (hierna: AVG) de meldplicht datalekken van toepassing. Deze meldplicht houdt in dat de VU verplicht is om datalekken zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur te melden bij de Autoriteit Persoonsgegevens (hierna: AP), tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van personen. Wanneer het waarschijnlijk is dat het datalek een hoog risico inhoudt voor de rechten en vrijheden van personen moet het datalek ook gemeld worden bij de betrokkenen (medewerkers, onderzoeksdeelnemers, studenten, etc.).

De AP kan handhavend optreden bij het niet, niet tijdig of niet juist melden van een datalek. Hieronder valt ook de oplegging van een administratieve boete, die in (zeer) ernstige gevallen, op basis van de AVG, kan oplopen tot € 10.000.000, of 2% van de totale jaaromzet.

Het onderhavige werkproces helpt de VU om op een correcte manier te voldoen aan het wettelijke vereiste uit de AVG om een datalek tijdig te melden bij de AP en volgt het bepaalde in het Reglement ICT-voorzieningen voor medewerkers van de Vrije Universiteit Amsterdam (hierna: Reglement).

2. Wat is een datalek?

De term ‘datalek’ komt niet voor in de wet. In plaats daarvan spreekt de AVG over een ‘inbreuk in verband met persoonsgegevens’. Van een datalek is sprake bij ‘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’.

Er zijn in dit kader drie categorieën datalekken te onderscheiden[1]:

1. inbreuk op de vertrouwelijkheid > dit is een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens;
2. inbreuk op de integriteit > dit is een onbevoegde of onopzettelijke wijziging van persoonsgegevens; of
3. inbreuk op de beschikbaarheid > dit is een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

Eén datalek kan, afhankelijk van de omstandigheden, in meerdere categorieën vallen.

3. Werkproces afhandeling datalek

Voor een zorgvuldige afhandeling van een datalek is het van belang een helder werkproces te hebben. Met het onderhavige werkproces wil de VU waarborgen dat datalekken zo snel mogelijk worden gesignaleerd en afgehandeld.

[1] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

3.1 Aanleiding

Een (vermoeden van een) datalek kan aan het licht komen bij (automatische) constatering van een beveiligingsincident - zoals een computervirus of hack - of door melding hiervan door medewerkers, studenten of derden.

Medewerkers die een (potentieel) datalek constateren, dienen dit zo snel mogelijk te melden bij de IT-Servicedesk, zoals ook voorzien in artikel 7 van het Reglement. Voorbeelden van (potentiele) datalekken die moeten worden gemeld bij de IT-Servicedesk, zijn:

- het verlies van een computer, USB-stick of telefoon met niet-versleutelde persoonsgegevens (bij twijfel altijd melden);
- besmettingen met computervirussen en/of malware waarbij persoonsgegevens verloren zijn gegaan;
- een hack van een systeem waarbij persoonsgegevens ontoegankelijk zijn gemaakt;
- het versturen van (gevoelige) persoonsgegevens naar een verkeerde geadresseerde;
- het per ongeluk publiceren van (gevoelige) persoonsgegevens.

Omdat een datalek ook bijna altijd een (potentiële) inbreuk op de IT-beveiliging is, zet de IT-Servicedesk alle meldingen van (potentiële) datalekken zo snel mogelijk door naar het Security and Operations Control Center (hierna: SOCC) van de VU. Het voordeel hiervan is dat dan meteen de technische expertise is aangehaakt om te onderzoeken wat er (technisch) aan de hand is en welke technische maatregelen kunnen of moeten worden getroffen om verdere schade te voorkomen. Daarnaast worden de (potentiële) datalekken op die manier zoveel mogelijk uniform geregistreerd en afgehandeld.[2]

Het SOCC informeert op zijn beurt zo snel mogelijk de Functionaris Gegevensbescherming (hierna: FG) van de VU, voor zover de FG nog niet betrokken is en de Chief Information Security Officer (hierna: CISO). Voor datalekken binnen ACTA geldt dat deze worden gecoördineerd door de FG van ACTA.

3.2 Feiten en analyse

Na constatering van een beveiligingsincident dat een (potentieel) datalek betekent, worden de feiten verzameld en vervolgens een analyse gemaakt. Het verzamelen van feiten en het maken van de analyse wordt gecoördineerd door de FG en gebeurt in nauwe samenwerking met het SOCC en de CISO.

Bij het verzamelen van de feiten gaat het om de feiten met betrekking tot het incident zelf, maar ook om de feiten over de context van het incident. Denk bij dit laatste aan informatie over de betrokken systemen, de verwerkingen die mogelijk zijn geraakt door het incident, de categorieën van persoonsgegevens en betrokkenen en de (tijdelijke) maatregelen die moeten worden genomen om verdere schade te voorkomen.

Na verzameling van de feiten volgt een analyse van de feiten, waarbij ook richtsnoeren van de Europese toezichthouders van belang zijn.[3] Op basis van de beschikbare informatie wordt nagegaan wat de oorzaak van het beveiligingsincident is, of hier persoonsgegevens mee gemoeid zijn en wat de impact hiervan is op de rechten van betrokkenen. Deze informatie is nodig om te bepalen of daadwerkelijk sprake is van een datalek en of gemeld moet worden aan de AP. Indien gemeld moet worden aan de AP moet ook worden

[2] Wanneer een (potentieel) datalek rechtstreeks wordt gemeld bij de Functionaris Gegevensbescherming (FG), meldt zij dit direct bij het SOCC zodat ook de op die manier binnengekomen (potentiele) datalekken op dezelfde wijze worden geregistreerd en afgehandeld.
[3] 'Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679', Artikel 29 Werkgroep (WP29). De WP29 is op 25 mei 2018 vervangen door de European Data Protection Board (EDPB) als orgaan waarin alle nationale privacytoezichthouders uit de Europese Unie samenwerken bij hun toezicht op de AVG.

bepaald of de betrokkene(n) moet(en) worden geïnformeerd. Ten slotte moet worden bepaald of, en zo ja welke, derde partijen moeten worden geïnformeerd.

Waar nodig worden de directeur (bedrijfsvoering) en / of de Privacy Champion van de betreffende faculteit of dienst en / of een privacy-jurist van BJZ bij het verzamelen van de feiten en het analyseren van het incident betrokken. Bij ernstige beveiligingsincidenten neemt de FG, de CISO of de directeur IT (als intern verantwoordelijke van het SOCC) in dit stadium al contact op met (de secretaris van) het College van Bestuur (CvB) en voor zover relevant met de directeur bedrijfsvoering van de betrokken faculteit(en) en/of directeur van de betrokken dienst(en). Afhankelijk van de ingeschatte ernst en impact van het incident worden ook anderen in dit stadium al geïnformeerd.

3.3 Besluit melding

Afhankelijk van de ingeschatte ernst van het incident wordt beslist of het datalek moet worden gemeld aan de AP en de betrokkenen. De FG adviseert het CvB over het al dan niet melden van een datalek aan de AP en de betrokkenen door per datalek een gemotiveerd advies uit te brengen. Op basis van dit advies neemt het CvB een besluit inzake het datalek.

Wanneer er instructies zijn van het CvB in welke vooraf vastgestelde, welbepaalde en duidelijk omschreven gevallen een datalek niet hoeft te worden gemeld, onder andere gebaseerd op voorgaande incidenten, zal dit worden gevolgd, zonder voorafgaande advisering door de FG. De FG informeert het CvB periodiek, in elk geval jaarlijks, over deze datalekken.

De datalekken evenals de afwegingen om een datalek al of niet te melden bij de AP en eventueel de betrokkenen worden gedocumenteerd in het datalekdossier. Dit is een wettelijke verplichting (artikel 33.5 AVG).

3.4 Melding datalek

Melding AP
Wanneer een melding bij de AP nodig is, wordt deze gedaan door de FG, zodat wordt geborgd dat de FG controle kan houden over de gemelde datalekken. De AVG vereist dat de melding aan de AP ten minste bevat:

a. de aard van het datalek, waar mogelijk onder vermelding van de categorieën van betrokkenen en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
b. de naam en de contactgegevens van de FG of een ander contactpunt waar meer informatie kan worden verkregen;
c. de waarschijnlijke gevolgen van het datalek;
d. de maatregelen die de VU heeft voorgesteld of genomen om het datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Het formulier meldplicht datalekken van de AP is leidend voor de melding bij de AP. Dit formulier is te vinden op de website van de AP.

De VU moet een datalek ‘zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur’ na kennisneming aan de AP melden (artikel 33.1 AVG). De termijn voor het melden van het datalek begint te lopen op het moment dat de VU kennis heeft genomen van een (potentieel) datalek. Het lukt niet altijd om binnen 72 duidelijk te krijgen wat er precies aan de hand is. In die situatie kan de VU een voorlopige

melding doen op basis van de gegevens die op dat moment beschikbaar zijn. Naderhand kan de melding worden aangevuld of ingetrokken.

Wanneer de melding niet binnen 72 uur plaatsvindt, moet de vertraging in de melding worden gemotiveerd. Uiteraard dient dit zoveel mogelijk te worden voorkomen.

Melding betrokkene(n)
Wanneer een melding aan de betrokkene(n) nodig is, wordt in samenspraak met de FG bepaald wie binnen de VU de betrokkene(n) informeert. De kennisgeving aan de betrokkenen bevat een omschrijving, in duidelijke en eenvoudige taal, van het datalek en ten minste de hierboven onder b, c en d genoemde informatie. De VU moet op basis van artikel 34.1 AVG het datalek 'onverwijld', dat wil zeggen zo snel als redelijkerwijs mogelijk, aan de betrokkenen melden.

Wanneer de inbreuk zich beperkt tot een verhoudingsgewijs klein aantal betrokkenen, kan de VU ervoor kiezen hen persoonlijk en gericht te benaderen. Wanneer de inbreuk een groot aantal betrokkenen treft, wordt de Dienst C&M (woordvoerder) geraadpleegd voor bredere mediacommunicatie. In het geval van een ernstige inbreuk wordt de wijze van kennisgeving afgestemd met het CvB.

Het is belangrijk om vast te leggen dat betrokkenen zijn geïnformeerd en met welke kennisgeving. Er mag geen discussie bestaan over het tijdstip waarop en met welke middelen en boodschap de betrokkenen zijn geïnformeerd.

Melding andere partijen
Wanneer andere partijen ook geraakt (kunnen) worden door het datalek, worden ook zij tijdig geïnformeerd over het datalek. In samenspraak met de FG wordt bekeken wie deze andere partijen informeert.

Voor datalekken binnen ACTA geldt dat deze worden gecoördineerd door de FG van ACTA. Hij zorgt ervoor dat de CvB's van de VU en UvA alsmede hun FG's tijdig en juist worden geïnformeerd.

In bepaalde situaties is het mogelijk dat de VU als verwerker optreedt voor een externe (samenwerkings)-organisatie. In die gevallen ligt de verantwoordelijkheid voor het melden van een datalek bij die externe (samenwerkings)organisatie. De VU heeft in die situatie wel de verplichting om een beveiligingsincident waarvan het waarschijnlijk is dat die de gegevensverwerking van de verwerkingsverantwoordelijke raakt, zo snel mogelijk te melden bij die verwerkingsverantwoordelijke. De VU zal in die situaties al het redelijke doen dat nodig is om ervoor te zorgen dat de verwerkingsverantwoordelijke aan zijn wettelijke verplichtingen kan voldoen.

4. Registratie en rapportage

De AVG vereist dat de VU alle inbreuken in verband met persoonsgegevens documenteert. Binnen de VU worden alle datalekken in elk geval gedocumenteerd in het informatie-incidentendossier van het SOCC.

Er wordt regelmatig aan het CvB en aan de RvT gerapporteerd over de datalekken die binnen de VU zijn afgehandeld. Deze rapportages dragen er onder andere aan bij dat trends kunnen worden gesignaleerd en dat waar nodig actie kan worden ondernomen.

***