Meldplicht Datalekken

Utrecht, 13 juni 2018
Versienummer: 4.0

Colofon

Meldplicht Datalekken

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

Auteurs
Project Moore in opdracht van SURF
Update uitgevoerd door SURF in juni 2018

Juni 2018

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inhoudsopgave

Dit document ‘Meldplicht Datalekken’ is een handreiking voor de instellingen die behoren tot de doelgroep van SURF. Het document bevat een stappenplan dat de instellingen kunnen gebruiken om compliant te worden met de wetgeving rond het melden van datalekken. Het stappenplan benadert het vraagstuk vanuit de optiek van integrale veiligheid en benadrukt daarom de taken en verantwoordelijkheden voor verschillende functionarissen binnen de organisaties van de doelgroep. Ter informatie is een korte vraagbaak opgenomen waarin SURF uitlegt wat de meldplicht inhoudt en waarin de antwoorden op de belangrijkste vragen over datalekken en de meldplicht zijn te vinden.

1. Inleiding

Geregeld lezen we in de media dat gegevens van werknemers, studenten of patiënten letterlijk op straat liggen; dossiers die worden aangeboden als oud papier, een gestolen smartphone of een verloren USB-stick. Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben spreken we van een datalek. Het risico op datalekken wordt steeds groter omdat onze persoonsgegevens in steeds meer databanken en/of op dragers zijn opgeslagen. Er zijn drie categorieën datalekken te onderscheiden:

- *Inbreuk op de vertrouwelijkheid*
  Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
- *Inbreuk op de integriteit*
  Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
- *Inbreuk op de beschikbaarheid*
  Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

In de Algemene Verordening Gegevensbescherming (AVG) is een meldplicht voor datalekken opgenomen in artikel 33 en 34. Deze meldplicht verplicht bedrijven om datalekken[1] te melden bij de toezichthouder, de Autoriteit Persoonsgegevens (AP) en, in sommige gevallen, ook bij de betrokkenen (de personen op wie de gegevens die zijn gelekt betrekking hebben). De Europese Werkgroep 29 heeft richtlijnen gepubliceerd omtrent deze meldplicht datalekken.[2] Deze richtlijnen zijn bedoeld om organisaties te helpen bij het bepalen of sprake is van een datalek en of er gemeld moet worden aan de AP en/of de betrokkenen. De richtlijnen zijn te vinden op de website van de AP.[3] De hiervoor geldende wetgeving, de Wet bescherming persoonsgegevens, kende ook een meldplicht die sterk leek hierop. Meer informatie over de meldplicht is te vinden op de website van de AP.[4]

Een datalek kan nadelige gevolgen hebben voor de persoonlijke levenssfeer van betrokkenen doordat de weggelekte gegevens oneigenlijk gebruikt kunnen worden. Identiteitsfraude is hiervan een voorbeeld maar ook kan gedacht worden aan ongewenste profilering of doorbreking van bewust gekozen anonimiteit. Om ernstige nadelige consequenties voor de bescherming van persoonsgegeven te beperken is de AVG 25 mei 2018 in werking getreden. Hoewel de meldplicht datalekken enkele kleine verschillen kent, blijft hij onder de AVG grotendeels hetzelfde. Wel kent de AVG bijvoorbeeld strengere regels omtrent de registratie van datalekken. De meldplicht draagt bij aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.
In de AVG is de verplichting voor de verwerkingsverwerkingsverantwoordelijke om datalekken te melden opgenomen. Hierdoor moeten onderwijs- en onderzoeksinstellingen een melding doen aan de AP van een datalek, wanneer het waarschijnlijk is dat deze een risico inhoudt voor de rechten en vrijheden van de betrokkenen.

[1] De AVG spreekt niet over een datalek, maar over een ‘inbreuk in verband met persoonsgegevens’: artikel 4 lid 12 AVG.
[2] Guidelines on Personal data breach notification under Regulation 2016/679.
[3] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/europese_guidelines_meldplicht_datalekken.pdf.
[4] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken.

Als een instelling hieraan niet voldoet riskeert zij een hoge boete die kan oplopen tot maximaal 10 miljoen euro of 2% van de totale wereldwijde omzet indien de meldplicht aan betrokkene en/of de AP niet wordt nagekomen (artikel 83 lid 4 AVG).

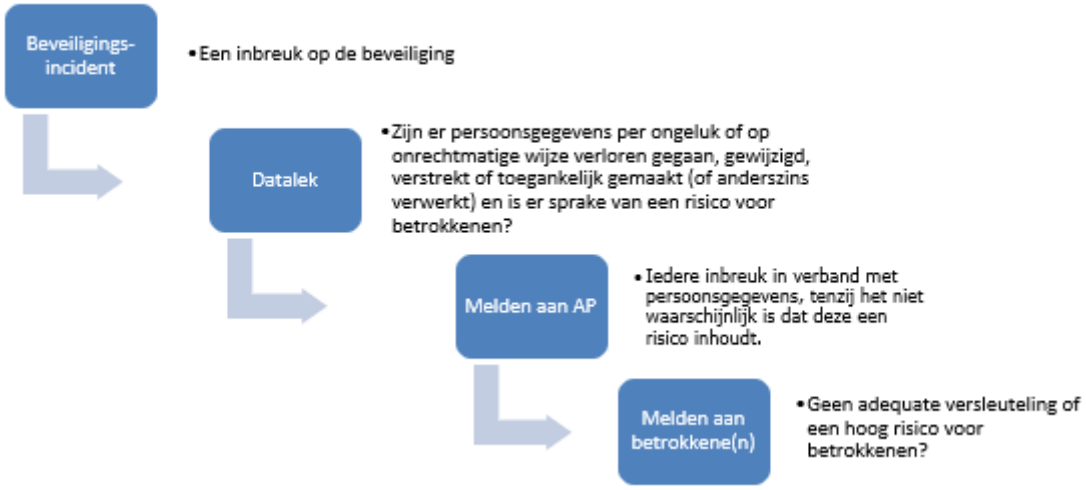
De meldplicht staat in nauw verband met de beveiligingsverplichting op basis waarvan zowel de verwerkingsverwerkingsverantwoordelijke als de verwerker passende technische en organisatorische maatregelen ten uitvoer moeten leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

Er is sprake van een geclausuleerde meldplicht: alleen die inbreuken die waarschijnlijk leiden tot een risico voor de rechten en vrijheden van de betrokkenen, moeten bij de AP worden gemeld. Door deze clausulering worden inbreuken met geringe nadelige gevolgen voor de bescherming van persoonsgegevens uitgezonderd van de meldplicht.

2. Het melden van een datalek

De AVG definieert een datalek als *'een inbreuk op de beveiliging die leidt tot aanzienlijke of onwettige vernietiging, verlies, wijziging, ongeautoriseerde openbaarmaking van of toegang tot, persoonlijke gegevens verzonden, opgeslagen of anderszins verwerkt'*. Niet elk datalek hoeft gemeld te worden aan de AP. Een onderwijs- of onderzoekinstelling hoeft de datalek niet te melden wanneer het onwaarschijnlijk is dat de inbreuk redelijkerwijs een risico voor betrokkenen met zich meebrengt. De meldplicht geldt voor de 'verwerkingsverantwoordelijke' zoals deze in de AVG is gedefinieerd. Omdat er sprake is van een hoge sanctie bij niet naleving van de meldplicht heeft dit een directe relatie met de governance van de instelling.

Zodra het datalek bekend is, moet de instelling beoordelen of het datalek gemeld moet worden bij de AP. De instelling moet hierbij een inschatting maken van de ernst van de risico's voor de bescherming van de persoonsgegevens. De instelling moet het datalek ook melden aan de betrokkenen (zoals studenten, (tijdelijke) werknemers van de instellingen, stagiaires, en/of patiënten) als de inbreuk op de verwerkte persoonsgegevens waarschijnlijk een hoog risico inhoudt voor hun rechten en vrijheden. De instelling zal bij een melding aan de AP moeten aangeven of zij van plan is om ook de betrokkenen van de inbreuk in kennis te stellen. De AP kan deze melding aan betrokkenen zo nodig afdwingen.
Om te inventariseren of iets een datalek is en of er gemeld moet worden, kan het onderstaande schema aangehouden worden. De stappen van dit schema worden hieronder verder toegelicht.



1) <u>Is er sprake van een inbreuk op de beveiliging (een datalek)?</u>

Om te kunnen spreken van een datalek moet er sprake zijn van persoonsgegevens die zijn 1) vernietigd of verloren, 2) gewijzigd, 3) verstrekt of 4) toegankelijk gemaakt, alles op een onrechtmatige manier.

Bij de beantwoording van deze eerste vraag moet niet alleen gedacht worden aan actieve handelingen om de beveiliging te doorbreken zoals hacken van bestanden maar moet ook diefstal of verlies van dragers waarop persoonsgegevens zijn opgeslagen worden meegenomen.

2) Moet er worden gemeld aan de AP?

Een melding aan de AP moet alleen gebeuren wanneer het datalek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokkenen. Volgens de AVG moet hier zowel naar de *waarschijnlijkheid* als de *ernst* van de risico's voor de rechten en vrijheden van betrokkenen worden gekeken. Voor de inschatting van het risico moet een objectieve beoordeling worden gemaakt.
De volgende aspecten moeten worden meegewogen in de beoordeling van het risico voor de rechten en vrijheden van betrokkenen:

- *Het soort datalek*
  Een datalek waarbij derde partijen toegang hebben gekregen tot medische gegevens, zal wellicht andere gevolgen hebben voor een betrokkene dan een datalek waarbij medische gegevens per ongeluk zijn vernietigd en niet langer beschikbaar zijn.

- *De aard, gevoeligheid en omvang van de persoonsgegevens*
  Doorgaans zal gelden, hoe gevoeliger de gegevens, hoe groter het risico voor de rechten en vrijheden van de betrokkenen. Hier zal echter ook aandacht moeten worden besteed aan eventuele andere gegevens die al bekend zijn van de betrokkene, waar deze gelekte gegevens mee gecombineerd kunnen worden. Een combinatie van gegevens zal vaak gevoeliger zijn dan één enkel gegeven van een betrokkene. Er zal daarom altijd rekening moeten worden gehouden met de omstandigheden van het geval.

- *De inspanningen voor identificatie van de betrokkenen*
  Afhankelijk van de omstandigheden van het geval, zal identificatie op twee manieren kunnen plaatsvinden. Identificatie is direct mogelijk op basis van de gelekte gegevens. Daarnaast is indirecte identificatie ook een mogelijkheid, waarbij het zeer lastig zal zijn om de gelekte data een aan natuurlijk persoon te koppelen, maar via een omweg toch mogelijk.

  Onder bepaalde omstandigheden mag er worden afgezien van een melding aan de AP, als de persoonsgegevens waarover het gaat goed zijn versleuteld, waardoor identificatie niet meer mogelijk is. WP29 spreekt hier over het criterium 'appropriate level of encryption'. De instelling is verantwoordelijk voor de beoordeling of voldaan is aan dit criterium.

- *De ernst van de gevolgen voor de betrokkenen*
  De ernst van de gevolgen voor de betrokkenen kan afhankelijk zijn van meerdere factoren, waaronder 1) de aard van de data; 2) de categorieën betrokkenen; 3) de relatie met de derde partij die toegang heeft gekregen tot de data, en 4) de duur van de gevolgen voor de betrokkenen, waarbij geldt dat hoe langer de gevolgen, hoe groter de impact voor de betrokkenen.

- *Speciale kenmerken van de verwerkingsverwerkingsverantwoordelijke*
  De aard en rol van de verwerkingsverwerkingsverantwoordelijke kan het risico voor de betrokkenen beinvloeden. Een medische organisatie verwerkt bijzondere persoonsgegevens, en dit zal een groter risico inhouden voor betrokkenen dan bijvoorbeeld e-mailadressen of een krant.

- *Het aantal betrokkenen*
  In het algemeen geldt, hoe groter het aantal betrokkenen, hoe groter de gevolgen van de inbreuk zullen zijn. Dit is echter altijd afhankelijk van de omstandigheden van het geval. Gelekte medische gegevens zullen een groot risico betekenen voor één betrokkene.

- *Algemene punten*

De verwerkingsverwerkingsverantwoordelijke zal een inschatting moeten maken van de ernst van de eventuele gevolgen voor de betrokkenen en de waarschijnlijkheid dat deze gevolgen plaatsvinden. Er zal altijd rekening moeten worden gehouden met de omstandigheden van het geval.

Als termijn geldt dat de verwerkingsverantwoordelijke het datalek moet melden aan de AP, uiterlijk 72 uur nadat hij er kennis van heeft genomen. Hier geldt dat de verwerkingsverantwoordelijke een korte termijn mag nemen om te onderzoeken of er inderdaad sprake is van een datalek, voordat deze 72 uur begint te lopen. Dit 'vooronderzoek' dient wel zo snel mogelijk te beginnen en afgerond te worden.

3) Moet er worden gemeld aan de betrokkenen?

Een datalek hoeft alleen aan de betrokkenen te worden gemeld, wanneer het waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van de betrokkenen. Hierbij zal onder andere moeten worden gekeken of het datalek kan leiden tot fysieke, materiele of immateriële schade voor de betrokkenen. Hierbij kan worden gedacht aan discriminatie, (identiteits-)fraude, financiële schade en reputatieschade.
Een melding aan de betrokken is in de volgende drie gevallen niet nodig:

- Er zijn voordat het datalek plaatsvond, passende maatregelen getroffen, waardoor de gelekte persoonsgegevens onbegrijpelijk zijn voor onbevoegden. Bijvoorbeeld doordat de betreffende gegevens goed zijn versleuteld of vervangen door een hashwaarde. Deze uitzondering geldt alleen maar als: 1) de gegevens nog volledig intact zijn; 2) de instelling nog steeds de volledige controle over de gegevens heeft; 3) de sleutel die voor de encryptie of voor de hashing is gebruikt bij de inbreuk geen gevaar heeft gelopen en voor onbevoegden met de beschikbare technologische middelen niet te vinden is.

- Er zijn, onmiddellijk nadat het datalek heeft plaatsgevonden, maatregelen getroffen waardoor het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen. Bijvoorbeeld wanneer de gelekte persoonsgegevens onmiddellijk na het datalek op afstand zijn gewist, nog voordat de onbevoegde ontvanger iets met de gegevens kon doen.

- Een melding is niet nodig wanneer dat noodzakelijk en evenredig is ter waarborging van: a) de nationale veiligheid; b) landsverdediging; c) de openbare veiligheid; d) de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Wanneer het individueel informeren van de betrokkenen een onevenredige inspanning vergt, mogen de betrokkenen worden geïnformeerd door middel van een openbare mededeling of soortgelijke maatregel, waarbij betrokkenen even doeltreffend worden geïnformeerd.
Ook is de verwerkingsverantwoordelijke verplicht alle datalekken te documenteren, dus ook degene die niet ernstig genoeg waren om te melden aan de AP. Dit overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, de gevolgen van de inbreuk en de genomen corrigerende maatregelen.

Verder rust op de onderwijsinstelling de verplichting om in de contracten met (IT-)leveranciers een vergelijkbare meldplicht op te nemen, die erop neerkomt dat deze leveranciers de instelling informeren indien sprake is van een datalek. Het Juridische Normenkader Cloudservices voor het hoger onderwijs in Nederland en de bijbehorende model verwerkersovereenkomst geven voorbeelden van bepalingen die hiervoor gebruikt kunnen worden[5].

[5] Juridische Normenkader Cloudservices Hoger Onderwijs
https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html.

3. Stappenplan meldplicht datalekken

De onderwijsinstelling kan zich als volgt voorbereiden op de meldplicht datalekken:

- Inventariseer waar in de onderwijs- en onderzoeksorganisatie welke gegevens worden verwerkt. Oftewel, breng de datastromen van de organisatie in kaart. Let daarbij op gevoelige gegevens die worden verwerkt zoals bijvoorbeeld medische en etnische gegevens van studenten en medewerkers. Denk ook aan de gegevens die in het kader van wetenschappelijk onderzoek worden verwerkt.

- Neem de huidige beveiligingsmaatregelen onder de loep. Inventariseer de mogelijke risico's van verlies van gegevens en pas waar nodig het beveiligingsbeleid aan. Basis voor deze risicoanalyse kan het SURFnet model Privacy Impact Assessment[6] of de Hoger Onderwijs Referentie Architectuur (HORA) zijn waar al in staat aangegeven welke gegevensentiteiten vertrouwelijke gegevens bevatten.

- Opstellen duidelijke interne procedure (actieplan). Zorg voor een procedure waaruit duidelijk blijkt wie de verwerkingsverantwoordelijke is en welke afdeling/functionaris betrokken moet worden indien een datalek wordt geconstateerd. Denk hierbij aan het bestuur of hun gemandateerde eigenaar van de gegevens, de functionaris gegevensbescherming, de veiligheidsfunctionaris, de juridische afdeling en niet te vergeten de afdeling communicatie. Beschrijf hierbij de rollen en taken van deze afdelingen/functionarissen en sluit hierbij aan op bestaande processen binnen de instelling. Zo zou bijvoorbeeld de melding van een datalek overeen kunnen komen met de afhandeling van meldingen in het kader van Computer Security Incident Response Teams (CSIRT). In de procedure moet in ieder geval worden geregeld aan wie een datalek intern wordt gemeld, welke maatregelen door wie binnen welke termijnen moeten worden genomen en hoe het datalek naar buiten toe wordt gecommuniceerd. Indien er een functionaris gegevensbescherming aanwezig is moet deze in ieder geval in kennis gesteld worden. Een communicatieplan voor het naar buiten brengen van de melding zal hier ook deel van uitmaken. Denk er verder over na of het datalek gemeld moet worden bij de verzekering en of er een advocaat ingeschakeld moet worden. Zorg ook voor voldoende interne training met betrekking tot deze procedure.

- Zorg voor een strikt beleid met betrekking tot het verwerken van persoonsgegevens. Hiervoor kunt u gebruik maken van het SURFnet model privacy beleid[7]. Stel richtlijnen op voor het opslaan van persoonsgegevens door werknemers/studenten op draagbare apparatuur. Het opstellen van een protocol inclusief een procedure voor melding aan de AP en betrokkenen kan hier eveneens deel van uitmaken.

- Inventariseer de contracten met de Verwerkers en zorg dat die waar nodig worden aangepast. Neem de verplichting op dat de Verwerker onverwijld een melding aan de organisatie moet doen als er bij hem een datalek heeft plaatsgevonden. Vraag aan de Verwerker een beschrijving van

[6] Model privacy impact assessment en PIA risico formulier, https://www.surf.nl/themas/beveiliging/beleidsondersteuning-privacy/algemene-verordening-gegevensbescherming-avg/impact-en-riskassessment/index.html.
[7] Model Beleid Verwerking Persoonsgegevens, versie maart 2018, https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2018/201803-model-beleid-verwerking-persoonsgegevens.pdf.

de gevolgen van de inbreuk en de maatregelen om de gevolgen te verhelpen. Spreek duidelijk met de Verwerker af wie bepaalt of een datalek wel of niet meldingsplichtig is (bij voorkeur de instelling). Maak ook duidelijk welke datalekken gemeld moeten worden (dit zijn bij voorkeur alle incidenten en niet alleen de meldingsplichtige beveiligingsincidenten). Regel daarnaast hoe wordt omgegaan met eventuele boetes die als gevolg van een datalek bij de Verwerker aan de organisatie worden opgelegd. Stel van te voren vast hoe omgegaan wordt met een keten van verwerkers, sub-verwerkers en sub-subverwerkers. Wees duidelijk over de geschillenprocedure hiervoor.

- Overweeg toereikende encryptie waardoor melding aan de AP en de betrokkenen in sommige gevallen achterwege gelaten kan worden.

4. Veel gestelde vragen

Moet de onderwijsorganisatie straks elk datalek gaan registreren?
Ja, sinds 25 mei 2018 dient u intern alle datalekken te registreren, ook als het om kleine kwesties gaat. In dit opzicht is de AVG strenger dan de daarvoor geldende Wbp. Belangrijk is het onderscheid tussen de registratie en de meldplicht. Het betreft hier een interne registratie, wat betekent dat een registratie niet gemeld hoeft te worden bij de AP en/of betrokkene

Moet de onderwijsorganisatie straks elk datalek gaan melden? Ook als een medewerker bijvoorbeeld een telefoon of usb-stick verliest?
Nee, een datalek hoeft alleen gemeld te worden als het datalek waarschijn een risico oplevert voor de rechten en vrijheden van de betrokkenen. Denk hierbij aan identiteitsfraude of reputatieschade.
De Werkgroep 29 heeft richtlijnen gepubliceerd die kunnen helpen om te bepalen of sprake is van een risico.

Hoe dient de melding eruit te zien?
Een melding moet worden gedaan bij de toezichthouder, de AP. Dit kan door middel van het invullen van een formulier op de website.[8] Of in sommige gevallen telefonisch of per fax.
Van ieder datalek dient in ieder geval de volgende informatie te worden bijgehouden:

- Een korte omschrijving van het lek;
- Wanneer het lek plaatsvond;
- Wat er met de gegevens is gebeurd (zijn ze verloren gegaan, of door een onbevoegde ingezien, gekopieerd of gewijzigd?);
- Van welke groep(en) personen er gegevens gelekt, en om hoeveel personen gaat het;
- Om welke soorten gegevens het gaat;
- De (mogelijke) gevolgen van de inbreuk (bijvoorbeeld een risico op identiteitsfraude of reputatieschade);
- De maatregelen die zijn genomen naar aanleiding van het lek;
- Welke actie is ondernomen om schade te voorkomen of zo veel mogelijk te beperken;
- Wat heeft u gedaan om te zorgen dat het niet nog een keer kan gebeuren?

Moet de instelling een datalek ook melden aan de betrokkenen?
Als een datalek een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene, dan moet dit ook aan de betrokkenen worden gemeld. Het informeren aan de betrokkenen kan onder meer achterwege worden gelaten als de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, tenzij de AP alsnog beveelt om een melding aan de betrokkenen te doen. De melding aan de betrokkene moet op een zodanige wijze gebeuren dat deze op een behoorlijke en zorgvuldige wijze wordt geïnformeerd.

Wanneer moet de organisatie een boete betalen? En hoe hoog zal deze boete zijn?
De AP kan handhavend optreden als niet aan de verplichtingen met betrekking tot de meldplicht datalekken wordt voldaan. Er gelden geen vaste boetebedragen; de AP is vrij te bepalen óf en welk boetebedrag zij in een gegeven geval wenselijk acht. Onder de AVG kan een boete worden opgelegd van maximaal 10 miljoen euro of 2% van de totale wereldwijde omzet indien de meldplicht aan betrokkene en/of de AP niet wordt nagekomen.[9] Boetes kunnen direct opgelegd worden.

Welke afspraken moet ik maken met mijn leveranciers?
Met betrekking tot de contracten met de leveranciers geldt de verplichting dat de leverancier een melding aan de onderwijsorganisatie doet, als er bij hem een datalek heeft plaatsgevonden met persoonsgegevens waarvoor de onderwijsorganisatie verantwoordelijk is.

[8] https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.
[9] Het maximale bedrag is voor de andere categorie overtredingen hoger. Zie artikel 83 lid 5 AVG.

Daarnaast is het raadzaam afspraken te maken over hoe partijen omgaan met eventuele boetes die als gevolg van een datalek bij de leverancier aan de onderwijsorganisatie worden opgelegd.

Wat betekent de meldplicht datalekken voor de beveiliging?
De meldplicht staat in nauw verband met de beveiligingsverplichting, op basis waarvan zowel de verwerkingsverwerkingsverantwoordelijke als de verwerker passende technische en organisatorische maatregelen ten uitvoer moeten leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.

Wat doet de Autoriteit Persoonsgegevens met de melding?
De AP slaat de melding op in een register met alle ontvangen meldingen over datalekken. Dit register is niet openbaar. Daarnaast kan de AP contact opnemen over de melding, om te controleren of de melding daadwerkelijk van de instelling afkomstig is eventueel inhoudelijke vragen over de melding. Ook zou de AP kunnen vragen om alsnog betrokkenen te informeren over het datalek. Ten slotte kan de melding, eventueel in combinatie met ander meldingen, aanleiding zijn voor de AP om een onderzoek te starten naar de naleving van de privacywetgeving.

Valt het verlies van een papieren dossier onder de reikwijdte van de meldplicht?
Ja, het verlies van een papieren dossier valt ook onder de meldplicht indien er sprake is van inbreuk op de beveiliging waarvan redelijkerwijs kan worden aangenomen dat dit een risico vormt voor de rechten en vrijheden van de betrokkenen.

Valt bewust lekken van een medewerker onder de meldplicht?
Ja, als er redelijkerwijs kan worden aangenomen dat dit leidt tot een risico voor de privacy van de betrokkenen.

Kan de betrokkene zelf ook melden?
Nee, de meldingsplicht rust op de verwerkingsverantwoordelijke; het is de instelling die de AP onverwijld in kennis moet stellen van een datalek.

Zijn er formulieren voor de melding?
Ja er is een webformulier beschikbaar op de website van de AP.

Krijg je altijd de maximum boete als je niet meldt?
Nee, dat kan afhangen van verschillende factoren en is afhankelijk van de omstandigheden van het geval. Een omstandigheid van het geval kan bestaan uit het feit dat de gegevens waarover het gaat niet door derden zijn ingezien.

Hoe zit het met versleutelde gegevens?
Als de instelling passende technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn hoeft de instelling de inbreuk niet te melden aan de AP of de betrokkenen. De registratieplicht blijft wel gelden.

Wat moet een instelling doen als deze de betrokkenen wil informeren maar deze niet weet wie precies betrokkenen zijn of hoe deze te bereiken zijn?
Dit is afhankelijk van de situatie maar een instelling zou bijvoorbeeld via berichten in de media aan betrokkenen kunnen laten weten dat er sprake is geweest van een datalek. Het is aan te raden dit in overleg met de afdeling communicatie te doen.

Moet een instelling de betrokkenen ook laten weten wat ze het beste kunnen doen om de schade te beperken?
De instelling moet betrokkenen verschillende zaken laten weten: de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

Wat zijn passende maatregelen in het geval van een datalek?
In geval van een datalek moet de instelling haar interne procedures volgen, het actieplan uitvoeren en het datalek dichten. Hiertoe moet de instelling de omvang van het datalek en de benodigde maatregelen inventariseren. Alle acties en beslissingen moeten gedocumenteerd worden.