De meldplicht datalekken in het onderwijs

De meldplicht datalekken rust op de verantwoordelijke in de zin van de Wbp. Dat is degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1 Wbp). De onderwijsinstelling is de verantwoordelijke voor de verwerking van de persoonsgegevens van haar leerlingen en werknemers. Dit artikel heeft betrekking op het lekken van leerlinggegevens. Dit zijn in Wbp-termen veelal 'gevoelige' of, wanneer ze iets zeggen over iemands gezondheid, ras, godsdienst of levensovertuiging, zelfs 'bijzondere' persoonsgegevens. Informatiebeveiliging en de meldplicht datalekken verdienen daarom een hoge plek op de agenda van onderwijsinstellingen.

Nicole Niessen en Floor de Roos*

1. Inleiding

Vrijdagavond 15 juli 2016 om 19.58 uur verschijnt op nu.nl het bericht "Gegevens scholieren mogelijk op straat na hack".[1]

Door een inbraak in de centrale database Edu-IX van verschillende digitale leersystemen, zijn mogelijk de persoonsgegevens van duizenden middelbare scholieren op straat komen te liggen. Naam, adres, woonplaats, geboortedatum, e-mailadres en wachtwoorden van accounts zijn mogelijk ontvreemd, zo stelt de nieuwssite in navolging van de VO-raad. Wat de consequenties van de hack zijn is dan nog niet duidelijk. De distributeurs van deze leermiddelen hebben de hack gemeld bij de Autoriteit Persoonsgegevens (AP) en de scholen, die daarop hun leerlingen hebben ingelicht. Ook zijn bestaande wachtwoorden onbruikbaar gemaakt om het lek te dichten.[2]

De Wet bescherming persoonsgegevens (Wbp) kent sinds 1 januari 2016 een meldplicht datalekken (artikel 34a Wbp). Deze wetswijziging loopt vooruit op de Europese Privacyverordening die vanaf 25 mei 2018 van kracht zal zijn.[3] De meldplicht datalekken houdt in dat organisaties in geval van een 'ernstig' datalek verplicht zijn een melding te doen bij de toezichthoudende instantie, de AP. Een 'ernstig' datalek is een inbreuk op de beveiliging met (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. In sommige gevallen moet het datalek ook worden gemeld aan de betrokken personen. Het lijkt erop dat na de hack bij Edu-IX volgens het Wbp-spoorboekje is gehandeld.

Een datalek is helaas geen zeldzaamheid. Dagelijks zijn er nieuwsberichten over ernstige datalekken in uiteenlopende sectoren, ook in het onderwijs. Door digitalisering van leermiddelen en leerlingvolgsystemen alsmede door toenemende samenwerking tussen onderwijs en ketenpartners ('1 kind 1 plan'), is het risico (eerder) aanwezig dat leerlinggegevens in verkeerde handen komen. De meldplicht datalekken maakt de verplichting tot informatiebeveiliging niet anders, maar vergroot wel de alertheid op het voorkomen van een datalek.

2. Beveiligingsplicht persoonsgegevens

De meldplicht datalekken vloeit voort uit de beveiligingsverplichting van de verantwoordelijke. De hack bij Edu-IX was een gerichte aanval. In veel gevallen komt een datalek onbedoeld aan het licht.

Op grond van artikel 13 Wbp is de verantwoordelijke (hier: de onderwijsinstelling) verplicht passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Dit houdt in dat de onderwijsinstelling een adequaat informatiebeveiligingsniveau moet hanteren. Wat passend is, is niet in zijn algemeenheid te zeggen en hangt af van de concrete situatie. De volgende factoren zijn onder meer van belang: de stand van de techniek (welke maatregelen zijn mogelijk en proportioneel gelet op de stand van de techniek), de gevoeligheid van de persoonsgegevens, de context waarin de gegevens worden gebruikt, de kosten van de maatregelen, enzovoort.

De beveiligingsverplichting geldt voor alle bestanden, hardcopy en digitaal, waarin de onderwijsinstelling de persoonsgegevens van leerlingen verwerkt. Dat kan zijn een gecentraliseerd bestand (administratie bestuursbureau), maar het bestand kan ook functioneel (groep, zorg- en adviesteams) of geografisch (scholen) verspreid zijn. Vaak zijn er koppelingen tussen (deel)bestanden. Hoewel de aandacht uitgaat naar de risico's van digitale verwerkingen, kan een datalek

* Nicole Niessen en Floor de Roos zijn werkzaam bij Boels Zanders Advocaten waar zij leiding geven aan het team Onderwijs respectievelijk het team Privacy

ook offline plaatsvinden, bijvoorbeeld als een leerlingdossier per ongeluk bij het oud papier wordt gezet. Bij digitale verwerkingen is de omvang van het datalek echter al gauw vele malen groter.

3. Digitale leermiddelen

Met de opkomst van digitale leermiddelen staat de uitwisseling van leerlinggegevens tussen de onderwijsinstelling en de leverancier (doorgaans een educatieve uitgever) volop in de belangstelling. Daarbij geldt in Wbp-termen de onderwijsinstelling als de verantwoordelijke voor de verwerking van leerlinggegevens en de leverancier als de bewerker.[4] De bewerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. De verantwoordelijke is verplicht de afspraken met de bewerker vast te leggen in een bewerkersovereenkomst (artikel 14 lid 2 Wbp). Over de *Model bewerkersovereenkomst digitale onderwijsmiddelen* (hierna: Model Bewerkersovereenkomst), versie 2015, hebben Hoen en Van Lammeren in School en Wet van februari dit jaar geschreven.[5] De directe aanleiding voor de Model Bewerkersovereenkomst is de Snappet-kwestie geweest.

Snappet is een digitaal leermiddel dat op veel basisscholen wordt gebruikt. Het bleek dat de leverancier verkregen leerresultaten niet alleen bewerkte voor de school die de opdracht had verstrekt, maar deze tevens gebruikte voor de verdere ontwikkeling van het onderwijsmateriaal zonder dat de school ervan wist. Dit is een 'ernstig' datalek, zij het dat destijds de meldplicht datalekken nog niet gold. De AP heeft Snappet hierover op de vingers getikt, omdat leerresultaten gevoelige persoonsgegevens zijn waaraan bovendien conclusies worden verbonden voor het latere maatschappelijke leven. Het is volgens de AP belangrijk dat scholen zeggenschap houden over de gegevens van hun leerlingen en weten wat daarmee gebeurt. Zij moeten weloverwogen keuzes maken voor specifieke gegevensverwerkingen, zodat zij ouders daarover kunnen informeren. Voor sommige verwerkingen is zelfs de toestemming van ouders vereist. Inmiddels heeft Snappet haar werkwijze en de informatievoorziening aan scholen aangepast.

> De nieuwe Model Bewerkersovereenkomst verplicht de onderwijsinstelling om in geval van een datalek te voldoen aan *'eventuele wettelijke meldingsplichten'*. Verder ziet de Versie 2.0 niet alleen op het gebruik van leermiddelen en toetsen maar ook op school- en leerlinginformatiemiddelen.

De Model Bewerkersovereenkomst van 2015 waarover Hoen en Van Lammeren in School en Wet van februari 2016 schreven[6], heeft in juni 2016 een opvolger gekregen: de Model Bewerkersovereenkomst Versie 2.0.[7] Een van de nieuwe onderdelen betreft de meldplicht datalekken. Artikel 8 lid 4 van de nieuwe Model Bewerkersovereenkomst verplicht de onderwijsinstelling om in geval van een datalek te voldoen aan *'eventuele wettelijke meldingsplichten'*. Verder ziet de Versie 2.0 niet alleen op het gebruik van leermiddelen en toetsen maar ook op school- en leerlinginformatiemiddelen. Daarbij moet worden gedacht aan een digitaal leerlingadministratiesysteem, roostersysteem, ouderportaal, leerling- en oudersysteem, een elektronische leeromgeving en een leerlingvolgsysteem.[8]

De Snappet-kwestie heeft niet alleen geleid tot het maken van een Model Bewerkersovereenkomst, maar ook (mede) geleid tot het concept wetsvoorstel, op 16 mei 2016 ter internetconsultatie aangeboden, tot wijziging van de sectorwetten voor het funderend en middelbaar beroepsonderwijs in verband met het pseudonimiseren van leerling- of deelnemergegevens ten behoeve van de toegang tot en het gebruik van digitale leermiddelen.[9] Een pseudoniem is een unieke identiteit voor leerlingen die door elke leverancier kan worden gebruikt, zonder dat direct te herleiden is om welke specifieke leerling het gaat. Het concept wetsvoorstel gaat uit van één pseudoniem per leerling voor verschillende toepassingen van de onderwijsinstelling en haar leveranciers.

Daarbij weet alleen de onderwijsinstelling om welke leerling het gaat en niet de uitgever. Het risico van een koppeling tussen het pseudoniem en de betreffende leerling wordt daarmee geminimaliseerd, maar niet volledig weggenomen. Bij anonimisering van leerlinggegevens is die koppeling uitgesloten, maar het nadeel hiervan zou zijn dat leervorderingen niet kunnen worden bijgehouden. Het volgen van de leerling heeft immers voor zowel de leerling, de onderwijsinstelling als de leverancier belangrijke voordelen. Daarbij moet worden gedacht aan gerichte interventies om de leerling te ondersteunen en/of de verbetering van digitale leermaterialen. Met de keuze voor een pseudoniem blijft er dus sprake van een persoonsgegeven en geldt onverkort de Wbp, inclusief de meldplicht datalekken.

4. Wat is een datalek?

Ingevolge de wet kan een datalek aan de orde zijn, wanneer sprake is van een 'inbreuk op de beveiliging, bedoeld in artikel 13 Wbp'. Er moet zich daadwerkelijk een beveiligingsincident hebben voorgedaan, bijvoorbeeld verlies van een USB-stick, diefstal of verlies van een laptop of mobiele telefoon, inbraak door een hacker, ongeautoriseerde toegang tot gegevens, etcetera. De toegang tot een bestand met leerlinggegevens is doelgebonden en mag niet vrij toegankelijk zijn voor alle werknemers. Daarover dienen binnen de onderwijsinstelling specifieke afspraken te worden gemaakt die in protocollen worden vastgelegd.

Van ongeautoriseerde toegang is ook sprake indien derden kennis kunnen nemen van foto's en video's van leerlingen, terwijl de betrokkenen daarvoor geen toestemming hebben gegeven. De verspreiding van deze beelden door c.q. vanuit een computer van de onderwijsinstelling kan ongewenst en zelfs schadelijk zijn. De privacy van een leerling vereist dat voor de verspreiding van beeldmateriaal eerst uitdrukkelijk om toestemming moet worden gevraagd. Hierbij moet de onderwijsinstelling rekening houden met de leeftijd van een leerling. Als leerlingen 16 jaar of ouder zijn, dienen zijzelf op grond van artikel 5 Wbp toestemming te geven, voor leerlingen jonger dan 16 jaar is de toestemming van de wettelijk vertegenwoordiger vereist.

Kenmerkend voor een inbreuk op de beveiliging is verder dat het beveiligingsincident daadwerkelijk gevolgen heeft voor de persoonsgegevens die de onderwijsinstelling verwerkt. Dat is het geval wanneer i) persoonsgegevens verloren zijn gegaan of ii) niet redelijkerwijs is uit te sluiten dat er persoonsgegevens onrechtmatig zijn

verwerkt. Van verlies is sprake als de onderwijsinstelling de gegevens niet meer heeft en ook niet beschikt over een (volledige) back-up. Onder onrechtmatige verwerking vallen de aantasting van de persoonsgegevens en onbevoegde kennisneming, wijziging of verstrekking daarvan.

Op 7 maart 2016 kwam in het nieuws dat de Hogeschool Van Hall Larenstein in Leeuwarden en Velp per ongeluk het woonadres, telefoonnummer, e-mailadres en het BSN van haar 4.400 studenten had rondgemaild. Het volledige studentenbestand was abusievelijk als bijlage aan de mail gehecht die de studenten, ieder individueel, van de hogeschool ontvingen.[10] Op 20 juni 2016 werd bericht dat studentgegevens van de Universiteit van Amsterdam en de Hogeschool van Amsterdam makkelijk vindbaar zijn door een systeemlek. Student Nelson Berg kon daardoor bij de gegevens van honderdduizenden studenten, waaronder hun namen, telefoonnummers en foto's. Het lek zou daags erna zijn gedicht.[11]

Na de invoering van de meldplicht datalekken op 1 januari 2016 leken datarampen zich tot 15 juli 2016 vooral voor te doen in het hoger onderwijs. Dat ook het funderend onderwijs er niet aan ontkomt, toont de hack op Edu-XI.

5. Ernstige nadelige gevolgen

Niet iedere inbreuk op de beveiliging (datalek) hoeft te worden gemeld bij de toezichthouder (de AP). Alleen datalekken met (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens – zogenaamde 'ernstige' datalekken – moeten worden gemeld. De onderwijsinstelling zal zelf moeten bepalen of daarvan sprake is.

Indien persoonsgegevens van gevoelige aard zijn gelekt, is in ieder geval sprake van een 'ernstig' datalek. De specifiek in artikel 16 Wbp benoemde bijzondere persoonsgegevens – zoals gegevens betreffende iemands gezondheid, ras, godsdienst of levensovertuiging – zijn per definitie gevoelige persoonsgegevens. Maar ook gegevens over prestaties op school worden beschouwd als gevoelig, omdat deze kunnen leiden tot stigmatisering of uitsluiting van de betreffende personen. Zo kan dus de enkele inschrijving van een leerling op een bepaalde school een gevoelig persoonsgegeven zijn. Verder vallen gebruikersnamen, wachtwoorden en andere inloggegevens in deze categorie.

Niet iedere inbreuk op de beveiliging (datalek) hoeft te worden gemeld bij de toezichthouder (de AP). Alleen datalekken met (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens – zogenaamde 'ernstige' datalekken – moeten worden gemeld. De onderwijsinstelling zal zelf moeten bepalen of daarvan sprake is.

Daarnaast is sprake van een 'ernstig' datalek als de aard en omvang van het lek leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen. In dit verband is onder meer relevant of er veel persoonsgegevens zijn gelekt en hoe groot de (potentiële) impact van het verlies of de onrechtmatige verwerking is. Gelet op de gevoelige, bijzondere aard van leerlinggegevens zal een datalek al gauw als ernstig worden aangemerkt in welk geval een onderwijsinstelling het datalek zal moeten melden.

6. Wanneer en aan wie melden?

Een ernstig datalek moet op grond van artikel 34a lid 1 Wbp 'onverwijld' door de onderwijsinstelling *bij de toezichthouder* (AP) worden gemeld. De AP heeft in haar beleidsregels[12] aangegeven dat de melding zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek, moet plaatsvinden. Er is dus enige, maar niet al te veel, tijd voor nader onderzoek. Een melding kan naderhand nog worden aangevuld of ingetrokken, indien nader onderzoek daartoe aanleiding geeft. Melding van een datalek bij de AP kan plaatsvinden via het meldloket datalekken op de website van de AP.[13]

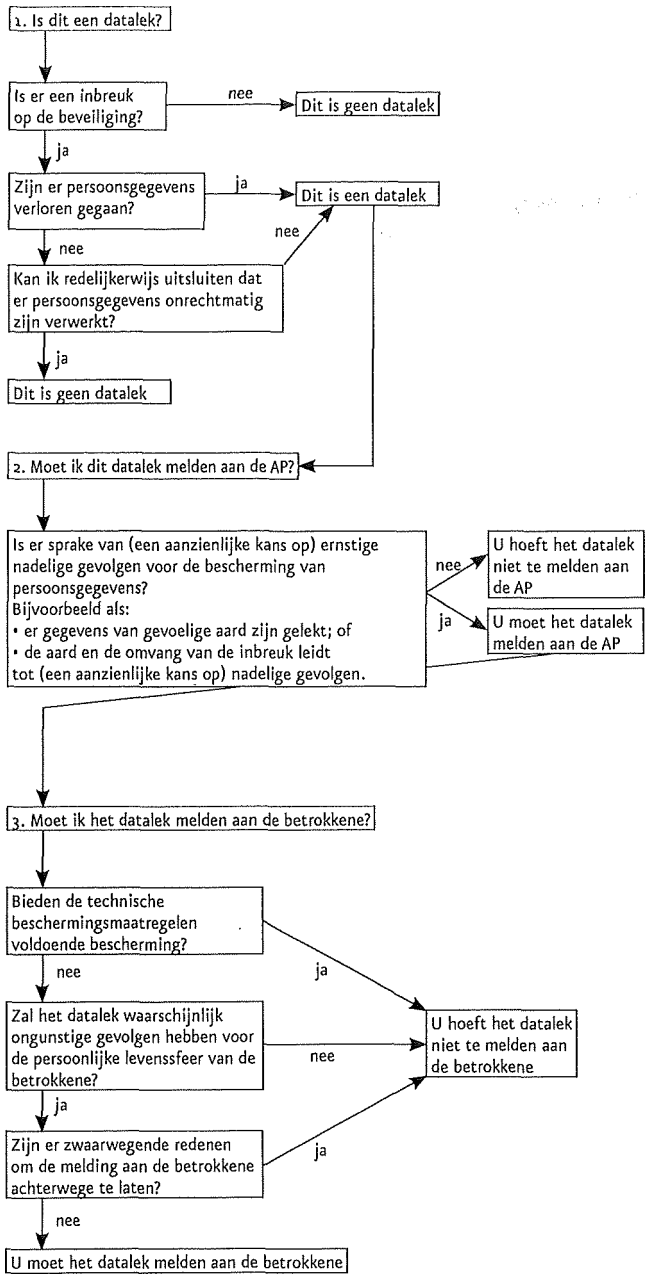
Een ernstig datalek moet op grond van artikel 34a lid 1 Wbp 'onverwijld' door de onderwijsinstelling bij *de toezichthouder* (AP) worden gemeld. De AP heeft in haar beleidsregels[12] aangegeven dat de melding zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking van het datalek, moet plaatsvinden.

Indien de getroffen technische beschermingsmaatregelen onvoldoende bescherming bieden en het datalek waarschijnlijk ongunstige gevolgen heeft voor *de personen over wier gegevens het gaat* (de 'betrokkene'), dan is de onderwijsinstelling bovendien verplicht om de betrokkenen van het lek op de hoogte te stellen. Dat is in beginsel het geval wanneer persoonsgegevens van gevoelige aard zijn gelekt. In alle andere gevallen moet de onderwijsinstelling op basis van de omstandigheden van het geval een afweging maken. De kennisgeving aan de betrokkenen omvat in ieder geval de aard van de inbreuk (het datalek), de instanties waar meer informatie over het lek kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van het lek te beperken.

Ook de kennisgeving aan betrokkenen moet 'onverwijld' geschieden. Hiervoor heeft de AP in de beleidsregels echter geen concrete termijn genoemd, maar zij geeft aan dat hoe eerder de betrokkene wordt geïnformeerd, hoe eerder deze in actie kan komen.

7. Beslisschema datalek en meldplicht

Hieronder wordt schematisch weergegeven wanneer sprake is van een datalek en wanneer een onderwijsinstelling een melding bij de toezichthouder en de betrokkene moet doen. Hierbij zijn enkele voorvragen reeds met "ja" beantwoord, zoals "Is sprake van verwerking van persoonsgegevens?, "Ben ik de verantwoordelijke voor de verwerking?" en "Is de Wbp van toepassing op de verwerking?".



8. Sanctiebevoegdheid AP

Met de nieuwe wetgeving is de sanctiebevoegdheid van de AP per 1 januari 2016 aanzienlijk uitgebreid. Bij schending van de meldplicht datalekken (het niet, niet tijdig of niet correct melden) heeft de AP de mogelijkheid om forse boetes uit te delen die kunnen oplopen tot maximaal € 820.000,- of 10% van de jaaromzet.[14]

De AP kan bovendien in meer gevallen een boete opleggen. Voornoemde boetes gelden namelijk niet alleen bij overtreding van de meldplicht datalekken, maar ook van diverse andere verplichtingen van de Wbp. Dat betekent dat ook boetes kunnen worden uitgedeeld aan onderwijsinstellingen die persoonsgegevens onzorgvuldig verwerken of niet adequaat beveiligen. Voldoende reden dus voor onderwijsinstellingen om op een behoorlijke en zorgvuldige manier persoonsgegevens te verwerken en het beheer van die gegevens op deugdelijke wijze te organiseren.

Daarbij verdienen met name aandacht de gegevensverwerkingen door onderwijsinstellingen in het kader van passend onderwijs, bij het gebruik van digitale leermiddelen en bij de inzet van sociale media en/of digitale portalen door scholen voor de communicatie met leerlingen en ouders.

9. Europese Privacyverordening

Ten slotte zorgt de komst van een Europese Privacyverordening voor nieuwe ontwikkelingen op het gebied van de bescherming van persoonsgegevens. Deze verordening is met ingang van 25 mei 2018 van toepassing. Zij werkt vanaf dat moment rechtstreeks door in alle EU-lidstaten en gaat alsdan vóór de Wbp. Onderwijsinstellingen hebben dus nog ongeveer anderhalf jaar de tijd om aan de nieuwe regels te voldoen. De beginselen van de verordening zijn in grote lijnen vergelijkbaar met de uitgangspunten van de Wbp. Maar let op, de verordening is op bepaalde punten strenger en concreter dan de Wbp. Hieronder lichten wij een aantal belangrijke verschillen tussen de Wbp en de verordening toe.

De verordening bevat een andere toets ter beoordeling van de vraag of sprake is van een meldingsplichtig datalek. Iedere inbreuk in verband met persoonsgegevens moet worden gemeld bij de toezichthouder, *tenzij* het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De verordening specificeert niet nader welke risico's dit (kunnen) zijn. Op grond van de Wbp moet enkel een datalek dat leidt tot (de aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens worden gemeld. Er zal vermoedelijk minder snel sprake zijn van "(een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens", dan van "een risico voor de rechten en vrijheden van natuurlijke personen". Per 25 mei 2018 moet dus in meer gevallen het datalek worden gemeld.

In Nederland geldt sinds 1 januari 2016 de verplichting om een overzicht bij te houden van alle meldingsplichtige inbreuken op de beveiliging (artikel 34a lid 8 Wbp). Op grond van artikel 33 lid 5 van de Europese Privacyverordening moeten alle, dus niet alleen de meldingsplichtige, inbreuken in verband met persoonsgegevens worden gedocumenteerd. Met de verordening wordt de administratieverplichting van de verantwoordelijke (onderwijsinstelling) dus een stuk omvangrijker.

Verder stelt de verordening meer en concretere eisen aan de melding die bij de toezichthouder moet worden gedaan. De Wbp bepaalt dat de melding in ieder geval moet vatten: de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen, de vermoedelijke gevolgen en de aanbevolen maatregelen om de negatieve gevolgen te beperken en. Op grond van de verordening worden in de melding echter ook, indien mogelijk, de categorieën van en bij benadering het aantal betrokkenen en persoonsgegevensregisters omschreven.

Een andere belangrijke verandering op grond van de verordening is dat een Privacy Impact Assessment (PIA)[15] moet worden uitgevoerd wanneer een verwerking van persoonsgegevens een hoog privacyrisico inhoudt.[16] Gelet op de in veel gevallen grootschalige verwerking van bijzondere persoonsgegevens zullen onderwijsinstel-

lingen al snel verplicht zijn een PIA uit te voeren en bovendien een zogenaamde functionaris voor gegevensbescherming aan te wijzen. Tot slot verdient vermelding dat de boetes die op grond van de verordening kunnen worden opgelegd, fors hoger zijn dan de boetes op basis van de Wbp. De verordening introduceert boetes van maximaal 20 miljoen euro of 4% van de totale wereldwijde omzet.

10. Conclusies

Sinds de invoering van de meldplicht datalekken per 1 januari 2016 is privacy "hot" nieuws. Kennelijk hebben (te) veel organisaties, ook in het onderwijs, de privacybescherming niet op orde. Voor onderwijsinstellingen geldt bovendien op grond van de Wbp een verzwaard beschermingsregime, want leerlinggegevens worden beschouwd als gevoelige gegevens (extra zorgvuldigheid betrachten) of zelfs bijzondere gegevens (verboden te verwerken, tenzij). Dit vraagt om een hoog beveiligingsniveau.

Aan de hand van de beleidsregels die de AP heeft opgesteld, hebben wij voor de meldplicht datalekken in deze bijdrage een beslisschema opgenomen. Dit schema biedt onderwijsinstellingen houvast bij de vraag of er sprake is van een datalek, en zo ja, hoe dan te handelen. Verplicht melden aan de AP betekent niet automatisch dat ook aan de betrokkene moet worden gemeld. Bij het lekken van gevoelige of bijzondere persoonsgegevens zal echter in beginsel ook de betrokkene daarvan in kennis dienen te worden gesteld.

De eerstvolgende aanscherping van de privacyregels ligt besloten in de Europese Privacyverordening die met ingang van 25 mei 2018 van toepassing is. Het is van belang dat onderwijsinstellingen daar vroegtijdig op acteren. Ons advies is om niet te wachten tot 25 mei 2018, maar hier nu al mee te beginnen.

Noten

1. http://www.nu.nl/internet/4294035/gegevens-scholieren-mogelijk-straat-hack.html. De kopij voor dit artikel was gereed op 22 juli 2016, ontwikkelingen na deze datum zijn daarom niet meer in deze bijdrage meegenomen.
2. http://www.vo-raad.nl/themas/privacy/mogelijk-datalek-in-overkoepelend-digitaal-leermiddelensysteem.
3. Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming.
4. Zie echter de kanttekeningen van Mw. Mr. I.A. Hoen en mr. B.A.J. van Lammeren in "Privacy van leerlingen in het digitale onderwijs", *School en Wet* 2016-1, p. 5-11.
5. Mw. Mr. I.A. Hoen en mr. B.A.J. van Lammeren in "Privacy van leerlingen in het digitale onderwijs", *School en Wet* 2016-1, p. 5-11.
6. Hoen en Van Lammeren, *ibid.*
7. De Model Bewerkersovereenkomst 2.0 is een bijlage bij het Convenant Digitale Onderwijsmiddelen en Privacy 2.0 dat is afgesloten tussen de PO-raad, VO-raad en de brancheorganisaties van educatieve uitgeverij (GEU), distribiteurs van leermiddelen (leden van sectie educatief van de Koninklijke Boekverkopersbond) en digitale dienstverleners in het onderwijs-ICT (VDOD). Bewerkersovereenkomsten op basis van de Model Bewerkersovereenkomst uit 2015 blijven in beginsel hun gelding houden totdat deze bewerkersovereenkomsten door partijen worden beëindigd en aansluitend worden opgevolgd door een nieuwe bewerkersovereenkomst op basis van de Model Bewerkersovereenkomst 2.0.
8. Volgens de definitie van artikel 1, aanhef en onder h, Model Bewerkersovereenkomst Versie 2.0.
9. https://www.internetconsultatie.nl/wetpseudonimiseren.
10. "Hogeschool Van Hall Larenstein lekt persoonsgegevens", *Omropfryslan* 7 maart 2016, www.omropfryslan.nl (zoek op Van Hall Larenstein persoonsgegevens).
11. "Studentgegevens UvA en HvA waren makkelijk vindbaar door systeemlek", *Nu* 20 juli 2016, www.nu.nl (zoek op Studentgegevens UvA en HvA).
12. "De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp) – Beleidsregels voor toepassing van artikel 34a van de Wbp" d.d. 8 december 2015.
13. https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?1.
14. Uit een bericht van NOS van 13 mei 2016 blijkt dat de AP betwijfelt of datalekken wel altijd gemeld worden. NOS meldt dat Vicevoorzitter Wilbert Tomesen vreest van niet gezien het relatief lage aantal gemelde datalekken (sinds 1 januari 2016 ruim 1600 volgens het bericht) en het feit dat er 130.000 organisaties in Nederland zijn die persoonsgegevens verwerken. Zie voor het bericht: http://nos.nl/artikel/2104842-privacywaakhond-datalekken-worden-niet-gemeld.html. Gevallen waarin de AP daadwerkelijk een boete heeft opgelegd, zijn ons (nog) niet bekend. Wel verschijnen in de media berichten dat hoge boetes dreigen voor organisaties omdat zij niet voldoen aan de meldplicht datalekken. Zie bijvoorbeeld: http://www.ad.nl/amersfoort/hoge-boete-dreigt-na-niet-melden-gemeentelijk-datalek~a1d040c7/.
15. In het Nederlands: een Gegevensbeschermingseffectbeoordeling.
16. Op grond van artikel 35 van de verordening is een PIA onder meer verplicht bij de grootschalige verwerking van bijzondere categorieën persoonsgegevens. Met name de grotere onderwijsinstellingen kunnen hiervoor dus in aanmerking komen.