

Vergaderjaar 2009–2010

32 123 VIII

Vaststelling van de begrotingsstaten van het Ministerie van Onderwijs, Cultuur en Wetenschap (VIII) voor het jaar 2010

Nr. 121

BRIEF VAN DE STAATSSECRETARIS VAN ONDERWIJS, CULTUUR EN WETENSCHAP

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 april 2010

Bij de behandeling van de Rijksbegroting voor het jaar 2010 van het Ministerie van Onderwijs, Cultuur en Wetenschap (32 123-VIII) is door minister Plasterk toegezegd per brief nader in te gaan op het toezicht op de beveiliging van leerlinggegevens bij de onderwijsinstellingen (zie handelingen 23–2017). Met voorliggende brief doe ik deze toezegging gestand.

De heer Biskop heeft bij de begrotingsbehandeling aandacht gevraagd voor de beveiliging van leerlinggegevens bij de onderwijsinstellingen. Daarbij heeft hij een rapport overhandigd met de resultaten van een onderzoek naar deze beveiliging. Het rapport, dat is opgesteld door enkele mbo-studenten, ziet met name door het nog wel eens achterwege blijven van de installatie van beschikbare updates van softwarepakketten waarin leerlinggegevens worden geregistreerd, een risico voor de veiligheid van de leerlinggegevens: via updates worden er immers nog wel eens veiligheidslekken in de software gedicht.

In het debat heeft minister Plasterk aangegeven de beveiliging van informatiesystemen en meer in zijn algemeenheid, de naleving van de bepalingen uit de Wet Bescherming Persoonsgegevens (WBP) bij de onderwijsinstellingen, de verantwoordelijkheid van de onderwijsinstellingen zelf te vinden. Deze verantwoordelijkheid is geregeld in de WBP. De heer Bisschop vroeg vervolgens of de minister hier verder geen enkele verantwoordelijkheid heeft en daar per brief nader op in te willen gaan.

Uiteraard heb ik een brede verantwoordelijkheid voor het goed functioneren van het onderwijssysteem. Mocht er binnen dit systeem sprake blijken te zijn van meer dan incidentele problemen bij de beveiliging van leerlinggegevens, dan zou dat voor mij aanleiding zijn voor het

overwegen van maatregelen. Ook zie ik voor mezelf een rol waar op mijn instigatie informatiesystemen worden geïmplementeerd. Dan past het om aanbevelingen te doen – ter ondersteuning van de verantwoordelijkheden van de onderwijsinstellingen ter zake – rond beveiligingsaspecten, met name waar er zich bijzondere risico's voordoen.

Zoals aangegeven, de verantwoordelijkheid voor de beveiliging van de leerlinggegevens op de instellingen, ligt bij de onderwijsinstellingen zelf. De onderwijs-raden laten zich – in het belang van (het imago van) de sectoren en ter ondersteuning van de bij de Raden aangesloten onderwijsinstellingen – ook goed aanspreken op een goede naleving van de WBP-bepalingen binnen de onderwijssectoren. Een mooi voorbeeld is het convenant met betrekking tot de bescherming van leerling-, deelnemer- en studentgegevens op scholen en instellingen, dat naar aanleiding van de introductie van het persoonsgebonden nummer binnen het onderwijsdomein, is gesloten tussen OCW en de Raden en – voor het po en vo – organisaties voor bestuur en management. Binnen de sectoren po en vo is door de organisaties voor bestuur en management in het verlengde van het convenant een modelreglement opgesteld voor de verwerking van leerlinggegevens.

Ik merk hierbij nog op dat ook de Raden nog wel eens t.b.v. de onderwijsinstellingen, informatiesystemen implementeren. Hierbij is mij gebleken dat er steeds grote zorg en aandacht is voor de privacy van personen, waar die in het geding zou kunnen zijn.

De onderwijsinstellingen zijn zich terdege bewust van de privacygevoeligheid van individuele gegevens van leerlingen. Daar wordt in het algemeen zorgvuldig mee omgegaan. Slechts sporadisch komen er schendingen van de WBP voor.

Niettemin, het kan zijn dat er in de loop der tijd nieuwe risico's ontstaan, bij voorbeeld als gevolg van nieuwe technologische ontwikkelingen. Ook al mag je verwachten dat er binnen de kring van professionals op de instellingen (ik denk in dit geval aan de systeembeheerders en administrateurs) hiervoor de nodige aandacht is, het kan natuurlijk geen kwaad om instellingen hierop te attenderen. Dat kan vanuit mijn positie, maar het past mijns inziens beter bij de positie van de Raden en de organisaties van eerder genoemde professionals.

Instellingen attenderen op de risico's van het niet tijdig installeren van updates van softwarepakketten valt wat mij betreft in de categorie van risico's waar mogelijk, ondanks de goede zorgen op de instellingen voor de privacy, te weinig aandacht voor is.

Hoewel ik, als boven geschetst, niet de aangewezen partij ben om scholen op deze risico's te wijzen, is het voor mij (met name voor de Dienst Uitvoering Onderwijs) weinig moeite om dit risico onder de aandacht van de administrateurs van de onderwijsinstellingen te brengen. DUO heeft hiervoor geëigende communicatielijnen met de administrateurs (ondermeer opgezet n.a.v. de invoering van het persoonsgebonden nummer binnen het onderwijs en de daarbij benodigde gegevensbewerkingen en -uitwisselingen). Ik zeg daarom, los van de vraag of dat nu wel past bij de door mij geschetste verantwoordelijkheidsverdeling, graag toe in de reguliere communicatie richting administrateurs van de onderwijsinstellingen nog eens te wijzen op het belang van gegevensbeveiliging. Ik zal daarbij aandacht vragen voor de updates en mogelijk nog wat soortgelijke tips geven waarmee administrateurs geattendeerd worden op verdere mogelijk bij de administrateurs minder bekende risico's voor de veiligheid van de leerlinggegevens op de onderwijsinstelling.

De staatssecretaris van Onderwijs, Cultuur en Wetenschap,
J. M. van Bijsterveldt-Vliegenthart