Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2017–2018

34 741 Wijziging van diverse onderwijswetten in verband met het pseudonimiseren van het persoonsgebonden nummer van een onderwijsdeelnemer ten behoeve van het bieden van voorzieningen in het kader van het onderwijs en de begeleiding van onderwijsdeelnemers

B

MEMORIE VAN ANTWOORD

Ontvangen 17 november 2017

De regering is de leden van de fracties van de VVD, de SP, GroenLinks en de PvdA van de vaste commissie voor Onderwijs, Cultuur en Wetenschap erkentelijk voor de gestelde vragen. Op de vragen zal hierna in de volgorde van het voorlopig verslag worden ingegaan.

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij achten het van belang dat een eenvoudigere, minder privacygevoelige mogelijkheid wordt gecreëerd om leerlingen toegang te geven tot digitale leermiddelen. Genoemde leden hebben enkele vragen. De leden van de fracties van SP, GroenLinks en de PvdA sluiten zich bij deze vragen aan.

De beantwoording van de vragen van de leden van de VVD-fractie is daarmee tevens de beantwoording van de vragen van de leden van de fracties van SP, GroenLinks en de PvdA.

Het is een feit van algemene bekendheid dat scholen en gemeenten niet of onvoldoende aan de voor hen toepasselijke privacywetgeving voldoen. Toch heeft de regering tijdens de behandeling van dit wetsvoorstel in de Tweede Kamer de verwachting uitgesproken dat gemeenten en scholen ook na invoering van de onderhavige wetswijziging in staat zullen zijn om te voldoen aan de Algemene verordening gegevensbescherming die op 25 mei 2018 in werking treedt. Waarop baseert de regering zich bij deze verwachting, zo vragen de leden van de VVD-fractie.
De (vertegenwoordigers van) onderwijsinstellingen en leveranciers spannen zich de laatste jaren stevig en op vele manieren in om door middel van zelfregulering de privacy van leerlingen te borgen. Zo hebben de PO-Raad, VO-raad en brancheorganisaties van leveranciers in juni 2016 het convenant «Digitale onderwijsmiddelen en privacy 2.0» gesloten. Dit convenant creëert waarborgen voor de zorgvuldige omgang met persoonsgegevens door onderwijsinstellingen en leveranciers die worden verwerkt in het kader van het gebruik van digitale onderwijsmiddelen. In het convenant worden de verplichtingen die voortvloeien uit de Wbp en

kst-34741-B
ISSN 0921 - 7371
's-Gravenhage 2017

Avg geconcretiseerd. Met het wetsvoorstel ondersteunt de regering deze zelfregulering.

Het wetsvoorstel maakt het voor onderwijsinstellingen mogelijk om het persoonsgebonden nummer (PGN) eenmalig te gebruiken om een pseudoniem te genereren. Dit pseudoniem vormt de basis om voor specifieke gevallen andere pseudoniemen (ketenID's) te kunnen genereren en gebruiken. Het gebruik van een ketenID maakt een veiliger, betrouwbaarder en meer efficiënte digitale uitwisseling van gegevens door onderwijsinstellingen met andere partijen mogelijk. Het wetsvoorstel voorziet erin dat een dergelijk ketenID gegenereerd kan worden voor de toegang tot en het gebruik van digitale leermiddelen en het digitaal afnemen van toetsen en examens. Dit leidt ertoe dat het aantal persoonsgegevens dat een onderwijsinstelling gebruikt voor de digitale uitwisseling van gegevens met betrokken leveranciers tot een minimum beperkt kan worden. Deze dataminimalisatie is een verplichting die voortvloeit uit de Wbp en in de Avg onverminderd is overgenomen. In aanvulling hierop is in de verordening opgenomen dat de toepassing van pseudonimisering op persoonsgegevens de risico's voor de betrokkenen kan verminderen en de verantwoordelijken en de bewerkers in staat kan stellen om hun verplichtingen inzake gegevensbescherming na te komen. Het wetsvoorstel draagt er op deze manier aan bij dat onderwijsinstellingen en leveranciers die betrokken zijn bij het gebruik van digitaal leermateriaal op een goede manier kunnen voldoen aan de Avg.

Kan de regering in dit verband aangeven op welke criteria gemonitord en geëvalueerd gaat worden, zo vragen de leden van voornoemde fractie. Het wetsvoorstel heeft tot doel om een veiliger, betrouwbaarder en meer efficiënte digitale uitwisseling van gegevens door onderwijsinstellingen mogelijk te maken, waarbij bovendien zo min mogelijk persoonsgegevens worden gebruikt van leerlingen, deelnemers of studenten. Het werken met een pseudoniem en ketenID dient beide doelen, daarbij is het wel van belang dat de invoering zorgvuldig gebeurt. Bij de start van dit schooljaar bleek dat duizenden leerlingen geen toegang hadden tot hun digitale lesstof. Om deze problemen voor de toekomst te voorkomen, is het nodig dat de systemen van alle betrokken partijen (onderwijsinstellingen en aanbieders van schoolinformatiesystemen, distributeurs en uitgeverijen) onderling goed kunnen communiceren, omdat ze anders niet weten welke lesstof bij welke leerling hoort. Een zorgvuldige invoering is van belang om de continuïteit van het onderwijs te kunnen waarborgen. Tegelijkertijd is het zaak dat wanneer het verantwoord is dat alle partijen volgens de nieuwe systematiek kunnen werken, deze wordt ingevoerd. Deze twee criteria zijn voor de regering de belangrijkste aandachtspunten voor de jaarlijkse monitoring, waarbij de continuïteit van het onderwijs voorop staat. Aanvullend voor de evaluatie geldt dat breder wordt gekeken naar de werking van zelfregulering en zal onderzocht worden of onderwijsinstellingen de Avg voldoende in acht nemen.

Kan de regering een tijdige signalering garanderen als scholen en leveranciers ondanks deze wet onvoldoende zouden gaan werken via het pseudoniem, zo vragen deze leden. En hoe zal de regering in voorkomend geval ingrijpen, zo vragen de leden van voornoemde fractie.

Als uit de monitoring blijkt dat er onvoldoende voortgang wordt geboekt, zullen in overleg met de sectororganisaties en brancheorganisaties van leveranciers aanvullende maatregelen worden ontwikkeld om op een verantwoorde manier een tijdige invoering te bevorderen. Mocht de evaluatie aantonen dat de gekozen aanpak van zelfregulering in de praktijk onvoldoende effect sorteert, dan zal een nadere afweging plaatsvinden over de te nemen maatregelen, zoals het wettelijk voorschrijven van het

gebruik van het pseudoniem/ketenID en/of de aanvullende persoonsgegevens die mogen worden verstrekt. Ten aanzien van de omgang met het PGN, pseudoniem en ketenID worden de kaders gesteld door de Avg, dit wetsvoorstel en de daarop gebaseerde lagere regelgeving. De Autoriteit Persoonsgegevens ziet toe op de naleving van deze regelgeving.

De regering heeft als reactie op het commentaar van de Raad van State een vijfjaarlijkse wetsevaluatie aangekondigd. Daarnaast heeft de regering een motie van de Tweede Kamer (motie van het lid Westerveld van 4 oktober 2017) overgenomen, waarin wordt opgeroepen om bovenop de vijfjaarlijkse evaluatie ook nog jaarlijks een stand van zaken-overzicht te geven over de implementatie van deze wet en om hierbij de bescherming van persoonsgegevens van alle onderwijsdeelnemers te betrekken, alsmede de ontwikkelingen die op dit vlak hebben plaatsgevonden en hoe hierop wordt ingespeeld.[1]

Wat was de reden van de regering om genoemde motie over te nemen, zo vragen de leden van de VVD-fractie. Acht de regering deze veelheid aan evaluatiemomenten en -criteria proportioneel, zo vragen deze leden. Het is belangrijk dat de nieuwe systematiek zorgvuldig wordt ingevoerd, zodat de continuïteit van het onderwijs niet in het geding komt en tegelijkertijd de privacy van onderwijsdeelnemers wordt bevorderd. De problemen die zijn ontstaan aan het begin van dit schooljaar, waarbij duizenden leerlingen geen toegang hadden tot digitaal leermateriaal, onderstrepen dit belang. Om het pseudoniem en ketenID zorgvuldig in te voeren bij onderwijsinstellingen en leveranciers is een programma ingericht dat de implementatie coördineert. Om te kunnen bepalen of het pseudoniem en ketenID zorgvuldig ingevoerd kunnen worden bij bepaalde scholen en leveranciers worden de nodige tests uitgevoerd. De informatie die hieruit voortkomt, zal de basis zijn voor onderwijsinstellingen en leveranciers om te bepalen of de nieuwe systematiek ingevoerd kan worden. Deze informatie dient tegelijkertijd om de voortgang op het geheel te monitoren en daarover te rapporteren. De regering hecht eraan de Tweede Kamer goed te informeren over de invoering van de nieuwe systematiek. Gelet op het feit dat de benodigde informatie hiervoor al voorhanden is en geen verzwaring voor betrokken partijen meebrengt, heeft de regering ervoor gekozen de motie over te nemen en acht zij deze proportioneel.

Welke inspanning zal ter zake worden gevergd van veldpartijen en departement, zo vragen de leden van voornoemde fractie. En wat zijn de geraamde kosten van implementatie van deze wet en wat zijn de kosten van de evaluaties, inclusief de kosten voor de instellingen, zo vragen de leden van voornoemde fractie.

De inspanningen aan de kant van de onderwijsinstellingen die gemoeid zijn met de implementatie van de wet verschillen per sector (po, vo en mbo), maar zijn beperkt. Het zijn vooral de leveranciers die gebruik van het pseudoniem mogelijk moeten maken in hun systemen. Het programma dat belast is met de coördinatie van de invoering van het pseudoniem onderhoudt de contacten met leveranciers en heeft daardoor een goed overzicht van het aantal leveranciers dat het pseudoniem gebruikt en daarmee van de voortgang op het geheel. Aangezien gebruik wordt gemaakt van bestaande informatie levert de monitoring geen extra inspanningen of kosten op voor veldpartijen en het departement. De incidentele, centrale ontwikkelkosten (ca. € 300.000) van de voorziening die de pseudoniemen en ketenID's genereert en de kosten van het beheer daarvan, worden gefinancierd door de Minister van OCW. Het centrale

[1] Kamerstukken II 2017/18, 34 741, nr. 7.

programma (ca. € 1.000.000) wordt ook door de Minister gefinancierd. De invoering van het pseudoniem en ketenID's heeft geen directe financiële gevolgen voor onderwijsinstellingen. De leveranciers maken kosten om de aanpassingen in hun systemen te kunnen doen, deze kosten zijn niet inzichtelijk voor de regering. De kosten voor de evaluatie zijn nog niet geraamd, maar zullen – gelet op de kosten van andere evaluaties – naar verwachting tussen de € 30.000 en € 60.000 bedragen.

De leden van de VVD-fractie achten het van belang dat de wijze van pseudonimiseren, dus de techniek die in het kader van de uitvoering van dit wetsvoorstel wordt toegepast, ook leidt tot de nodige digitale veiligheid. Kan de regering hierop ingaan, zo vragen de leden van voornoemde fractie. Hoe weet de regering dat de toegepaste technieken om tot pseudonimiseren te komen sterk genoeg zijn, zo vragen deze leden.
Er is uitgebreid onderzoek verricht naar de verschillende technische mogelijkheden. De keuze voor de huidige techniek van pseudonimiseren, de wijze waarop deze pseudoniemen tot stand komen en de bijbehorende beveiligingseisen (waaronder de versleuteling van gegevens) zijn gebaseerd op twee overwegingen. Er is gekozen voor een systematiek die in de praktijk is bewezen (proven technology) en waarbij gebruik wordt gemaakt van de op dit moment gangbare internationale standaarden. Daarnaast is de gekozen techniek goed te implementeren in de systemen van leveranciers, waarmee een zorgvuldige en tijdige invoering mogelijk is. Bij het ontwerp en de realisatie van de voorziening die de pseudonimisering verzorgt (de Nummervoorziening) zijn de volgende (inter)nationaal geldende veiligheidseisen gehanteerd:
- CBP Richtsnoeren beveiliging persoonsgegevens, feb 2013.
- ICT beveiligingsrichtlijnen voor TLS, NCSC, nov 2014.
- Algorithms, key sizes and parameters report 2014, ENISA.
- ISO/TS 25237 Health informatics / pseudonymisation.
- Stichting Kennisnet is ISO 27001 gecertificeerd.

Daarnaast is voorzien in de volgende waarborgen om de nodige digitale veiligheid bij de totstandkoming en het gebruik van het pseudoniem en ketenID te kunnen waarborgen:
– het PGN in het administratiesysteem van de school wordt gehasht voordat dit via een versleutelde verbinding naar de Nummervoorziening wordt verstuurd;[2]
– de Nummervoorziening hasht het PGN om een pseudoniem te genereren (de Nummervoorziening slaat het PGN niet centraal op);
– het pseudoniem wordt gehasht om een ketenID te genereren;
– het pseudoniem en ketenID wordent versleuteld naar het leerlingadministratiesysteem verstuurd;
– het pseudoniem en ketenID worden apart van elkaar en van andere persoonsgegevens opgeslagen in de leerlingadministratie;
– het pseudoniem wordt met geen enkele andere partij uitgewisseld;
– het ketenID wordt slechts met partijen uitgewisseld die digitale onderwijsdiensten aanbieden die het gebruik van digitale leermiddelen en digitale toetsen en examens mogelijk maakt.

Hoe gemakkelijk is het om op basis van de gepseudonimiseerde gegevens tot de werkelijke identiteitsgegevens te komen, zo vragen de leden van de VVD-fractie.
De kans dat op basis van het pseudoniem zelf een onderwijsdeelnemer geïdentificeerd kan worden is minimaal. Naast het pseudoniem is het voor de onderwijsinstelling echter ook nodig om een paar andere gegevens

[2] «Hashing» is een cryptografische functie die ervoor zorgt dat het PGN wordt omgezet in een code, die niet teruggerekend kan worden naar het PGN.

van onderwijsdeelnemers uit te wisselen met leveranciers, om digitale leermiddelen in de klas goed te kunnen laten werken. De kans bestaat dat op basis van de voornaam en groep de identiteit van een leerling te herleiden is. Om ervoor te zorgen dat dit alleen door bevoegde personen gebeurt, maken onderwijsinstellingen concrete afspraken met leveranciers over het gebruik en de beveiliging van deze gegevens. Het risico op onbevoegde identificatie van leerlingen wordt daarmee tot een minimum beperkt. Het pseudoniem maakt verdere dataminimalisatie mogelijk. Doordat het aantal noodzakelijke persoonsgegevens dat met leveranciers wordt uitgewisseld, wordt teruggebracht, neemt de kans op identificatie af. Wanneer er onverhoopt sprake is van een datalek, waarbij gegevens van leerlingen voor onbevoegden inzichtelijk zijn, neemt de impact eveneens af doordat er minder persoonsgegevens bij de leveranciers bekend zijn.

De regering voorziet implementatie per schooljaar 2018/2019. Voorkomen moet worden dat leerlingen in het nieuwe schooljaar gedupeerd worden door een mogelijk gebrekkige toegang tot digitale leermiddelen doordat systemen moeten worden aangepast. Op grond waarvan meent de regering dat invoering inclusief proeftesten in genoemd schooljaar voor de betrokken instellingen uitvoerbaar is, zo vragen de leden van de VVD-fractie.
De regering onderschrijft het belang van een betrouwbare toegang tot digitaal leermateriaal, zodat de continuïteit van het onderwijs niet in het geding komt.

De problemen die begin dit schooljaar zijn ontstaan, zijn voor de sectororganisaties en brancheverenigingen van leveranciers aanleiding om een onafhankelijk onderzoek te laten uitvoeren en daarmee een analyse te maken van de problematiek. De uitkomsten van dit onderzoek zullen ook benut worden om de plannen voor implementatie en afspraken daarover te verbeteren. Naast goede implementatieplannen en afspraken is het belangrijk om tijdig en zorgvuldig te testen, voordat tot invoering overgegaan kan worden. Deze testen zullen uitwijzen in welke gevallen het al wel mogelijk is om tot zorgvuldige invoering over te gaan en in welke gevallen nog niet. In alle gevallen is het nodig dat het wetsvoorstel begin 2018 in werking treedt, om met ingang van volgend schooljaar tot implementatie over te kunnen gaan.
De Onderwijsraad heeft aanbevolen dat er standaarden komen voor digitale veiligheid op scholen. De regering heeft in een Algemeen Overleg in de Tweede Kamer toegezegd hierover te overleggen met de PO-raad en VO-raad. Inmiddels is een convenant gesloten tussen sectororganisaties en leveranciers en is een standaard voor digitale beveiliging ontwikkeld. Kan de regering aangeven of, en zo ja, op grond waarvan zij deze standaard voldoende acht en hoe het inmiddels staat met de uitwerking ervan met het oog op haalbaarheid van invoering per schooljaar 2018/2019, zo vragen de leden van de VVD-fractie.
Er bestaan standaarden die leveranciers kunnen gebruiken om de informatiebeveiliging en privacy op een passend niveau te krijgen en dit aantoonbaar te kunnen maken. Voor het onderwijs is een specifieke standaard ontwikkeld, namelijk het certificeringsschema «informatiebeveiliging en privacy ROSA». Deze standaard is een vertaling van geldende (inter)nationale standaarden en specifiek toegesneden op het onderwijs. Dit certificeringsschema voorziet in een set van maatregelen die verzekeren dat gegevens van leerlingen goed beveiligd zijn. Toepassing hiervan leidt er onder meer toe dat personen die daartoe niet bevoegd zijn geen toegang kunnen krijgen tot de systemen van leveranciers en de gegevens van leerlingen die daarin zijn opgeslagen. De invoering van het certificeringschema wordt door leveranciers in samenhang met de invoering van het pseudoniem opgepakt.

In het kader van consistentie van beleid zouden de leden van de VVD-fractie graag van de regering vernemen hoe de in dit wetsvoorstel voorgestelde regeling zich verhoudt tot de wijze waarop een en ander is geregeld in de andere onderwijssectoren. Genoemde leden hebben vernomen dat de problematiek ook speelt rond Studielink en brancherapportages voor bijvoorbeeld Vereniging Hogescholen en MBO-Raad. Persoonsgegevens zijn daar niet inzichtelijk, terwijl informatie op brancheniveau wel geëvalueerd moet kunnen worden. Genoemde leden hebben begrepen dat daar momenteel de methode van omnummeren wordt gebruikt. Overweegt de regering om de systematiek voor alle onderwijssectoren gelijk te trekken, zo vragen de leden van voornoemde fractie.
Uitgangspunt van de regering is om éénduidige oplossingen te creëren bij vergelijkbare omstandigheden. Dit wetsvoorstel is daar een goed voorbeeld van, omdat het voor alle onderwijssectoren dezelfde bevoegdheid regelt.

Hiermee kunnen alle onderwijsinstellingen het persoonsgebonden nummer gebruiken om een pseudoniem en ketenID te genereren en dit vervolgens gebruiken voor de toegang tot en het gebruik van digitale leermiddelen. Verder bevordert dit wetsvoorstel éénduidigheid door te voorzien in de mogelijkheid om bij AMvB andere welomschreven gevallen aan te wijzen, waarvoor andere ketenID's kunnen worden gegenereerd. De regering zal daartoe overgaan wanneer op basis van onderzoek (waaronder een privacy impact assessment) is vastgesteld dat het gebruik van een ketenID de betrouwbaarheid, efficiëntie en veiligheid van digitale uitwisseling tussen onderwijsinstelling en een andere partij vergroot en/of verdere dataminimalisatie als gevolg hiervan mogelijk wordt gemaakt.

Een ketenID is alleen nodig wanneer een onderwijsinstelling met een derde partij een unieke, kwalitatief hoogwaardige en persistente identiteit van onderwijsdeelnemers nodig heeft om digitaal gegevens te kunnen uitwisselen. Tegen deze achtergrond is ook verkend of dit wetsvoorstel een verbetering kan betekenen voor het gebruik van gegevens voor brancherapportages. Hieruit is gebleken dat het doel, de betrokken partijen en de inrichting van deze informatievoorziening dusdanig verschilt van het gebruik van digitale leermiddelen door onderwijsinstellingen, dat het invoeren van een ketenID hiervoor geen meerwaarde biedt.

Om de uitvoerbaarheid van het wetsvoorstel te kunnen beoordelen hebben de leden van de VVD-fractie behoefte aan nader inzicht in de financieringsafspraken over de digitale infrastructuur. In het hoger onderwijs kwam tot dit jaar het gebruik voor digitale voorzieningen, zoals DigiD en mijnoverheid.nl, voor rekening van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De kosten daarvan zijn echter door de toenemende digitalisering van de dienstverlening zo gestegen, dat in de ministerraad besloten is deze, vooruitlopend op de Wet generieke digitale infrastructuur, per 1 januari 2018 te gaan doorbelasten aan de eindgebruikers, via een prijs per tik (in het geval van DigiD is een tik dan een login bij DigiD). Dit besluit is recent uitgewerkt en er is een prijs vastgesteld, zo hebben genoemde leden vernomen. Het betekent dat OCW jaarlijks een rekening ontvangt voor het aantal DigiD-logins bij DUO, die dus worden berekend op basis van een p*q (aantal logins keer prijs). Graag vernemen de leden van de VVD-fractie of dit juist is. Gaat het Ministerie van Onderwijs, Cultuur en Wetenschap op zijn beurt deze kosten doorberekenen aan de instellingen, zo vragen deze leden. Zo ja, hoe hoog worden deze kosten dan voor de individuele instellingen, zo vragen de leden van voornoemde fractie.

Organisaties die in hun digitale dienstverlening aan burgers gebruik mogen maken van DigiD, krijgen inderdaad een rekening voor het gebruik van deze voorziening over 2018.
De rekening die OCW ontvangt betreft het gebruik voor inloggen van studenten op de processen bij DUO, zoals het aanvragen van studiefinanciering en het versturen van een digitaal afschrift uit het diplomaregister. Het is niet de bedoeling dit aan instellingen of studenten/burgers door te belasten, dit wordt in de uitvoeringskosten van DUO verrekend. Het inschrijven van studenten bij een HO-instelling verloopt via Studielink. Zij zullen één rekening ontvangen voor het gebruik van DigiD ten behoeve van de HO-instellingen. Studielink en de instellingen moeten samen bezien hoe om te gaan met deze extra gebruikskosten.

Is bij de uitvoering van het onderhavige wetsvoorstel ook een dergelijk kostenbeslag te verwachten, zo vragen deze leden. Zo ja, welk kostenbeslag is hier dan voor de individuele instellingen mee gemoeid, zo vragen de leden van voornoemde fractie. En wat betekent dit voor de totale kosten van invoering van onderhavige wetswijziging, zo vragen leden van voornoemde fractie.
Het onderhavige wetsvoorstel betekent geen extra kosten voor onderwijsinstellingen als gevolg van besluitvorming in de ministerraad. Voor de pseudonimisering wordt geen gebruik gemaakt van de generieke digitale infrastructuur van de overheid, maar van de infrastructuur die voor het onderwijs is georganiseerd. De Nummervoorziening is bij Stichting Kennisnet ontwikkeld en zij rekent geen bedrag aan onderwijsinstellingen voor het gebruik van deze voorzieningen.

De Minister van Onderwijs, Cultuur en Wetenschap,
I.K. van Engelshoven

De Minister voor Basis- en Voortgezet Onderwijs en Media,
A. Slob