

Ministerie van Onderwijs, Cultuur en
Wetenschap

>Retouradres Postbus 16375 2500 BJ Den Haag

De Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Primair Onderwijs
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Onze referentie
1255711

Uw brief van
6 september 2017

Uw kenmerk
2017Z11539

Datum 27 september 2017

Betreft Beantwoording vragen van de leden Becker en Wörsdörfer (VVD) over het op straat belanden van gevoelige gegevens van 1800 kwetsbare leerlingen

Hierbij zend ik u, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de antwoorden op de vragen van de leden Becker en Wörsdörfer (VVD) over het op straat belanden van gevoelige gegevens van 1800 kwetsbare leerlingen.

De staatssecretaris van Onderwijs, Cultuur en Wetenschap,

Sander Dekker

2017Z11539

Vragen van de leden Becker en Wörsdörfer (beiden VVD) aan de staatssecretaris van Onderwijs, Cultuur en Wetenschap en de minister van Binnenlandse Zaken en Koninkrijksrelaties over het op straat belanden van gevoelige gegevens van 1800 kwetsbare leerlingen (ingezonden 6 september 2017)

1

Kent u het bericht 'Gevoelige gegevens 1800 kwetsbare kinderen op straat'? 1)

Ja.

2

Klopt het dat maar liefst 21 gemeenten in het openbare aanbestedingsproces voor het leerlingvervoer de leerlinggegevens niet hebben geanonimiseerd, waardoor het mogelijk werd om via internet de huisadressen, geboortedata, schoollocaties en roostertijden van kwetsbare kinderen in te zien?

Ja, ik ben bekend met deze problematiek.

3

Deelt u de mening dat ouders erop moeten kunnen rekenen dat de (lokale) overheid prudent met de gegevens van kinderen omgaat en zich daarbij houdt aan de Wet bescherming persoonsgegevens? Hoe verklaart u dat gemeenten daar in dit geval te weinig oog voor hebben gehad?

Daar ben ik het uiteraard mee eens. Gemeenten dienen altijd wanneer er persoonsgegevens in het geding zijn te handelen conform de Wet bescherming persoonsgegevens. Waarom de betreffende gemeenten daar in dit geval te weinig oog voor hebben gehad is mij niet bekend. De gemeenten zijn daarover verantwoording verschuldigd aan de gemeenteraad.

4

Kunt u aangeven of er andere openbare gemeentelijke aanbestedingen zijn waar een risico bestaat op het openbaar geraken van privacygevoelige informatie van inwoners? Zo ja, welke?

De gemeenten kunnen allerlei taken die betrekking hebben op individuele burgers uitbesteden bij openbare aanbesteding. Bijvoorbeeld wijkteams en maatschappelijke ondersteuning. Dit wordt niet bijgehouden op rijksniveau.

5

Bent u bereid gemeenten naar aanleiding van deze gebeurtenis nog eens actief te wijzen op de eisen uit de Wet bescherming persoonsgegevens en daarbij gemeenten van elkaar te laten leren?

In het kader van het interdepartementale en interbestuurlijke Programma sociaal domein vormt Uitwisseling Persoonsgegevens en Privacy één van de thema's waar specifiek aandacht aan zal worden besteed. Daarnaast wordt er op dit moment gewerkt aan een handreiking voor aanbesteding in het sociaal domein, daarin zal ook aandacht zijn voor privacy.

6

Zal het wetsvoorstel pseudonimiseren van leerlinggegevens ook een rol spelen in het gebruik van leerlinggegevens door gemeenten en kunnen daarmee situaties zoals deze, in elk geval voor wat betreft leerlinggegevens, worden voorkomen? Zo ja, op welke wijze? Zo nee, waarom niet? 2)

Het wetsvoorstel pseudonimiseren van leerlinggegevens is niet gericht op het gebruik van leerlinggegevens door gemeenten. Dit ligt voor situaties als deze ook niet voor de hand: voor dergelijke aanbestedingen volstaat een eenmalige uitwisseling van gegevens, waarbij het kunnen identificeren van leerlingen niet noodzakelijk is.

Het wetsvoorstel pseudonimiseren heeft tot doel een veiliger, betrouwbaarder en meer efficiënte digitale uitwisseling van leerlinggegevens door onderwijsinstellingen met andere partijen mogelijk te maken. Daarbij richt het voorstel zich in eerste instantie op het pseudonimiseren van leerlinggegevens voor de toegang tot en het gebruik van digitale leermiddelen en het digitaal afnemen van toetsen en examens.

Het wetsvoorstel voorziet wel in de mogelijkheid om bij algemene maatregel van bestuur andere gevallen aan te wijzen, waarvoor per geval een ander pseudoniem wordt gegenereerd. Dit zal alleen plaatsvinden nadat uit nader onderzoek en een privacy impact assessment nut en noodzaak van het introduceren van een ander pseudoniem evident is. Dat zal slechts in gevallen zijn waarbij een kwalitatief hoogwaardige, unieke en persistente identiteit van leerlingen nodig is om het doel van de gegevensverwerking te bereiken.

7

Heeft u kennisgenomen van de stelling in de berichtgeving dat TenderNed niet verantwoordelijk is voor de verspreiding van de leerlinggegevens, maar dat de gemeenten zelf die deze gegevens aanleverden? Erkent u dat TenderNed weliswaar niet verantwoordelijk is, maar als publieke organisatie wel degelijk een rol kan spelen om aanbestedende partijen te wijzen op de Wet bescherming persoonsgegevens? Bent u bereid dit bij de Rijksdienst voor Ondernemend Nederland onder de aandacht te brengen?

Ja. Het afgelopen jaar werden door aanbestedende diensten ruim 99.000 documenten geüpload op TenderNed (als onderdeel van PIANOo gehuisvest binnen de Rijksdienst voor Ondernemend Nederland). Bij registratie op TenderNed worden zij erop gewezen dat de inhoud van die documenten hun verantwoordelijkheid blijft. Daarnaast wordt een extra melding in TenderNed toegevoegd, om aanbestedende diensten voorafgaand aan het openbaar maken van documenten nogmaals te wijzen op hun verantwoordelijkheid als het gaat om privacygevoelige informatie. Dit blijft primair een verantwoordelijkheid van de aanbestedende diensten zelf. Ik deel wel uw mening dat PIANOo, als expertisecentrum aanbesteden, een informerende rol kan spelen richting aanbestedende diensten. Deze rol pakt PIANOo ook. PIANOo heeft in reactie op de verspreiding van leerlinggegevens meer informatie geplaatst over hoe als aanbestedende dienst om te gaan met gevoelige informatie in een aanbesteding.¹

8

Erkent u dat door toenemende digitalisering van leerlinggegevens het risico in de toekomst groter wordt dat gevoelige informatie toegankelijk wordt voor derden en dit ook bewustwording bij scholen vraagt? Zo ja, welke acties onderneemt u hiertoe?

Ik ben het hiermee eens. Dagelijks vertrouwen miljoenen ouders hun kinderen toe aan de school en zij moeten erop kunnen rekenen dat leerlingen én hun gegevens veilig zijn. De toenemende digitalisering vraagt om bewustwording en het zorgvuldig omgaan met persoonsgegevens. Waar vroeger de kast met leerlinggegevens op slot werd gedraaid en de sleutel op een veilige plek bewaard, moet hetzelfde gebeuren met digitale gegevens. Dit kan alleen op de scholen zelf gebeuren.

Om het bewustzijn op scholen te vergroten en ervoor te zorgen dat zij zorgvuldig omgaan met leerlinggegevens, heb ik afspraken gemaakt met de PO-Raad, VO-raad en Kennisnet over de uitvoering van verschillende activiteiten. Zo wordt in oktober wederom de jaarlijkse Maand van de Informatiebeveiliging en Privacy georganiseerd. Dan staat dit thema hoog op de agenda in workshops en campagnes.

De sectororganisaties en Kennisnet bieden scholen een toegankelijke aanpak voor het op orde brengen van de informatiebeveiliging en privacy.² Daarin zijn hulpmiddelen opgenomen, zoals een voorbeeldprotocol datalekken, een model privacyreglement, een voorbeeld sociale mediaprotocol, voorbeeldteksten om ouders te informeren over privacy op school, een online 'Quickscan privacy' en een voorbeeldbrief voor toestemming van ouders voor gebruik van foto's en video's beschikbaar voor scholen.

Ook hebben de sectororganisaties met aanbieders van digitale onderwijsmiddelen een privacyconvenant afgesloten.³ Deze afspraken zijn uitgewerkt in een modelbewerkerovereenkomst die scholen kunnen gebruiken om goede afspraken te maken met aanbieders van digitale onderwijsmiddelen op het gebied van privacy. Steeds meer scholen maken hier gebruik van.

Tot slot starten de PO-Raad en VO-raad dit najaar met een onderzoek (monitor) naar de stand van zaken met betrekking tot informatiebeveiliging en privacy op scholen.

¹ <https://www.pianoo.nl/actueel/nieuws/privacygevoelige-informatie-in-aanbestedingsdocumenten>

² https://maken.wikiwijs.nl/81891/Informatiebeveiliging___Privacy

³ Voor meer informatie: <https://www.privacyconvenant.nl/>

9

Wat is de stand van zaken met betrekking tot uw toezegging om met de sectoren primair en voortgezet onderwijs standaarden te ontwikkelen voor de digitale veiligheid van leerlinggegevens? Zijn deze standaarden er in het najaar, op het moment dat u hebt toegezegd de Kamer over de voortgang te informeren? Zo nee, waarom niet?

Ja, voor het onderwijs is een standaard ontwikkeld, het zogeheten 'certificeringsschema informatiebeveiliging en privacy'. Leveranciers kunnen deze standaard gebruiken om de beveiliging van leerlinggegevens op een passend niveau te krijgen en dit aantoonbaar te maken aan scholen. De standaard voorziet in een set van maatregelen die verzekeren dat gegevens van leerlingen goed beveiligd zijn.⁴ Er zijn steeds meer leveranciers die deze standaard gebruiken, mede omdat het een invulling is van de eisen die de Europese Algemene verordening gegevensbescherming stelt. Het gebruik van de standaard wordt verder gestimuleerd in samenhang met de invoering van het wetsvoorstel pseudonimiseren. Ik ben hier nader op ingegaan in de beantwoording van de schriftelijke inbreng van uw Kamer, die ik u begin deze week heb doen toekomen.

1) RTL Nieuws d.d. 5 september 2017

2) Kamerstuk 34 741

⁴ Zie voor meer informatie de website van EduStandaard:
https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-2017/