Tweede Kamer der Staten-Generaal

2

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

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 25 september 2017

Deze nota naar aanleiding van het verslag wordt gegeven in overeenstemming met de Minister van Economische Zaken.

Graag willen wij de leden van de vaste commissie voor Onderwijs, Cultuur en Wetenschap danken voor hun inbreng en voor de vragen die ze hebben gesteld en de opmerkingen die zijn gemaakt. Op de gestelde vragen gaan wij hieronder in, waarbij de volgorde van het verslag wordt aangehouden.

ALGEMEEN

De leden van de VVD-fractie hebben kennisgenomen van het wetsvoorstel 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. Zij hebben nog enkele vragen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het onderhavige wetsvoorstel. Deze leden hebben nog wel een vraag.

De leden van de D66-fractie hebben kennisgenomen van het wetsvoorstel inzake het pseudonimiseren van het persoonsgebonden nummer van een onderwijsdeelnemer. Zij hebben nog enkele vragen en opmerkingen.

De leden van de GroenLinks-fractie hebben kennisgenomen van het wetsvoorstel over het gebruik van pseudonimisering in het onderwijs. Zij hebben enkele vragen.

De leden van de SP-fractie hebben kennisgenomen van de wijziging van diverse onderwijswetten in verband met het pseudonimiseren van het persoonsgebonden nummer van een onderwijsdeelnemer ten behoeve

kst-34741-6
ISSN 0921 - 7371
's-Gravenhage 2017

van het bieden van voorzieningen in het kader van het onderwijs en de begeleiding van onderwijsdeelnemers. Zij hebben daar nog enkele vragen over.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het onderhavige wetsvoorstel. Zij hechten eraan dat bij de gegevensuitwisseling tussen actoren in het onderwijsveld de privacy van de deelnemers voldoende wordt gewaarborgd, zoals ook is uitgedrukt in de motie van het lid Ypma c.s., die de Kamer in 2015 heeft aangenomen.[1]

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het voorstel tot 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. Met betrekking tot dit voorstel hebben de leden van deze fractie nog op een enkel punt behoefte aan een nadere toelichting.

De leden van de SGP-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel.

1. Inleiding

1.1. Probleemanalyse

De leden van de VVD-fractie zien veel kansen voor verbetering van het onderwijs door benutting van digitalisering. Tegelijkertijd gaat digitalisering in het onderwijs gepaard met stevige privacy- en informatiebeveiligingsvraagstukken. De leden zijn dan ook te spreken over het doel van het wetsvoorstel; namelijk de uitwisseling van persoonsgegevens tussen onderwijs en leveranciers van onderwijskundige producten veiliger, betrouwbaarder en efficiënter maken. Hebben de leden van voornoemde fractie het goed begrepen dat leveranciers van digitale producten of diensten door dit wetsvoorstel van het bevoegd gezag van een onderwijsinstelling een pseudoniem (ketenID) van een leerling verstrekt kunnen krijgen dat is gegenereerd op basis van het initiële pseudoniem dat weer gegenereerd is op basis van het persoonsgebonden nummer. En betekent dit dat de school de enige partij is die direct tot de leerling herleidbare gegevens heeft, zo vragen zij.
Het wetsvoorstel maakt inderdaad mogelijk dat onderwijsinstellingen het persoonsgebonden nummer eenmalig kunnen gebruiken om een pseudoniem te genereren. Dit pseudoniem vormt de basis om voor specifieke gevallen andere pseudoniemen (ketenID's) te kunnen genereren en gebruiken, waarmee een veiliger, betrouwbaarder en meer efficiënte digitale uitwisseling van gegevens door onderwijsinstellingen met andere partijen mogelijk wordt gemaakt. Het wetsvoorstel maakt mogelijk 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 heeft tot gevolg dat het aantal persoonsgegevens dat wordt gebruikt voor de digitale uitwisseling van gegevens tot een minimum beperkt kan worden.
Aangezien onderwijsinstellingen zorgdragen voor het geven van goed onderwijs, zijn zij als verantwoordelijken in de zin van de Wet bescherming persoonsgegevens (Wbp) aan te merken. Onderwijsinstellingen zijn daarmee verantwoordelijk voor een zorgvuldige omgang met persoonsgegevens. Om goed onderwijs te kunnen bieden, maken zij gebruik van de diensten van verschillende partijen, die eraan bijdragen een goed gebruik van digitale leermiddelen mogelijk te maken. Aanbieders van schoolinfor-

[1] Kamerstuk 32 034, nr. 13.

matiesystemen (zij verzorgen onder meer de leerlingadministratie voor de onderwijsinstelling), distributeurs (zij verzorgen onder meer de toegang tot digitale leermiddelen) en educatieve uitgevers (de ontwikkelaars van digitale leermiddelen) werken hierin samen (hierna: leveranciers). Leveranciers hebben leerlinggegevens nodig om hun diensten te kunnen verlenen, maar hebben hierbij de rol van bewerker. Dit houdt in dat leveranciers altijd in opdracht en onder verantwoordelijkheid van de onderwijsinstelling handelen. Het is de onderwijsinstelling die zeggenschap heeft en houdt over wat er met de leerlinggegevens gebeurt. Dit betekent bijvoorbeeld dat een aanbieder die de leerlingadministratie verzorgt de gegevens van leerlingen weliswaar in haar systemen heeft, maar daar alleen mee mag omgaan zoals de onderwijsinstelling als verantwoordelijke dat bepaalt.

Hoe is geborgd dat deze goed beveiligd zijn, zo vragen de leden van voornoemde fractie. Zullen daar standaarden voor bestaan in zowel po als vo voordat dit wetsvoorstel van kracht wordt, zo vragen de leden van de VVD-fractie.[2] [3]
Alle partijen hebben een rol en verantwoordelijkheid bij het goed beveiligen van gegevens. Onderwijsinstellingen moeten erop kunnen vertrouwen dat persoonsgegevens op een veilige manier worden bewerkt door leveranciers. Er bestaan standaarden die leveranciers kunnen gebruiken om deze beveiliging 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. 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.
Ten aanzien van het pseudoniem en het ketenID heeft de regering een bijzondere verantwoordelijkheid, omdat dit pseudoniem op het persoonsgebonden nummer (PGN), waarvoor strenge regels gelden, is gebaseerd. Daarom zullen nadere voorwaarden over de beveiliging bij ministeriële regeling worden gesteld. Deze nadere voorwaarden borgen in ieder geval dat:
– het PGN in het administratiesysteem van de school wordt gehasht voordat dit via een versleutelde verbinding naar de Nummervoorziening wordt verstuurd;[4] [5]
– de Nummervoorziening het PGN hasht 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 versleuteld naar het leerlingadministratiesysteem wordt verstuurd;
– het pseudoniem en ketenID apart van elkaar en van andere persoonsgegevens worden opgeslagen in de leerlingadministratie;
– het pseudoniem met geen enkele andere partij wordt uitgewisseld;
– het ketenID slechts met partijen wordt uitgewisseld die digitale onderwijsdiensten aanbieden.

Bij de bouw van de Nummervoorziening en implementatie van de systematiek bij leveranciers is uitgegaan van relevante (internationale) standaarden. Zo is voor de versleuteling van de communicatie tussen systemen aangesloten bij bestaande standaarden voor veilige uitwisseling

[2] po: primair onderwijs.
[3] vo: voortgezet onderwijs.
[4] Hashing is een cryptografische functie die ervoor zorgt dat het PGN wordt omgezet in een code, die niet teruggerekend kan worden naar het PGN.
[5] De Nummervoorziening is de ICT-voorziening die de pseudonimisering technisch uitvoert. Deze voorziening wordt beheerd door Stichting Kennisnet als onderdeel van de basisinfrastructuur.

(Edukoppeling 1.2, gebaseerd op de overheidsstandaard Digikoppeling, zoals ontwikkeld door het Nationaal Cyber Security Centrum en Logius). Voor hashing is gebruik gemaakt van de standaarden zoals deze door de European Union Agency for Network and Information Security (ENISA) zijn ontwikkeld. Naast de technische kant ligt er bij onderwijsinstellingen zelf een belangrijke verantwoordelijkheid om de beveiliging van de informatie over leerlingen op orde te hebben en houden. Wanneer op onderwijsinstellingen wachtwoorden rondslingeren, of systemen niet op slot worden gezet, zijn gegevens van onderwijsdeelnemers alsnog niet veilig. Daarom is het cruciaal om te werken aan bewustwording. De sectorraden en Stichting Kennisnet ondersteunen onderwijsinstellingen op het gebied van informatiebeveiliging en privacy. Door middel van concrete producten wordt gewerkt aan de bewustwording en ondersteuning van onderwijsinstellingen op deze terreinen.

En hoe wordt op het gebruik hiervan toegezien, zo vragen de leden van voornoemde fractie.
Het is aan de onderwijsinstelling om als verantwoordelijke zich ervan te verzekeren dat de leveranciers die zij als bewerker inschakelen voldoende maatregelen hebben genomen om een passend beveiligingsniveau te realiseren. Leveranciers kunnen hiervoor gebruik maken van de beschikbare standaard (zoals hierboven is aangegeven), die hen ook in staat stelt om richting onderwijsinstellingen aan te tonen dat hun beveiligingsniveau passend is. Leveranciers kunnen ook andere methodes kiezen om dit te bereiken en daarmee aan de verplichtingen van de Wbp te voldoen. Het gebruik van de standaard heeft evenwel als voordeel voor leverancier en onderwijsinstelling dat ze zeker weten dat ze aan de vereisten voldoen en dit bevordert het overleg daarover tussen onderwijsinstelling en leverancier. Ten aanzien van de omgang met het PGN, pseudoniem en ketenID worden de kaders gesteld door dit wetsvoorstel en de daarop gebaseerde lagere regelgeving. De Autoriteit Persoonsgegevens (AP) ziet toe op de naleving van deze regelgeving.

In artikel 1A, lid 13, van het wetsvoorstel wordt de mogelijkheid gecreëerd om bij AMvB andere gevallen voor andere categorieën aan te wijzen, waarvoor een school ook een pseudoniem zou kunnen genereren. De leden van de VVD-fractie vragen of de regering een voorbeeld kan noemen van zo'n mogelijk geval en mogelijke categorie.
De wereld digitaliseert in toenemende mate. De uitwisseling van gegevens zal steeds vaker via de digitale weg verlopen. Wanneer dit het geval is, kan een ketenID een goed middel zijn om digitale uitwisseling efficiënt, veilig en met de nodige privacywaarborgen te laten plaatsvinden. Een mogelijk voorbeeld van een dergelijk geval betreft de uitwisseling van gegevens tussen onderwijsinstelling en stagebedrijf in het kader van de beroepspraktijkvorming in het middelbaar beroepsonderwijs (mbo). Dat kan bijvoorbeeld gaan over aanwezigheid of voortgang van de stage. Wanneer nut en noodzaak van dergelijke voorbeelden evident worden, voorziet het wetsvoorstel in de mogelijkheid om, na onderzoek waaruit nut en noodzaak blijken en een privacy impact assessment, bij AMvB te regelen dat hiervoor een ander pseudoniem (ketenID) gegenereerd kan worden.

De leden van voornoemde fractie vragen waarom hier geen voorhangbepaling is opgenomen.
In het wetsvoorstel is geen voorhangbepaling ten aanzien van de AMvB opgenomen. Dit is conform kabinetsbeleid, zoals neergelegd in de Aanwijzingen voor de regelgeving, waarin terughoudendheid wordt betracht bij parlementaire betrokkenheid bij gedelegeerde regelgeving. In aanwijzing 35 van de Aanwijzingen voor de regelgeving wordt aangegeven dat in een wet geen formele betrokkenheid van het parlement bij

gedelegeerde regelgeving wordt geregeld, tenzij daarvoor bijzondere redenen bestaan. In de toelichting hierbij staat dat het wenselijk is dat bij de verdeling van een regeling over de wet en algemeen verbindende voorschriften van lager niveau duidelijke keuzes worden gemaakt waarbij ofwel een onderwerp in de wet wordt geregeld, ofwel het geven van voorschriften daaromtrent wordt gedelegeerd aan een lagere regelgever. Bij voorkeur moet worden vermeden dat de vaststelling van bepaalde voorschriften aan een lagere regelgever wordt gedelegeerd en tegelijkertijd wordt vastgelegd dat het parlement bij deze regelgeving moet worden betrokken.

Het convenant platform Edu-K draagt volgens de regering bij aan de borging van de privacy van onderwijsdeelnemers, kan zij motiveren waarom dit zo is, zo vragen de leden van de VVD-fractie.
De PO-Raad, de VO-raad, de MBO Raad, de Groep Educatieve Uitgeverijen (GEU), de Vereniging Digitale Onderwijs Dienstverleners (VDOD) en de leden van de sectie Educatief van de Koninklijke Boekverkopersbond maken publiek-private afspraken in het platform Edu-K die beogen bij te dragen aan een betere borging van de privacy van onderwijsdeelnemers. In juni 2016 hebben de PO-Raad, VO-raad en brancheorganisaties leveranciers het convenant «Digitale onderwijsmiddelen en privacy 2.0» gesloten. Dit convenant heeft tot doel om waarborgen te creëren voor de zorgvuldige omgang met persoonsgegevens door onderwijsinstellingen en leveranciers die worden verwerkt in het kader van het gebruik van digitale onderwijsmiddelen. Uitgangspunt van het convenant is dat de onderwijsinstellingen, en niet de leveranciers van digitale leermiddelen, de regie hebben over wat er gebeurt met de gegevens van onderwijsdeelnemers die worden verwerkt bij het gebruik van digitale leermiddelen. Ook is in het convenant opgenomen dat onderwijsinstellingen, onder meer op basis van gegevens van aanbieders, ouders en onderwijsdeelnemers informeren over het gebruik van persoonsgegevens en hoe ouders en onderwijsdeelnemers gebruik kunnen maken van hun rechten, zoals het recht op inzage en correctie. Daarnaast is in het convenant vastgelegd dat zowel het Platform Edu-K als de AP een rol hebben bij het houden van toezicht op de naleving van het convenant en de Wbp. Het convenant (met inbegrip van de bijbehorende modelbewerkersovereenkomst) concretiseert hiermee de verplichtingen van onderwijsinstellingen en hun leveranciers die uit de Wbp voortvloeien. Voor het mbo vindt nu een verkenning plaats om tot een vergelijkbaar convenant te komen, de betrokken partijen staan hier op dit moment positief tegenover.

Deze leden van voornoemde fractie vragen waarom de andere 5% niet deelneemt en of deze overwegingen bekend zijn bij de regering.
Er zijn veel leveranciers actief om mogelijk te maken dat onderwijsinstellingen op een goede manier gebruik kunnen maken van digitale leermiddelen. De meeste leveranciers zijn aangesloten bij de brancheverenigingen: de Groep Educatieve Uitgeverijen (GEU), de Vereniging Digitale Onderwijs Dienstverleners (VDOD) en de leden van de sectie Educatief van de Koninklijke Boekverkopersbond. De regering heeft geen gedetailleerd inzicht in de overwegingen van leveranciers om niet aan te sluiten bij deze verenigingen.

Wat zijn de gevolgen voor de privacy van scholieren wanneer scholen producten afnemen bij deze 5%, zo vragen de leden van de VVD-fractie.
De wettelijke verplichtingen ten aanzien van de privacy van leerlingen gelden onverminderd voor alle partijen, of zij nu zijn aangesloten bij een branchevereniging of niet. Privacyregelgeving stelt diverse eisen ten aanzien van de omgang met persoonsgegevens. Onderwijsinstellingen en leveranciers hebben verschillende mogelijkheden om daaraan te voldoen. De Wbp kent veelal open normen (zoals dataminimalisatie, doelbinding,

passende beveiliging), waar via verschillende wegen invullling aan gegeven kan worden. Wanneer leveranciers andere keuzes maken bij de ontwikkeling van hun producten of diensten, mag de privacy van leerlingen daar niet onder lijden.

De leden van voornoemde fractie vragen of de regering heeft overwogen om deelname aan dit convenant verplicht te stellen in dit wetsvoorstel en of zij dit kan motiveren.
Aangezien (de bevoegd gezagen van) onderwijsinstellingen de zorg dragen voor het geven van goed onderwijs, zijn zij als verantwoordelijken in de zin van de Wbp aan te merken. Dit betekent dat op onderwijsinstellingen de verplichting rust om de Wbp na te leven. De PO-Raad en VO-raad hebben namens de bevoegd gezagen het convenant met brancheverenigingen van leveranciers gesloten. Deze partijen spannen zich de laatste jaren stevig en op vele manieren in om door middel van zelfregulering de privacy van leerlingen te borgen. Het wetsvoorstel ondersteunt deze zelfregulering door onderwijsinstellingen in staat te stellen een ketenID te hanteren als zij gegevens uitwisselen met andere partijen. Het wetsvoorstel heeft niet tot doel nadere verplichtingen te stellen ten aanzien van onderwijsinstellingen of leveranciers. Uiteraard ontslaat hen dit niet van de plicht om de privacy van leerlingen te waarborgen. Tegelijkertijd kunnen leveranciers ook zonder deel te nemen aan het convenant wel voldoen aan de eisen die de Wbp aan hen stelt, doordat de leverancier zelf andere maatregelen heeft getroffen om de persoonsgegevens van leerlingen voldoende te beschermen. De regering onderkent dat de keuze voor zelfregulering op gespannen voet kan staan met het doel van het voorstel om bij de uitwisseling zo min mogelijk persoonsgegevens te gebruiken. Om aan deze zorg tegemoet te komen, is het wetsvoorstel voorzien van een evaluatiebepaling, die inhoudt dat de regering binnen vijf jaar na de inwerkingtreding van deze wet aan de Staten-Generaal verslag uitbrengt over de doeltreffendheid en de effecten van deze wet in de praktijk.

De leden van de VVD-fractie vragen wat de daadwerkelijke invloed van onderwijsdeelnemers en ouders is en of de regering dit kan toelichten.
De rechten van onderwijsdeelnemers en hun ouders ten aanzien van het gebruik van persoonsgegevens door onderwijsinstellingen zijn vastgelegd in de Wbp. Zo hebben zij het recht om geïnformeerd te worden en het recht op inzage en correctie van persoonsgegevens. Daarnaast heeft de medezeggenschapsraad, waarin ouders deelnemen, instemmingsrecht op de privacyreglementen die onderwijsinstellingen vaststellen.

Dezelfde leden vragen in hoeverre een onderwijsdeelnemer zelf kan beslissen welke gegevens vrij worden gegeven samen met het ketenID, bijvoorbeeld door zelf te kunnen bepalen of het geslacht bekend wordt via de ketenID bij de leverancier.
Voor het bieden van goed onderwijs is het nodig dat onderwijsinstellingen over gegevens van leerlingen beschikken. Onderwijsinstellingen hebben eigen ambities en visies op goed onderwijs, waardoor zij ook verschillende keuzes maken op het gebied van (digitale) leermiddelen en de persoonsgegevens van leerlingen die zij daarvoor gebruiken. Het is aan de onderwijsinstelling als verantwoordelijke om in goed overleg met de ouders en de medezeggenschapsraad te treden en een zorgvuldige afweging te maken over welke persoonsgegevens zij van onderwijsdeelnemers ter beschikking stelt en voor welke doeleinden. Wanneer een individuele onderwijsdeelnemer (of zijn wettelijk vertegenwoordiger wanneer hij de leeftijd van 16 jaar nog niet heeft bereikt) zich hier niet in kan vinden, heeft hij op grond van artikel 40 van de Wbp het recht om hiertegen verzet aan te tekenen.

En zijn hier verschillen tussen de verschillende onderwijsniveaus, zo vragen de leden van voornoemde fractie.
Er zijn hierbij geen verschillen tussen de verschillende onderwijsniveaus. Het feit dat een ouder (of voogd) optreedt namens een minderjarige onderwijsdeelnemer maakt geen verschil voor de rechten en plichten die onderwijsdeelnemers en onderwijsinstellingen hebben.

Tevens vragen deze leden of er ook wordt vastgelegd dat dit duidelijk gecommuniceerd dient te worden naar de onderwijsdeelnemers en ouders.
De onderwijsinstelling is de verantwoordelijke en maakt vanuit haar eigen ambities en visie op goed onderwijs, en in goed overleg met ouders en de medezeggenschapsraad, een zorgvuldige afweging over de persoonsgegevens die zij van onderwijsdeelnemers ter beschikking stelt en voor welke doeleinden. Deze verplichtingen zijn vastgelegd in bestaande regelgeving ten aanzien van de privacy en medezeggenschap binnen onderwijsinstellingen en nader geconcretiseerd in het convenant. De regering acht de bestaande verplichtingen voldoende en voegt daar met onderhavig wetsvoorstel geen nieuwe verplichtingen aan toe.

De voornoemde leden vragen wat de motivatie is om deze verantwoordelijkheid bij de scholen neer te leggen.
De verantwoordelijkheid voor een zorgvuldige omgang met persoonsgegevens ligt reeds bij onderwijsinstellingen. De regering beoogt met het wetsvoorstel onderwijsinstellingen te ondersteunen bij het invullen van deze verantwoordelijkheid.

De leden van de D66-fractie vragen de regering het beleid rondom digitale leermiddelen nader toe te lichten.
Het is aan onderwijsinstellingen zelf om de keuze te maken of en zo ja welke digitale leermiddelen ingezet worden. Het beleid rondom digitale leermiddelen is erop gericht die keuzevrijheid voor leraren en instellingen te ondersteunen en de randvoorwaarden op landelijk niveau op orde te hebben en te houden. Het gaat dan op hoofdlijnen om:
– het ontwikkelen en beheren van de noodzakelijke afspraken en standaarden tussen leveranciers en het onderwijs;
– ondersteuning op sectorale vraagstukken als privacy en beveiliging, connectiviteit en professionalisering;
– financiering van Stichting Kennisnet om de landelijke ondersteuning op ict-randvoorwaarden voor onderwijsinstellingen vorm te geven;
– het via Wikiwijsleermiddelenplein stimuleren van het delen, arrangeren en hergebruiken van open leermiddelen;
– het stimuleren van onderzoek naar een effectief gebruik van digitale leermiddelen;
– naast de activiteiten op de randvoorwaarden stimuleert het Doorbraakproject Onderwijs en ICT ook tijdelijk actief het gebruik van digitale leermiddelen in de klas, vanuit de vragen die onderwijsinstellingen hierover hebben.

Worden licenties met leveranciers altijd op het niveau van onderwijsinstelling of onderwijsdeelnemer afgesloten, zo vragen de leden van voornoemde fractie.
In het primair en voortgezet onderwijs worden licenties met leveranciers vrijwel altijd op niveau van de onderwijsinstelling afgesloten. In het middelbaar beroepsonderwijs vrijwel altijd op niveau van de student.

De leden van de D66-fractie vragen of er inkoopvoordeel is te halen door op stelselniveau inkoop te regelen en wat de voor- en nadelen hiervan zijn.

Binnen het Doorbraakproject Onderwijs en ICT wordt op dit moment verkend welke voor- en nadelen er zijn als schoolbesturen op stelselniveau gezamenlijk leermiddelen zouden inkopen. Vooruitlopend op de exacte uitkomsten hiervan, zijn er in ieder geval voordelen te behalen in het afdwingen van de voorwaarden waaronder leermiddelen geleverd worden. Denk aan de gewenste standaarden op het vlak van privacy, beveiliging, toegang en het metadateren van materiaal of aan de gewenste flexibiliteit in licentievormen. De professionaliteit van het gehele inkoopproces en de aanbestedingen kunnen worden verbeterd door de beschikbare kennis centraal te organiseren. Scholen kunnen ontzorgd worden op zaken als contractmanagement. Wellicht is er ook prijsvoordeel te behalen, maar daar staat tegenover dat centrale inkoop kan leiden tot meer uniformiteit en daarmee verschraling van het aanbod. Ook zal er goed gekeken worden naar risico's op marktverstoring.

De leden van voornoemde fractie vragen wie de eigenaar is van de data gegenereerd door digitale leermiddelen.
De onderwijsdeelnemer is degene op wie de persoonsgegevens betrekking hebben en is de enige die blijvend over deze gegevens moet kunnen beschikken. De onderwijsinstelling is de verantwoordelijke die – binnen de geldende wettelijke termijnen – over de gegevens mag beschikken voor het bieden van goed onderwijs.

Kunnen gebruikers van de digitale leermiddelen hun «leerdata» makkelijk overbrengen naar een andere leverancier, zo vragen de leden van voornoemde fractie.
Voor het overbrengen van «leerdata» is de open UWLR-standaard (Uitwisseling Leerlinggegevens en Resultaten)ontwikkeld. Steeds meer leveranciers maken van deze standaard gebruik. Per 25 mei 2018 wordt de Algemene verordening gegevensbescherming van toepassing, waarin het recht op dataportabiliteit is vastgelegd. Een pseudoniem maakt het voor onderwijsdeelnemers eenvoudiger om hun gegevens mee te nemen wanneer zij van school wisselen.

Welke mogelijkheden hebben leveranciers om data van onderwijsdeelnemers, bijvoorbeeld over hoe mensen leren, te delen met derden, zo vragen de voornoemde leden.
Leveranciers hebben daar zelf geen mogelijkheden toe. Zij kunnen alleen data van onderwijsdeelnemers met derden delen wanneer dat in opdracht en onder verantwoordelijkheid van de onderwijsinstelling gebeurt.

De leden van de GroenLinks-fractie merken op dat het convenant Digitale Onderwijsmiddelen en Privacy 2.0 is ondertekend door de brancheverenigingen van primaire onderwijs, voortgezet onderwijs en middelbaar beroepsonderwijs en de Groep Educatieve Uitgeverijen en Vereniging Digitale Onderwijs Dienstverleners. Is de regering voornemens om bij de ontwikkeling van het pseudoniem op basis van het BSN-nummer samen op te trekken met het platform dat dit convenant ondersteunt, zo vragen de leden.
Ja, het is uitdrukkelijk de intentie van zowel de regering als het platform om hier gezamenlijk in op te trekken. In het huidige convenant is de intentie neergelegd dat onderwijsinstellingen en leveranciers gebruik maken van gepseudonimiseerde leerlinggegevens wanneer dat mogelijk is. Samen met het platform is deze intentie nader geconcretiseerd in nadere afspraken over de invoering van het pseudoniem.

1.2. Privacy en digitale onderwijsmiddelen: onderwijsinstellingen voeren de regie

De leden van de CDA-fractie vragen de regering wat de reden is om verschillende partijen een rol te geven bij het houden van toezicht op de verstrekking van de gegevens. Deze leden lezen dat zowel de Inspectie van het Onderwijs, de AP en het Platform Edu-K hun eigen rol hebben hierbij. Graag ontvangen de leden van voornoemde fractie een nadere toelichting en vragen zij tevens of dit voor de betrokken instellingen ook extra administratieve lastendruk oplevert.
De AP is de instantie die toezicht houdt op de naleving van de Wbp en de verplichtingen die daaruit voortvloeien. De Inspectie van het Onderwijs houdt toezicht op onderwijsinstellingen. Beide organisaties hebben onderling een samenwerkingsovereenkomst afgesloten, waarin het volgende is afgesproken:

– de AP informeert de inspectie wanneer zij van plan is onderzoek te doen naar hoe een onderwijsinstelling de Wbp naleeft;
– de inspectie en de AP informeren elkaar desgevraagd over alles wat relevant kan zijn voor hun taken;
– als iemand bij het loket van de inspectie melding maakt van mogelijke overtreding van de Wbp, verwijst de inspectie de melder door naar de AP;
– krijgt de inspectie signalen (door derden of vanuit eigen waarneming) over mogelijke schendingen van de Wbp door onderwijsinstellingen, dan geeft de inspectie die meteen door aan de AP. Het toezicht op verwerking van persoonsgegevens blijft ook in die gevallen bij de AP berusten.

Het convenant bevat een concretisering van de Wbp en nadere afspraken tussen onderwijsinstellingen en leveranciers om een zorgvuldige omgang met persoonsgegevens te borgen. Het platform Edu-K ziet toe op de naleving van deze afspraken door middel van onderlinge werkafspraken. Gezamenlijk zorgen deze partijen voor een goede naleving van alle geldende wettelijke verplichtingen en gemaakte afspraken om een zorgvuldige omgang met persoonsgegevens te garanderen en vindt onderlinge afstemming plaats, zodat onderwijsinstellingen hier geen aanvullende administratieve last van ondervinden.

1.3. Pseudoniem maakt verdere dataminimalisatie mogelijk

De leden van de GroenLinks-fractie delen het uitgangspunt van dataminimalisatie. Zij vragen de regering daarom of de toename in gebruiksvriendelijkheid – die bijvoorbeeld verkregen zou worden bij het delen van de voornaam – opweegt tegen het grotere risico van koppelbaarheid van gegevens.
De toename in gebruiksvriendelijkheid weegt op tegen het risico van koppelbaarheid van gegevens. De vertegenwoordigers van onderwijsinstellingen en leveranciers hebben in het platform Edu-K afgesproken welke aanvullende gegevens gebruikt kunnen worden tussen onderwijsinstellingen en private partijen voor de toegang tot en het gebruik van digitale leermiddelen en toetsen (de standaardattributenset). Het gaat om gegevens zoals de voornaam van de onderwijsdeelnemer, in welke groep de onderwijsdeelnemer onderwijs volgt en leerresultaten (zoals de score van een toets die de deelnemer heeft gemaakt). Deze standaardattributenset is juridisch getoetst en voldoet aan het vereiste van doelbinding; de gegevens die erin zijn opgenomen zijn nodig voor het goed laten functioneren van digitale onderwijsmiddelen.[6] Zonder deze gegevens kan de leraar in de klas geen digitale leermiddelen gebruiken.

[6] https://www.edu-k.nl/s/Juridische-toets-attributenbeleid.pdf.

De voornoemde leden vragen de regering dan ook of zij overwogen heeft artikelen aangaande het delen van aanvullende gegevens in de wet op te nemen en zo ja, wat haar afwegingen waren dit toch niet op te nemen.
De standaardattributenset geeft de onderwijsinstelling heldere richtlijnen en biedt haar tegelijkertijd de ruimte om daar in voorkomend geval gemotiveerd van af te kunnen wijken. Het reguleren van het delen van aanvullende gegevens zou deze ruimte wegnemen, terwijl deze wel gewenst is. Een aanbieder van digitale leermiddelen kan bijvoorbeeld een adaptief leermiddel ontwikkelen waarbij ook de geboortedatum van een leerling wordt gebruikt, omdat daarmee op een goede manier kan worden ingespeeld op verschillen tussen vroege en late leerlingen. Juist in dit soort gevallen is het belangrijk dat de onderwijsinstelling als verantwoordelijke, vanuit haar eigen ambities en visie op goed onderwijs, en in goed overleg met de ouders en de medezeggenschapsraad, een zorgvuldige afweging maakt over de persoonsgegevens die zij van hun onderwijsdeelnemers ter beschikking stelt en voor welke doeleinden.

De leden de GroenLinks-fractie vragen de regering welke (juridische) middelen Edu-K heeft om dit attributenbeleid op te leggen en scholen die te veel gegevens delen tot de orde te roepen.
Edu-K heeft geen middelen om het attributenbeleid op te leggen. Het attributenbeleid is een standaard die heldere richtlijnen biedt over de gegevens die uitgewisseld kunnen worden voor het gebruik van digitale leermiddelen. Onderwijsinstellingen kunnen hier beredeneerd en gemotiveerd van afwijken, wanneer dat nodig is. Wanneer onderwijsinstellingen zonder goede redenen meer gegevens delen dan noodzakelijk, is de AP de instantie die handhavend kan optreden.

De leden van de SGP-fractie constateren dat door het beperken van data de risico's voor betrokkenen zouden moeten verminderen. Het is bijvoorbeeld niet langer nodig om namen en geboortedata uit te wisselen. Tegelijkertijd lezen zij dat in de praktijk nog steeds gebruik gemaakt zal worden van voornamen en een aanduiding van de groep van de leerling. Deze leden vragen in hoeverre in een dergelijke situatie daadwerkelijk sprake is van dataminimalisatie.
Er is sprake van dataminimalisatie indien er niet meer gegevens worden gebruikt dan noodzakelijk is voor het te bereiken doel. Uit de eerder genoemde juridische analyse is gebleken dat de gegevens die in de standaardattributenset zijn opgenomen voldoen aan het vereiste van doelbinding; hiermee wordt dataminimalisatie bereikt. Scholen en leveranciers wisselen op dit moment meer gegevens uit dan de gegevens uit de standaardattributenset. Met de introductie van het pseudoniem, ketenID en de standaardattributenset zal het aantal gegevens worden teruggebracht.

Is het risico niet groot dat, zeker in het basisonderwijs, op basis van voornaam en groep de identiteit van leerlingen redelijk eenvoudig te herleiden kan zijn, zo vragen de leden van voornoemde fractie.
De kans bestaat dat op basis van de voornaam en groep de identiteit van leerlingen te herleiden is. Om ervoor te zorgen dat dit alleen door bevoegde personen gebeurt, maken onderwijsinstellingen afspraken met leveranciers over het gebruik en de beveiliging van gegevens. Het risico op onbevoegde identificatie van leerlingen wordt daarmee tot een minimum beperkt. Het pseudoniem maakt verdere dataminimalisatie mogelijk, het aantal noodzakelijke persoonsgegevens dat met leveranciers wordt uitgewisseld wordt daarmee teruggebracht. Dit draagt eraan bij dat de kans op identificatie afneemt. 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.

Kan de regering toelichten waarom andere alternatieven dan het gebruik van de voornaam niet werkbaar zijn voor een adequaat gebruik van de systemen, zo vragen de voornoemde leden.
Wanneer leraren digitale leermiddelen in de klas gebruiken, is het nodig dat zij weten om welke leerling het gaat die werkt met deze leermiddelen. Daarvoor is de voornaam van deze leerling nodig. Onderzochte alternatieven, zoals gebruikersnamen, zijn bewerkelijk en dermate ingewikkeld voor docenten om bij te houden, dat dit voor hen in de praktijk niet werkbaar is.

1.4. Nut en noodzaak wetsvoorstel

De leden van de D66-fractie vragen de regering nader toe te lichten in hoeverre het mogelijk is voor onderwijsdeelnemers (of ouders van onderwijsdeelnemers) om inzicht te verkrijgen in de studie- en gedragsgegevens die van hen zijn opgeslagen en met wie de gegevens gedeeld zijn. De Wbp geeft onderwijsdeelnemers of hun ouders het recht op inzage van persoonsgegevens. Zodra van dit recht gebruik gemaakt wordt, moet de onderwijsinstelling duidelijk maken om welke gegevens het gaat, wat het doel is van het gebruik, aan wie de organisatie de gegevens eventueel heeft verstrekt en wat de herkomst is van deze gegevens. Er komen in toenemende mate producten en diensten die onderwijsinstellingen helpen dit voor ouders inzichtelijk te maken, zoals ouderportalen.

Kan de regering uiteenzetten welke wettelijke restricties bestaan ten aanzien van de groepen personen die inzicht hebben in de onderwijs- en gedragsgegevens van onderwijsdeelnemers, zo vragen de leden van voornoemde fractie.
De Wbp schrijft voor dat persoonsgegevens op zorgvuldige wijze moeten en alleen voor heldere en gerechtvaardige doeleinden mogen worden verwerkt. Ten aanzien van de groepen personen die inzicht hebben in de onderwijs- en gedragsgegevens van onderwijsdeelnemers betekent dit dat binnen het onderwijs alleen diegenen hiervan kennis mogen nemen, voor wie het noodzakelijk is dat zij dit inzicht hebben voor het kunnen verzorgen van goed onderwijs. Wanneer onderwijsinstellingen vanuit hun rol als verantwoordelijke een bewerker inschakelen voor het leveren van diensten of producten waarvoor het verwerken van leerlinggegevens noodzakelijk is, geldt dat zij goede afspraken moeten maken die eveneens waarborgen dat gegevens niet voor meer personen inzichtelijk zijn dan noodzakelijk. Het kan niet zo zijn dat functionarissen inzicht krijgen in leerlinggegevens, wanneer dat niet noodzakelijk is voor het vervullen van hun taak.

2. Doel van het wetsvoorstel

2.1. Doel

Het lijkt de leden van de VVD-fractie duidelijk dat het thema privacy in het onderwijs aandacht verdient. Veel partijen hebben toegang nodig tot de gegevens van de onderwijsdeelnemers. Zij zouden graag weten of en welke eisen er gesteld worden aan softwareproducenten en andere leveranciers wanneer zij een ketenID en gegevens krijgen.
De regering heeft een bijzondere verantwoordelijkheid voor het genereren en gebruiken van pseudoniemen, omdat deze hun oorsprong vinden in het PGN; het gebruik van dit nummer is aan strenge wettelijke regels gebonden. De regering wil voorkomen dat pseudoniemen of ketenID's alsnog herleid kunnen worden tot het PGN, of dat een pseudoniem of ketenID de facto een nieuw PGN zou worden. Daarvoor is het nodig nadere voorwaarden te stellen ten aanzien van de beveiliging en het gebruik van pseudoniemen te beperken, door zowel de categorieën van

ontvangers van het pseudoniem te limiteren, als grenzen te stellen aan hoe lang het pseudoniem gebruikt mag worden (duur van het pseudoniem). Voor de beveiligingseisen wordt aangesloten bij de standaard voor informatiebeveiliging, het certificeringsschema informatiebeveiliging en privacy ROSA. Zie voor de concrete maatregelen de beantwoording van de vraag van de leden van de VVD-fractie over de beveiliging van gegevens in paragraaf 1.1.

Zijn de eisen die gesteld zijn aan de informatiebeveiliging voldoende, zo vragen de leden van voornoemde fractie. De eerder genoemde leden zouden graag een motivatie zien met betrekking tot het feit dat ondanks de grote verschillen in onderwijsvormen, er geen onderscheid gemaakt wordt in dit wetsvoorstel tussen de onderwijsvormen.
Om in adequate beveiligingsvoorschriften te voorzien, worden bij ministeriële regeling nadere voorwaarden gesteld ten aanzien van de beveiliging, waaronder gescheiden opslag van het PGN, het pseudoniem en het ketenID. Deze voorwaarden zullen naar verwachting dikwijls wijzigen, omdat zij sterk samenhangen met de snel voortschrijdende ontwikkelingen in de techniek. Daarom voorziet het wetsvoorstel in een grondslag voor een ministeriële regeling voor deze voorwaarden, waarmee de nodige flexibiliteit geboden kan worden. De eisen ten aanzien van de beveiliging van het PGN, pseudoniem en ketenID zijn voldoende en generiek, omdat hier geen verschillen tussen de onderwijssectoren bestaan. Voor wat betreft de aanvullende gegevens zijn de verschillen tussen onderwijssectoren wel relevant. Aan de verschillen tussen onderwijsvormen, zoals de rol van ouders, wordt recht gedaan in bestaande regelgeving op het gebied van privacy en medezeggenschap. Zo kunnen ouders voor de rechten van hun kind opkomen wanneer deze de leeftijd van 16 jaar nog niet heeft bereikt (voortvloeiend uit de Wbp) en hebben ouders op grond van de Wet op de medezeggenschap en een positie in de medezeggenschapsraad in het po en vo. Voor het mbo geldt dat in de Wet educatie en beroepsonderwijs is geregeld dat ouders op grond van artikel 8a.1.3 op verzoek van ten minste 25 ouders van deelnemers van een regionaal opleidingscentrum een ouderraad kunnen instellen en aan de agrarisch opleidingscentrum is een ouderraad verbonden. Omdat de bestaande regelgeving voldoende tegemoet komt aan de verschillen in onderwijsvormen acht de regering het niet nodig om in het onderhavig wetsvoorstel aanvullend te differentiëren.

Daarnaast wordt er in het hoger onderwijs al veel gebruik gemaakt van een studentnummer, waarom is met deze verschillen niet meer rekening gehouden in het wetsvoorstel, zo vragen de eerdergenoemde leden.
Binnen elke onderwijssector zijn er diverse manieren om tot identificatie van onderwijsdeelnemers te komen, zoals een studentnummer, dat in wezen als pseudoniem is aan te merken. Het wetsvoorstel maakt het mogelijk pseudoniemen te baseren op het persoonsgebonden nummer. Dit heeft belangrijke voordelen:
– het PGN is al een geverifieerde identiteit: dit garandeert een kwalitatief hoogwaardige identiteitsverzameling en voorkomt dat er een tweede systematiek naast het PGN moet worden opgetuigd;
– door het PGN als basis te gebruiken voor het pseudoniem is hetzelfde pseudoniem voor dezelfde onderwijsdeelnemer te genereren. Dit leidt tot de noodzakelijke persistentie van deze identiteit en van de ketenID's die erop gebaseerd worden. Dit maakt het bijvoorbeeld mogelijk dat onderwijsdeelnemers hun leermiddelen gemakkelijk kunnen meenemen als zij van onderwijsinstelling wisselen.

2.2. Bescherming persoonsgegevens

De leden van de VVD-fractie merken op dat het wetsvoorstel voorziet in een behoefte om minder gevoelige persoonsgegevens te delen. Onderwijsinstellingen zijn echter nog steeds verantwoordelijk voor de gegevens. Mocht een contractuele relatie met een leverancier echter stoppen, dan zijn de leveranciers verantwoordelijk voor het verwijderen van de gegevens inclusief de ketenID's. De leden vragen hoe de regering hier naar kijkt en of er een risico ontstaat voor de veiligheid van gegevens als een leverancier niet tot verwijdering overgaat. Hoe kan controle hierop plaatsvinden zo vragen de leden van voornoemde fractie.
De afspraken die onderwijsinstellingen met leveranciers maken gaan ook over de verwijdering van persoonsgegevens wanneer de contractuele relatie wordt verbroken, of wanneer de wettelijke bewaartermijn van gegevens is bereikt. De AP is de instantie die toezicht houdt op het naleven van de regelgeving op dit punt en kan haar bevoegdheden aanwenden wanneer leveranciers zich hier niet aan houden.

De leden van de VVD-fractie vragen of een praktische/technische oplossing denkbaar is, waarmee gegevens niet meer bruikbaar zijn als de contractrelatie is beëindigd.
Leveranciers hebben binnen hun eigen systemen en werkwijzes hier verschillende oplossingen voor ontwikkeld. Belangrijk is dat schoolbesturen met leveranciers afspraken maken over het bewaren, archiveren en vernietigen van gegevens en deze in overeenkomsten vastleggen. Na het beëindigen van de overeenkomst is de leverancier, als bewerker voor de school, verplicht om alle persoonsgegevens te (laten) vernietigen of over te dragen aan de school. In het privacyconvenant is afgesproken dat leveranciers een bevestiging sturen na afloop van de overeenkomst dat de persoonsgegevens zijn vernietigd.

De leden van de D66-fractie constateren dat leveranciers gehouden zijn om pseudoniemen op een zodanig beveiligde manier in hun administratie te bewaren, dat er geen koppeling kan plaatsvinden met gegevenssets van onderwijsdeelnemers die voor andere doeleinden zijn verkregen. Zij vragen of de regering nader kan toelichten welke veiligheidseisen gesteld worden.
De beveiligingseisen zullen bij ministeriële regeling worden vastgesteld en uitgaan van de standaard voor informatiebeveiliging, het certificeringsschema informatiebeveiliging en privacy ROSA. Daarbij zullen in ieder geval het pseudoniem en de ketenID's zowel gescheiden van elkaar als gescheiden van de (ten opzichte van het pseudoniem) aanvullende persoonsgegevens van de onderwijsdeelnemer worden bewaard, zoals vereist op grond van de Algemene verordening gegevensbescherming. Hiermee wordt het risico op koppelbaarheid tot een minimum beperkt. Zie hiervoor ook de beantwoording van de vraag van de leden van de VVD-fractie over de beveiliging van gegevens in paragraaf 1.1.

2.3. Reikwijdte van pseudoniemen

De leden van de VVD-fractie nemen kennis van het feit dat er scholen zijn die gegronde redenen zouden hebben om geen gebruik te maken van ketenID, maar de regering noemt één voorbeeld. Zijn er nog andere meer principiële redenen om niet deel te nemen, zo vragen deze leden.
Een onderwijsinstelling zal in het algemeen haar toegang en gebruik van digitale leermiddelen zo goed mogelijk willen regelen, met zo min mogelijk administratieve rompslomp. Principiële redenen om dat niet met een ketenID te willen doen, zijn de regering niet bekend.

De leden van voornoemde fractie vragen op hoeveel procent van de scholen in de verschillende sectoren de regering verwacht dat er geen gebruik van wordt gemaakt.
Het gebruik van het ketenID is opgenomen als uitgangspunt in het privacyconvenant. Het streven is dan ook om alle scholen gebruik te laten maken van het ketenID. Hoewel niet alle leveranciers zijn aangesloten bij de brancheorganisaties die het privacyconvenant hebben ondertekend, kunnen deze leveranciers ook gebruik maken van het ketenID. Het programma dat zorgt voor de implementatie van het ketenID spant zich in om alle relevante partijen hierop aan te sluiten.

Betekent het dat scholen die niet voor pseudonimisering kiezen in de toekomst waarschijnlijk minder goed met leveranciers kunnen samenwerken, omdat het pseudoniem de standaard zal worden, zo vragen de leden van voornoemde fractie.
Een school kan met iedereen blijven samenwerken die binnen de wettelijke kaders opereert. Een school die niet voor de standaard pseudonimisering kiest, is zelf verantwoordelijk voor het regelen van een vergelijkbaar alternatief. De kans is dan wel aanwezig dat dat gepaard gaat met meer administratieve lasten en minder gebruiksvriendelijkheid.

Hoe zorgen we ervoor dat het niet verplichten van het pseudoniem er niet toe leidt dat leerlingen benadeeld worden doordat hun school minder gebruik kan maken van digitale leermiddelen, zo vragen de leden van de VVD-fractie.
Alle scholen kunnen gebruik blijven maken van digitale leermiddelen. Invoering van het pseudoniem zorgt ervoor dat de huidige leveranciers van digitaal leermateriaal met minder persoonsgegevens van leerlingen toekunnen en op een efficiëntere manier gegevens kunnen uitwisselen. Door het pseudoniem niet te verplichten, houden leveranciers en onderwijsinstellingen de ruimte om op andere manieren hetzelfde doel te bereiken. Door andere werkwijzen niet uit te sluiten, worden geen onnodige drempels opgeworpen voor nieuwe, innovatieve toetreders. Ook worden bestaande leveranciers die al een vergelijkbaar alternatief hebben ontwikkeld, niet gedwongen om onnodige kosten te maken. Het niet verplichtende karakter van dit wetsvoorstel zorgt er daarmee voor dat de verdergaande digitalisering van het onderwijs niet onnodig geremd wordt.

De leden van voornoemde fractie vragen tevens hoe de regering de bescherming van persoonsgegevens borgt op scholen die niet werken met het pseudoniem.
Een school kan goede redenen hebben om geen gebruik te maken van een pseudoniem/ketenID, bijvoorbeeld omdat de school zelf al andere maatregelen heeft getroffen om persoonsgegevens van leerlingen te beschermen. De eisen die de Wbp stelt aan een zorgvuldige omgang met persoonsgegevens gelden ook in dat geval onverkort.
Op grond van de evaluatiebepaling in het wetsvoorstel zal binnen vijf jaar na inwerkingtreding onder meer worden onderzocht of ook de onderwijsinstellingen die niet werken met een pseudoniem, de Wbp voldoende in acht nemen. Mocht deze 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 van de aanvullende persoonsgegevens die mogen worden verstrekt.

Komen er standaarden voor anonimisering en worden deze wel verplicht, zo vragen de leden van de VVD-fractie en zo nee, waarom niet vragen deze leden.

De mogelijkheid van anonimisering voor de toegang tot en het gebruik van digitale leermiddelen is onderzocht. Bij anonimisering is de onderwijsdeelnemer bij elke inlogsessie echter weer een onbekende, waardoor het onmogelijk is om leervorderingen bij te houden. Om maatwerk te realiseren met behulp van adaptieve digitale leermiddelen, is het noodzakelijk dat de leermiddelen de onderwijsdeelnemers over een bepaalde periode kunnen herkennen. Anonimisering is daarom geen geschikt alternatief gebleken.

Tot slot vragen de leden van voornoemde fractie hoe ouders worden geïnformeerd over de vraag of een school de gegevens van hun kind geanonimiseerd met derden deelt en daar wel of niet een pseudoniem voor gebruikt.
Wanneer de onderwijsdeelnemer jonger dan 16 jaar is, hebben ouders op basis van de Wbp het recht op inzage van de persoonsgegevens van hun kind. Wanneer ouders daarnaar vragen, dient de onderwijsinstelling inzichtelijk te maken welke gegevens zij met welke partijen deelt. De onderwijsinstelling betrekt de medezeggenschapsraad bij de afwegingen die gemaakt worden om wel of niet persoonsgegevens te delen met leveranciers, bijvoorbeeld in een privacyreglement. Overigens wordt met dit wetsvoorstel ook geregeld welke partijen over een pseudoniem mogen beschikken, de onderwijsinstelling kan dus slechts voor uitwisseling met deze partijen een pseudoniem gebruiken.

De leden van de GroenLinks-fractie vragen de regering hoe tot op heden werd omgegaan met privacy en het aanbieden van digitale leermiddelen en toetsen.
Tot op heden is er voor de toegang tot en het gebruik van digitale leermiddelen en toetsen veelal gebruik gemaakt van leerlinggegevens, zodat leveranciers weten dat ze het over dezelfde leerling hebben. Deze systematiek is niet alleen gevoelig voor fouten, maar leidt er bovendien toe dat meer leerlinggegevens worden uitgewisseld dan strikt noodzakelijk hetgeen op gespannen voet staat met de Wbp. De invoering van een pseudoniem en ketenID brengt een verbetering op beide punten teweeg.

Tevens vragen deze leden of er in het verleden persoonsgegevens van leerlingen openbaar zijn geworden door gebrekkige beveiliging bij de uitgevers van digitale onderwijsmiddelen.
Daarvan zijn bij de regering geen voorbeelden bekend. Wel heeft in de zomer van 2016 een hack plaatsgevonden bij Edu-IX. Dit systeem fungeert als schoolportaal dat leerlingen in Nederland toegang biedt tot digitaal leermateriaal in opdracht van leveranciers van digitale leermiddelen, zoals Iddink en Van Dijk. Het incident is gemeld bij de AP en bij de politie, die na onderzoek heeft geconcludeerd dat er geen veiligheidsrisico voor de privacy van leerlingen is opgetreden.

De leden van de SP-fractie vragen hoeveel onderwijsinstellingen er in Nederland zijn die zelf al andere maatregelen hebben getroffen om persoonsgegevens te beschermen in plaats van pseudonimisering en het hanteren van een ketenID. En op welke wijze geven deze onderwijsinstellingen de bescherming van persoonsgegevens van hun leerlingen/studenten op dit moment vorm, zo vragen deze leden.
Het is niet te zeggen hoeveel onderwijsinstellingen maatregelen hebben getroffen die vergelijkbaar zijn met het hanteren van een ketenID en hoe deze maatregelen eruit zien. Onderwijsinstellingen maken hier met hun leveranciers afspraken over om dit voor de instellingen op een goede manier te regelen. De pseudonimisering in de vorm van het ketenID standaardiseert dit voor leveranciers en instellingen. De invoering van het ketenID is niet de enige maatregel die wordt getroffen om persoonsgegevens te beschermen. Ook de uitvoering van het privacyconvenant en de

maatregelen met betrekking tot de beveiliging van gegevens dragen daaraan bij.

Acht de regering het wenselijk dat er straks meerdere vormen van bescherming van persoonsgegevens ontstaan, zo vragen de leden van de SP-fractie. Deze leden vragen of de regering haar antwoord kan toelichten. Het is belangrijk dat persoonsgegevens van leerlingen veilig en goed beschermd zijn. In de Wbp zijn hier open normen voor geformuleerd, mede gelet op het feit dat er verschillende manieren zijn om dit te bereiken en de technologische ontwikkelingen op dit gebied snel voortschrijden. De regering draagt met dit wetsvoorstel bij aan standaardisering en daarmee aan een efficiënter functionerende digitale leermiddelenketen en verbetering van de privacy voor leerlingen. Door andere werkwijzen die hetzelfde doel bereiken niet uit te sluiten, worden geen onnodige drempels opgeworpen voor nieuwe, innovatieve toetreders. Ook worden bestaande leveranciers die al een vergelijkbaar alternatief hebben ontwikkeld, niet gedwongen om onnodige kosten te maken.

Wat zijn de gevolgen voor deze onderwijsinstellingen mochten zij verplicht worden tot pseudonimisering van het persoonsgebonden nummer van onderwijsdeelnemers en het hanteren van een ketenID, zo vragen de leden van voornoemde fractie.
Voor deze onderwijsinstellingen geldt dat zij onnodige kosten zouden moeten maken om een pseudoniem en ketenID in te voeren, aangezien zij al op andere manieren hetzelfde doel bereiken. Verder kan dit voor onderwijsinstellingen betekenen dat zij geen diensten of producten van andere partijen kunnen afnemen die niet met een ketenID werken. Zoals bij grote, internationale aanbieders, die op basis van internationale standaarden de privacy en beveiliging van leerlinggegevens borgen.

Tevens vragen deze leden hoe de motie van het lid Jasper van Dijk, waarin de regering wordt verzocht ervoor te zorgen dat de persoonlijke gegevens van onderwijsdeelnemers in handen van commerciële bedrijven worden vernietigd («overwegende dat gewerkt wordt aan pseudonimisering»), uitgevoerd gaat worden, aangezien onderwijsinstellingen vrijgelaten worden in de wijze waarop zij persoonsgegevens van hun leerlingen/studenten beschermen.[7]
Onderdeel van de afspraken met de leveranciers over de invoering van het pseudoniem is dat – na de invoering van het pseudoniem – alle persoonsgegevens van leerlingen die niet nodig zijn voor het aanbieden van onderwijs, worden verwijderd.

De leden van de ChristenUnie-fractie merken op dat de Raad van State in haar advies stelt dat het van belang is dat duidelijk is welke aanvullende gegevens wel en niet verstrekt mogen worden. Deze leden constateren dat de keuze om dit aan de onderwijsinstellingen zelf over te laten op gespannen voet lijken te staan met het doel van het wetsvoorstel om bij de uitwisseling zo min mogelijk persoonsgegevens te gebruiken. De regering stelt in reactie hierop dat de sector stevig inzet op een verbetering in de goede omgang en bescherming van persoonsgegevens van onderwijsdeelnemers, zo merken deze leden op. De leden van de fractie van de ChristenUnie verzoeken de regering nader toe te lichten, waarop de verwachting gebaseerd is dat dit voldoende effect zal sorteren. Zou het niet verstandig zijn het voorzorgsprincipe te hanteren en vooraf heldere voorwaarden vast te stellen die eventueel versoepeld kunnen worden nadat gebleken is dat de sector op een goede wijze met deze gegevens omgaat, zo vragen deze leden.

[7] Kamerstuk 32 034, nr. 9.

De wettelijke kaders en de uitwerking daarvan in het privacyconvenant schrijven helder voor onder welke voorwaarden onderwijsinstellingen leerlinggegevens mogen verstrekken. Onderwijsinstellingen hebben de ruimte om hier verschillende keuzes in te maken, afhankelijk van hun onderwijskundige visie en ambitie en de afstemming die zij hierover met ouders heeft. Het reguleren van welke gegevens uitgewisseld mogen worden doet geen recht aan de principiële verantwoordelijkheid van onderwijsinstellingen zelf en heeft bovendien nadelige gevolgen, zoals een rem op innovatie en het uitsluiten van andere oplossingen die hetzelfde doel bereiken en de daarmee gepaard gaande hogere kosten die voor aanbieders en scholen kunnen ontstaan. Met het pseudoniem, het ketenID, de standaardattributenset en de modelbewerkersovereenkomst is voor onderwijsinstellingen en leveranciers een heldere standaardsystematiek beschikbaar die zij kunnen gebruiken om een zorgvuldige omgang met persoonsgegevens op dit gebied te garanderen. De regering verwacht dat dit in de praktijk de norm zal worden en zodoende voldoende effect te sorteren. De evaluatie van de wet zal uitwijzen of deze verwachting bewaarheid wordt, of dat andere maatregelen nodig en wenselijk zijn.

De leden van de SGP-fractie vragen waarom de regering ervoor kiest om het gebruik van het eerste ketenID ten behoeve van leermiddelen in het voorstel vast te leggen, terwijl het gebruik van volgende ketenID's bij algemene maatregel van bestuur kan geschieden. In hoeverre is dit onderscheid ingegeven door de aard van de verschillende activiteiten waarvoor ketenID's worden gebruikt, zo vragen zij.
De belangrijkste aanleiding voor het wetsvoorstel vormt de wens van onderwijsinstellingen, leveranciers en de Tweede Kamer om de huidige gegevensuitwisseling tussen onderwijsinstellingen en leveranciers in het kader van de toegang tot en het gebruik van digitale leermiddelen te verbeteren. De regering heeft er uit het oogpunt van transparantie voor gekozen om dit ketenID in het wetsvoorstel zelf te regelen. Dit heeft als bijkomend voordeel dat er voor dit ketenID geen AMvB nodig is. Het wetsvoorstel voorziet in de mogelijkheid om bij AMvB andere gevallen aan te wijzen, waarvoor per geval een ander ketenID wordt gegenereerd. Dit zal slechts plaatsvinden nadat uit nader onderzoek en een privacy impact assessment nut en noodzaak van het introduceren van een ketenID evident is. Dat zal alleen in gevallen zijn waarbij een kwalitatief hoogwaardige, unieke en persistente identiteit van leerlingen nodig is om het doel van een zorgvuldige gegevensverwerking te bereiken.

2.4. Hoe komt een pseudoniem en ketenID tot stand?

De leden van de VVD-fractie merken op dat er wordt gesproken over het feit dat de technologische ontwikkelingen mogelijkheden meebrengen die maken dat een continue verbetering wordt aangebracht in het systeem. Deze leden vragen in hoeverre die continue verbetering mogelijk is in het voorgestelde kader.
Deze verbetering is mogelijk in het voorgestelde kader. Als het gaat om de bescherming van persoonsgegevens is het noodzakelijk om periodiek te bezien of de huidige beveiligingsmaatregelen nog afdoende zijn en of er betere technieken beschikbaar zijn op de markt. Zodra zo'n nieuwe techniek breed gedragen wordt, kan invoering ervan plaatsvinden. Het wetsvoorstel voorziet op dit punt in de gewenste flexibiliteit door de mogelijkheid om op het niveau van een ministeriële regeling nadere voorwaarden te stellen aan het pseudoniem en ketenID's.

Wordt in dit licht ook de wet geëvalueerd over vijf jaar, zo vragen de leden van voornoemde fractie.
De effecten van de maatregelen in het kader van de pseudonimisering worden binnen vijf jaar geëvalueerd. Zoals is aangegeven in de memorie

van toelichting besteedt de regering het onderzoek aan bij een wetenschappelijk onderzoeksbureau en zal zij zich laten adviseren over o.a. de opzet van het onderzoek. De precieze uitwerking van het onderzoek vindt dus te zijner tijd nog plaats, waardoor de technologische ontwikkelingen en de mogelijkheden die deze meebrengen voor verbetering in het voorgestelde kader hierbij kunnen worden betrokken. De evaluatie wordt vijf jaar na inwerkingtreding van de wet pseudonimisering naar de Staten-Generaal gestuurd.

Deze leden vragen of er andere landen of sectoren zijn die al op een dergelijke manier werken of gewerkt hebben en wat daar de ervaringen zijn.
Er wordt in andere landen veel gewerkt met vergelijkbare systematieken zoals we dat ook in Nederland met het persoonsgebonden nummer kennen. Voor zover de regering bekend is er geen ander land dat specifiek voor de toegang en het gebruik van digitale leermiddelen een pseudoniem of ketenID introduceert. In andere sectoren (zoals zorg en strafrecht) wordt wel met vormen van pseudonimisering gewerkt, maar omdat deze informatieketens op een andere manier werken en met andere technische middelen, zijn hier voor pseudonimisering in het onderwijs geen relevante ervaringen opgedaan.

De leden van de D66-fractie vragen de regering aan te geven bij welke organisatie de centraal georganiseerde nummervoorziening is belegd.
Het beheer van de nummervoorziening is bij Stichting Kennisnet belegd.

Welke eisen worden gesteld aan de versleuteling van het PGN, zo vragen de leden van voornoemde fractie.[8]
De concrete eisen die gesteld zijn aan de versleuteling van het PGN staan hierboven vermeld bij de beantwoording van de vraag van de leden van de VVD-fractie over de beveiliging van gegevens in paragraaf 1.1.

De leden van de D66-fractie vragen of de ontwikkelde nummervoorziening is gecontroleerd door de AP of NCSCop veiligheid.[9] [10]
Nee, de ontwikkelde nummervoorziening is niet gecontroleerd door de AP of NCSC. Deze organisaties rekenen dat niet tot hun taakgebied. Bij het ontwerp en de realisatie zijn wel de volgende veiligheidseisen gehanteerd, die direct of indirect voortvloeien uit de richtlijnen van deze organisaties:
- 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 tevens ISO 27001 gecertificeerd.

3. Reactie onderwijsorganisaties en uitkomst internetconsultatie

De leden van de GroenLinks-fractie vragen de regering waarom de voorkeur is uitgegaan naar één pseudoniem per leerling voor een hele onderwijssector.
Er is voor gekozen om de duur van het ketenID te beperken tot eenzelfde onderwijssector. Wanneer een leerling van het primair onderwijs naar het voortgezet onderwijs gaat, zal er een ander ketenID voor deze leerling worden gegenereerd. Daar is voor gekozen omdat vrijwel het gehele aanbod van leermiddelen op dit moment per onderwijssector is vormgegeven. Door het ketenID per onderwijssector gelijk te houden, vereenvoudigt dat de mogelijkheden voor onderwijsdeelnemers, wanneer dat de

[8] PGN: Persoonsgebonden nummer.
[9] AP: Autoriteit Persoonsgegevens.
[10] NCSC: Het Nationaal Cyber Security Centrum.

uitdrukkelijke wens is van (ouders en) onderwijsdeelnemers, om hun leerresultaten mee te nemen wanneer zij van school wisselen. De privacy impact assessment heeft onderschreven dat dit een verantwoorde en gerechtvaardigde keuze is.

De leden van voornoemde fractie vragen of het niet veiliger zou zijn om per partij waarmee gegevens worden uitgewisseld een eigen pseudoniem te ontwerpen om zo de koppeling van gegevens door derden tegen te gaan, zoals dr. E.R. Verheul reeds in de internetconsultatie heeft ingebracht. Deze leden vragen de regering of het technisch mogelijk is een dergelijk systeem in te voeren.[11]
Er is extern onderzoek gedaan naar de meerwaarde om per partij een eigen pseudoniem te ontwerpen. De conclusie is dat er op dit moment maar beperkte meerwaarde is ten opzichte van de voorgenomen oplossing van ketenpseudoniemen. Dit komt doordat in de huidige techniek ook attributen over de leerling worden uitgewisseld en partijen onderling over de leerling communiceren. Daarnaast is de technische en organisatorische impact op leveranciers en hun processen significant groter dan bij een ketenID. Op de langere termijn kan een situatie waarin per leverancier een pseudoniem gebruikt wordt een verbetering betekenen. Het is dan wel belangrijk dat de technologie bewezen werkt en ook daadwerkelijk een verbetering betekent. Mocht dat het geval zijn, dan is deze stap eenvoudiger te realiseren vanuit een situatie waarin het voorziene ketenID is geïmplementeerd dan vanuit de huidige situatie, zodat de continuïteit van het onderwijs geen onnodige extra risico's loopt. Om de koppelbaarheid van gegevens door derden verder te reduceren is de eis opgenomen dat het ketenID met een extra beveiligde maatregel wordt opgeslagen, apart van andere leerlinggegevens.

4. Reactie Autoriteit Persoonsgegevens

De leden van de D66-fractie constateren dat de AP heeft geadviseerd om in de toelichting op het wetsvoorstel nader te motiveren waarom een pseudoniem noodzakelijk is en op welke wijze een pseudoniem tot dataminimalisatie leidt. De leden van voornoemde fractie vragen of de regering kan uiteenzetten welke wijzen van pseudonimisering overwogen zijn en de mate waarin de alternatieven de privacy borgen.
Zoals hierboven uiteengezet zijn diverse alternatieven overwogen (waaronder anonimisering en polymorfe pseudonimisering, waarbij elke partij een ander pseudoniem krijgt). Hoewel anonimisering voordelen biedt voor de privacy, is dit geen werkbaar alternatief gebleken. Polymorfe pseudonimisering kan aanvullende voordelen bieden voor de privacy van leerlingen, maar deze voordelen wegen niet op tegen de aanvullende risico's en benodigde tijd om dit in de huidige situatie te implementeren. De keuze voor de huidige vorm van pseudonimiseren, de wijze waarop deze pseudoniemen tot stand komen en de bijbehorende beveiligingseisen (waaronder de mate van encryptie van gegevens) zijn gebaseerd op deze 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. Een nieuwe systematiek waarvan niet op voorhand bekend is of die op grote schaal toepasbaar is, zou te veel onzekerheden met zich meebrengen. Daarnaast kunnen alle leveranciers de benodigde aanpassingen in hun systemen sneller aanbrengen voor de huidige oplossing. Hoe moderner de techniek, hoe langer het duurt voordat alle partijen zijn aangesloten. Daarbij geldt eveneens dat het zetten van deze stap op dit moment, het eenvoudiger en minder risicovol maakt om later een geavanceerdere

[11] https://www.cs.ru.nl/E.Verheul/presentations/Reactie_op_wetsvoorstel_pseudonimisering_onderwijs.pdf.

techniek te implementeren, wanneer deze bewezen werkt en deze een duidelijke verbetering betekent. Het wetsvoorstel voorziet in haar opzet, door delegatie van relevante voorwaarden naar lagere regelgeving, in de mogelijkheid om bij te blijven met de laatste stand van de techniek.

De leden van de PvdA-fractie merken op dat in de memorie van toelichting de regering een gedetailleerde reactie geeft op het advies van de AP. De AP adviseert dat andere pseudoniemen niet worden gebaseerd op het PGN, tenzij dit geschiedt bij formele wet. De leden van voornoemde fractie vragen of de regering nader kan toelichten hoe de vastlegging van de voorwaarden waaronder een ketenID gebruikt mag worden in een ministeriële regeling, recht doet aan deze overweging.
Het advies van de AP heeft geleid tot een belangrijke herziening van het wetsvoorstel en methode van pseudonimiseren. In het onderhavige wetsvoorstel is de mogelijkheid voorzien voor onderwijsinstellingen om een pseudoniem op het PGN te baseren. KetenID's die voor bepaalde gevallen kunnen worden gebruikt, worden vervolgens op dat pseudoniem (in plaats van op het PGN) gebaseerd. Dit pseudoniem is naar zijn aard geen persoonsnummer als bedoeld in artikel 24 van de Wbp. Het is mede om die reden niet bezwaarlijk om de voorwaarden waaronder een ketenID gebruikt mag worden in een ministeriële regeling vast te leggen.

5. Uitvoering en handhaving

De leden van de PvdA-fractie lezen in de brief van de sectorraden voor het primair onderwijs, het voortgezet onderwijs en het mbo en de brancheorganisaties van uitgeverijen, distributeurs en softwareleveranciers dat zij aandringen op de inwerkingtreding van de wet per januari 2018.[12] Heeft de regering ook nagegaan of er bij de scholierenorganisatie LAKS, de deelnemersorganisatie in het mbo, JOB, of de ouderorganisaties Ouders & Onderwijs en de Vereniging Openbaar Onderwijs de wens leeft dat het wetsvoorstel zo spoedig mogelijk in werking treedt, zo vragen de leden van voornoemde fractie. In dat geval lijkt het de leden wenselijk om inderdaad de wetsbehandeling nu met voortvarendheid tot een goed einde te brengen.
LAKS en JOB steunen het doel van het wetsvoorstel. Op dit moment hebben zij zich beperkt kunnen verdiepen in de precieze invulling van het voorstel. Wij zullen het gesprek voortzetten met LAKS en JOB over dit wetsvoorstel en de andere maatregelen en mogelijkheden om de privacy van onderwijsdeelnemers te bevorderen. Ouders & Onderwijs schaart zich eveneens achter het wettelijk regelen van pseudonimiseren en juicht een spoedige Kamerbehandeling toe. Omdat Ouders & Onderwijs voor de regering als centrale ouderorganisatie het aanspreekpunt is voor het in kaart brengen van de voorkeuren van ouders, is niet aanvullend contact gezocht met de Vereniging Openbaar Onderwijs.

Het is nodig dat het wetsvoorstel begin 2018 in werking treedt, om met ingang van volgend schooljaar tot implementatie over te kunnen gaan. Gelet op de brede maatschappelijke steun voor het wetsvoorstel en het belang van dit onderwerp, verzoeken wij uw Kamer het wetsvoorstel met voorrang te behandelen.

De Minister van Onderwijs, Cultuur en Wetenschap,
M. Bussemaker

De Staatssecretaris van Onderwijs, Cultuur en Wetenschap,
S. Dekker

---

[12] Parlis nr. 2017Z08439, d.d. 16 juni 2017.