Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

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. 3 **MEMORIE VAN TOELICHTING**

Inhoudsopgave

kst-34741-3
ISSN 0921 - 7371
's-Gravenhage 2017

A. Algemeen

Dit wetsvoorstel voorziet in een grondslag op basis waarvan onderwijsinstellingen het persoonsgebonden nummer eenmalig kunnen gebruiken om een pseudoniem te genereren. Dit pseudoniem vormt de basis om voor specifieke gevallen andere pseudoniemen (in de technische uitvoering bekend als: 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 gebruik van een ketenID is in ieder geval voorzien voor de toegang tot en het gebruik van digitale leermiddelen en het digitaal afnemen van toetsen en examens en heeft tot gevolg dat het aantal persoonsgegevens dat wordt gebruikt voor de digitale uitwisseling van gegevens tot een minimum beperkt kan worden. Wijzigingen worden voorgesteld van de Wet op het primair onderwijs (WPO), de Wet primair onderwijs BES (WPO BES), de Wet op de expertisecentra (WEC), de Wet op het voortgezet onderwijs (WVO), de Wet voortgezet onderwijs BES (WVO BES), de Wet educatie en beroepsonderwijs (WEB), de Wet educatie en beroepsonderwijs BES (WEB BES) en de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). De nadere uitwerking van de andere specifieke gevallen waarvoor en de condities waaronder een ketenID gegenereerd en gebruikt mag worden, zal plaatsvinden in lagere regelgeving.

Deze memorie van toelichting is tot stand gekomen in overeenstemming met de Staatssecretaris van Economische Zaken.

1. Inleiding

1.1. Kern van het wetsvoorstel

Het wetsvoorstel heeft tot doel om een veiliger, betrouwbaarder en meer efficiënte digitale uitwisseling van gegevens door onderwijsinstellingen mogelijk te maken, waarbij zo min mogelijk persoonsgegevens worden gebruikt van leerlingen, deelnemers of studenten. Daartoe voorziet het wetsvoorstel in een grondslag om een pseudoniem te genereren op basis van het persoonsgebonden nummer. Dit pseudoniem vormt de basis om voor een specifiek geval een ander pseudoniem (in de technische uitvoering bekend als ketenID) te genereren, dat gebruikt kan worden bij de digitale uitwisseling van gegevens tussen een onderwijsinstelling en een andere partij. Het gebruik van een ketenID is in ieder geval voorzien voor de toegang tot en het gebruik van digitale leermiddelen en het digitaal afnemen van toetsen en examens. De nadere uitwerking van de andere specifieke gevallen waarvoor en de condities waaronder een ketenID gegenereerd en gebruikt mag worden, zal plaatsvinden in lagere regelgeving.

1.2. Leeswijzer

In deze memorie van toelichting worden de wijzigingen en voordelen van de nieuwe ten opzichte van de huidige situatie nader toegelicht. In paragraaf 1 komen onder meer de probleemanalyse, aanleiding en nut en noodzaak van het wetsvoorstel aan de orde. In paragraaf 2 wordt het doel van het wetsvoorstel nader toegelicht en wordt uitvoerig ingegaan op de bescherming van persoonsgegevens. Ook komen de wijze waarop het pseudoniem tot stand komt en de reikwijdte van het pseudoniem aan bod. Aan het slot van paragraaf 2 worden enkele aanvullende maatregelen beschreven. De daaropvolgende paragrafen behandelen achtereenvolgens de rol van de Inspectie van het Onderwijs (3), de uitkomsten van de openbare internetconsultatie (4), de reactie van de Autoriteit Persoons-

gegevens (5), de uitkomsten van het uitgevoerde privacy impact assessment (6), de positie van Caribisch Nederland (7), de uitkomst van de uitvoerings- en handhaafbaarheidstoets (8), de administratieve lasten (9) en de financiële gevolgen (10).

Daar waar in deze toelichting wordt gesproken over onderwijsdeelnemers, worden leerlingen in het primair, (voortgezet) speciaal onderwijs en voortgezet onderwijs, extraneï in het voortgezet onderwijs, (examen)deelnemers in het educatie en middelbaar beroepsonderwijs en studenten en extraneï in het hoger onderwijs bedoeld.

1.3. Probleemanalyse

De samenleving digitaliseert in toenemende mate. Het is vandaag de dag de normaalste zaak van de wereld om boodschappen via internet te bestellen, online een zorgverzekering af te sluiten, of de belastingaangifte digitaal te versturen. Ook in het onderwijs is digitalisering niet meer weg te denken. De onderwijsinstelling staat in het hart van de netwerksamenleving en heeft met veel organisaties contact over haar onderwijsdeelnemers. Zoals met samenwerkingsverbanden passend onderwijs om te bepalen of een onderwijsdeelnemer in aanmerking komt voor extra ondersteuning. En denk aan de uitwisseling van onderwijsdeelnemergegevens tussen onderwijsinstelling en stagebedrijf in het kader van de beroepspraktijkvorming in het mbo, of aan de gegevensuitwisseling tussen instellingen in het middelbaar beroepsonderwijs en hoger onderwijs indien de onderwijsdeelnemer een deel van het onderwijs bij een andere instelling geniet dan waar hij staat ingeschreven. Hiervoor is het nodig dat onderwijsinstellingen gegevens kunnen uitwisselen over onderwijsdeelnemers. Er is een groeiende behoefte om dit efficiënt, veilig en met de nodige privacywaarborgen via de digitale weg te kunnen doen.

Het meest in het oog springende voorbeeld is dat steeds meer leraren apps gebruiken die hen helpen om kinderen bijvoorbeeld taal of rekenen te leren. Onderwijsinstellingen in het primair onderwijs (po), (voortgezet) speciaal onderwijs ((v)so), voortgezet onderwijs (vo), middelbaar beroepsonderwijs (mbo) en het hoger onderwijs (ho) maken in toenemende mate gebruik van dergelijke digitale leermiddelen.[1] Of het nu gaat om onderwijsinstellingen die alle onderwijsdeelnemers met behulp van een laptop of tablet onderwijs geven, of om onderwijsinstellingen die voor sommige klassen of enkele vakken of delen van de opleiding digitale hulpmiddelen gebruiken, het gebruik van digitale leermiddelen neemt in het Nederlandse onderwijs gestaag toe.
Digitale leermiddelen brengen nieuwe mogelijkheden met zich mee, die veel kunnen betekenen voor de kwaliteit van het onderwijs. Zo kunnen digitale leermiddelen bijdragen aan maatwerk door oefenstof in het tempo en op het niveau van de onderwijsdeelnemer aan te bieden. Door onderwijsdeelnemers digitaal (formatief) te toetsen, kan de leraar de vorderingen goed op dag tot dag basis volgen. Dat maakt het voor docenten mogelijk om meer te differentiëren tussen onderwijsdeelnemers. Directe feedback en automatisch nakijken zijn voordelen waarmee leraren tijd besparen, die weer benut kan worden voor interactie met de onderwijsdeelnemers. Ook worden digitale leermiddelen veel gebruikt bij het aanleren van 21e-eeuwse vaardigheden zoals digitale geletterdheid, mediawijsheid en *computational thinking*. Naast formatieve toetsen worden ook steeds meer formele (summatieve) toetsen en

[1] Onder digitale leermiddelen wordt verstaan: digitale producten of digitale diensten, bestaande uit leerstof en/of (formatieve) toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens onderwijsinstellingen.

examens digitaal aangeboden. Centrale examens in het mbo, een deel van de centrale examens in het vo en de (adaptieve) eindtoets in het po kunnen digitaal afgenomen worden.

Tegelijkertijd brengt het gebruik van digitale leermiddelen nieuwe vraagstukken met zich mee. Om gebruik te kunnen maken van digitale leermiddelen en digitale toetsen moeten onderwijsdeelnemers vaak verbinding maken met de digitale leeromgeving van de leverancier van deze middelen (meestal een educatieve uitgever of een andere educatieve dienstverlener). Daarvoor is het nodig dat onderwijsdeelnemers probleemloos, met inachtneming van hun privacy, kunnen inloggen en de leermiddelen kunnen gebruiken waarvoor is betaald. Hiervoor worden licenties afgesloten tussen onderwijsinstelling of onderwijsdeelnemer en de leveranciers. Daarbij is een goede organisatie op stelselniveau van belang zodat onderwijsinstellingen, leraren en onderwijsdeelnemers op een efficiënte manier gebruik kunnen maken van deze leermiddelen, met oog voor een goede borging van de privacy van betrokkenen.

Verschillende partijen dragen eraan bij om een goed gebruik van digitale leermiddelen mogelijk te maken. Leveranciers van schoolinformatiesystemen (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 gezamenlijk: leveranciers). Om ervoor te zorgen dat onderwijsdeelnemers probleemloos gebruik kunnen maken van digitale leermiddelen, moeten zij uniek geïdentificeerd kunnen worden door de leveranciers. Hiervoor hebben de onderwijsinstelling en de desbetreffende leverancier een unieke identiteit nodig, zoals het persoonsgebonden nummer. Het persoonsgebonden nummer mag op grond van de huidige wetgeving echter niet gebruikt worden voor de uitwisseling tussen onderwijsinstellingen en leveranciers. Doordat onderwijsinstellingen nu niet kunnen beschikken over een unieke identiteit voor de uitwisseling van gegevens met leveranciers, ontstaan verschillende problemen. Zo kunnen identiteiten te laat beschikbaar komen of van onvoldoende kwaliteit zijn om een goede en tijdige werking van digitale leermiddelen bij aanvang van het schooljaar te garanderen. Ieder jaar levert dit de nodige administratieve rompslomp op voor zowel de onderwijsinstellingen als de leveranciers. Ook brengt dit andere problemen en risico's mee, zoals dat de resultaten aan de verkeerde leerling worden gekoppeld. Dit heeft tot gevolg dat leveranciers hun eigen maatregelen nemen om onderwijsdeelnemers uniek te identificeren. Hierbij wordt veelal gebruik gemaakt van persoonsgegevens of een eigen administratief nummer dat door leveranciers wordt toegekend om ervoor te zorgen dat een correcte koppeling gelegd kan worden tussen aangeschafte leermiddelen en de onderwijsdeelnemers voor wie deze leermiddelen zijn bestemd. Door deze «matchingsproblematiek» worden er vaak onnodig veel persoonsgegevens uitgewisseld. Wanneer leveranciers hun eigen administratieve nummers introduceren wordt het voor de leerling moeilijker gemaakt om zijn leervorderingen mee te nemen als hij van school wisselt, omdat elke leverancier er zijn eigen methodiek op na houdt. Het introduceren van een pseudoniem (ketenID) biedt hier een oplossing voor. Een pseudoniem is een unieke identiteit voor onderwijsdeelnemers die door elke leverancier kan worden gebruikt, zonder dat direct te herleiden is om welke specifieke onderwijsdeelnemer het gaat. Met dit wetsvoorstel wordt aangesloten bij de Algemene verordening gegevensbescherming, die per 25 mei 2018 van toepassing is. In deze verordening wordt pseudonimisering gedefinieerd als: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze (ten opzichte van het

pseudoniem) aanvullende gegevens gescheiden worden opgeslagen en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. In de verordening wordt onderschreven dat de toepassing van pseudonimisering op persoonsgegevens de risico's voor de betrokkenen kan verminderen en de verwerkingsverantwoordelijken en de verwerkers kan helpen om hun verplichtingen inzake gegevensbescherming na te komen.

Onderwijsinstellingen worden ook bij het digitaal afnemen van toetsen en examens ondersteund door verschillende systemen.[2] Ook voor toetsen en examens is er behoefte aan een unieke, persistente identiteit voor onderwijsdeelnemers om goed te kunnen plannen en te verifiëren dat de resultaten aan de juiste onderwijsdeelnemer gekoppeld worden. Ook in dit geval is een ketenID een bruikbare oplossing.

1.4. Aanleiding en achtergrond

De aanleiding voor het wetsvoorstel is de wens van onderwijsinstellingen, leveranciers en de Tweede Kamer om de huidige gegevensuitwisseling tussen onderwijsinstellingen en leveranciers te verbeteren. Het gaat hierbij om verbeteren in twee opzichten:

1. Onderwijsinstellingen wisselen op dit moment direct tot de persoon herleidbare gegevens van onderwijsdeelnemers uit met educatieve uitgevers en distributeurs. Dit is voor de werking van de leermiddelen niet altijd noodzakelijk. Vanuit het oogpunt van dataminimalisatie, een beginsel dat is vastgelegd in de Wet bescherming persoonsgegevens (hierna te noemen Wbp), mogen alleen de strikt noodzakelijke persoonsgegevens uitgewisseld worden. Pseudonimiseren maakt deze dataminimalisatie mogelijk;
2. Met het toenemend gebruik van digitale leermiddelen en digitale toetsen en de wens van onderwijsinstellingen en leraren om hun onderwijs beter te laten aansluiten op het tempo en niveau van de afzonderlijke onderwijsdeelnemer, neemt het belang van een goed functionerende leermiddelenketen toe. Om van de meerwaarde van digitale leermiddelen gebruik te kunnen maken, moeten onderwijsdeelnemers gedurende een bepaalde periode door de leermiddelen herkend kunnen worden. Alleen dan kunnen de vorderingen van een onderwijsdeelnemer worden gevolgd. De toegang tot en het gebruik van digitale leermiddelen en toetsen moeten soepel verlopen, zonder onnodige administratieve lasten voor onderwijsinstellingen en zodanig dat de leerresultaten snel en gemakkelijk toegankelijk zijn voor de onderwijsdeelnemer en de leraar. De onderwijsdeelnemer moet ook beter dan nu in staat worden gesteld om zijn materiaal en vorderingen mee te nemen wanneer hij van school wisselt. Dit zorgt ervoor dat de onderwijsdeelnemer zich verzekerd ziet van het recht op dataportabiliteit, dat in de Algemene verordening gegevensbescherming is opgenomen.

In het Doorbraakproject Onderwijs en ICT is in 2014 in publiek-private samenstelling (met onderwijsinstellingen en leveranciers) gesproken over de belangrijkste belemmeringen en oplossingen om een doorbraak in het gebruik van adaptieve digitale leermiddelen te bereiken. Eén van de adviezen van de publiek-private tafels betreft de introductie van een ketenID voor onderwijsdeelnemers om de toegang tot en het gebruik van

[2] Onder het afnemen van toetsen en examens wordt hier het volledige proces van plannen, inroosteren, afnemen, verwerken en terugkoppelen van resultaten van toetsen en examens verstaan.

digitale leermiddelen te optimaliseren.[3] Een ketenID is een unieke identiteit voor onderwijsdeelnemers die door elke leverancier kan worden gebruikt, zonder dat direct te herleiden is om welke specifieke onderwijsdeelnemer het gaat.

De Tweede Kamer heeft tijdens een Algemeen overleg op 21 januari 2015 haar zorgen geuit over de omgang met persoonsgegevens door onderwijsinstellingen en uitgevers van digitaal leermateriaal. Zij heeft aangegeven het onwenselijk te vinden dat onderwijsinstellingen direct identificerende persoonsgegevens van onderwijsdeelnemers gebruiken in de uitwisseling met private partijen. Ook als dit rechtmatig gebeurt in een situatie waarin de onderwijsinstelling als verantwoordelijke en de uitgever als bewerker in de zin van de Wbp optreedt.[4] De motie Rog vraagt de regering te realiseren dat persoonsgegevens van onderwijsdeelnemers alleen nog maar gepseudonimiseerd worden verstrekt aan leveranciers en ontwikkelaars van digitaal leermateriaal.[5] De motie Jasper van Dijk verzoekt de regering ervoor te zorgen dat de persoonlijke gegevens van onderwijsdeelnemers in handen van commerciële bedrijven worden vernietigd (overwegende dat er gewerkt wordt aan pseudonimisering).[6]

Bij het afnemen van digitale toetsen en examens lopen onderwijsinstellingen tegen vergelijkbare vragen aan. Hiervoor is ook een unieke digitale identiteit nodig, om de administratieve lasten zo beperkt mogelijk te houden en zo min mogelijk persoonsgegevens uit te wisselen. Daarom is onderhavig wetsvoorstel mede bedoeld om het gebruik van een ketenID voor het digitaal afnemen van toetsen en examens mogelijk te maken.

Tijdens de voorbereiding van dit wetsvoorstel is gebleken dat de behoefte aan een unieke digitale identiteit sterk en breed leeft in het hele onderwijs (zie de onder 1.3 genoemde voorbeelden). Onderwijsinstellingen willen gegevens digitaal op een veilige manier kunnen uitwisselen, met zo min mogelijk administratieve last en met gebruik van zo min mogelijk persoonsgegevens. Een ketenpseudoniem maakt het mogelijk om voor specifieke gevallen en processen dit op een goede manier te organiseren. De toenemende digitalisering maakt dat de vraag hiernaar alleen maar verder zal toenemen. Daarom richt het wetsvoorstel zich op het mogelijk maken van een adequate en toekomstbestendige oplossing voor digitale gegevensuitwisseling in het onderwijs.

1.5. Privacy en digitale onderwijsmiddelen: onderwijsinstellingen voeren de regie

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 bijdragen aan een betere borging van de privacy van onderwijsdeelnemers. In juni 2016 hebben deelnemende partijen het convenant «Convenant Digitale onderwijsmiddelen en privacy 2.0» gesloten.[7] De individuele partijen die dit convenant hebben ondertekend, dekken op dit moment gezamenlijk zo'n 95 procent van de markt van leermiddelen en leerlinginformatiesystemen.

---

[3] Doorbraakproject Onderwijs en ICT, Eindrapportage publiek-private tafels, oktober 2014. Te vinden op www.doorbraakonderwijsenict.nl

[4] Handelingen II 2014/15, nr. 44. Verslag van een Algemeen overleg privacy in het onderwijs, 21 januari 2015.

[5] Kamerstukken II 2014/15, 32 034, nr. 15

[6] Kamerstukken II 2014/15, 32 034, nr. 9

[7] Kamerstukken II 2014/15, 32 034, nr. 17. Te vinden op www.privacyconvenant.nl

Het convenant regelt onder meer 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 leveranciers, 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 Autoriteit Persoonsgegevens 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. Bij het convenant zijn een modelbewerkersovereenkomst en een privacybijsluiter gevoegd die onderwijsinstellingen en leveranciers kunnen gebruiken bij het sluiten van contracten voor de aanschaf of het gebruik van digitale leermiddelen. De uitgangspunten van deze modelbewerkersovereenkomst sluiten aan bij de bepalingen in het convenant, de Wbp en de uitgangspunten die de Autoriteit Persoonsgegevens (AP) in richtsnoeren en uitspraken heeft neergelegd. De modelbewerkersovereenkomst eist van de leveranciers een passende beveiliging van gegevens zoals op grond van de Wbp (artikel 14) wordt vereist. Als de leverancier en de onderwijsinstelling gebruik maken van de modelbewerkersovereenkomst, dan worden de afspraken uit het convenant automatisch onderschreven.

De modelovereenkomst ondersteunt onderwijsinstellingen bij het sluiten van contracten. Doordat een groot aantal leveranciers het convenant heeft ondertekend, zijn de uitgangspunten van het convenant in de praktijk de norm. Het bevoegd gezag van de onderwijsinstelling is en blijft altijd zelf verantwoordelijk voor het sluiten van deugdelijke contracten. Het convenant en de modelbewerkersovereenkomst ondersteunen dit gezag hierbij, maar het bevoegd gezag kan ook zelf, zonder modelovereenkomst, mits binnen de kaders van de wet, goede afspraken maken met leveranciers. De AP houdt hier toezicht op.

1.6. Pseudoniem maakt verdere dataminimalisatie mogelijk

Op dit moment wisselen onderwijsinstellingen en leveranciers onderling veelal nog een set aan persoonsgegevens uit om zich ervan te vergewissen dat ze het over dezelfde onderwijsdeelnemer hebben. Daarbij hebben ze vaak eveneens een eigen administratief nummer geïntroduceerd. Het is ook mogelijk om in plaats van deze set aan persoonsgegevens en eigen administratieve nummers een nummer te gebruiken dat voor iedere onderwijsdeelnemer uniek is. Het persoonsgebonden nummer (PGN) in het onderwijs – meestal het burgerservicenummer (BSN) – is zo'n uniek nummer. Het is echter ongewenst om het BSN zelf hiervoor te benutten, omdat dit nummer op meer plekken binnen en buiten het onderwijs wordt gebruikt en daardoor in meer systemen bekend is. Dat zou het risico op koppelbaarheid van gegevens vergroten en daarmee op gespannen voet komen te staan met de uitgangspunten van de Wbp.

Om die reden wordt het PGN omgezet naar een pseudoniem, dat alleen voor de school beschikbaar is en verder niet wordt gebruikt voor het uitwisselen van gegevens. Dit pseudoniem wordt per specifiek bepaald geval omgezet naar een ander pseudoniem dat in de uitwisseling voor specifieke ketens wordt gebruikt (ketenID). Het eerste ketenID dat is voorzien is voor de toegang tot en het gebruik van digitale leermiddelen, toetsen en examens. Dit ketenID leidt ertoe dat onderwijsinstellingen en

leveranciers van digitaal leermateriaal, toetsen en examens weten dat ze het over dezelfde onderwijsdeelnemer hebben. Alleen de onderwijsinstelling weet welke onderwijsdeelnemer dit is; het ketenID is voor anderen niet te herleiden tot een individuele onderwijsdeelnemer. Dit ketenID is een unieke identiteit in de computersystemen van de leveranciers en de school, verschijnt niet op het scherm en is in die zin niet door mensen te verwerken.

Het ketenID maakt verdere dataminimalisatie mogelijk. Onderwijsinstellingen hoeven alleen die gegevens met leveranciers uit te wisselen die nodig zijn voor een gebruiksvriendelijke inzet van digitale leermiddelen. Te denken valt aan een voornaam, zodat onderwijsdeelnemers die werken in een digitale leeromgeving die niet in de onderwijsinstelling zelf staat, aangesproken kunnen worden met hun voornaam. De onderwijsinstelling bepaalt welke gegevens dit precies zijn, vanuit haar verantwoordelijkheid op grond van de Wbp voor een zorgvuldige omgang met persoonsgegevens. Dit is onderdeel van de afspraken die de onderwijsinstelling maakt met de leverancier. Het eerder hierboven beschreven privacyconvenant en de bijbehorende modelbewerkersovereenkomst ondersteunen de onderwijsinstellingen in het po en vo hierbij.

De deelnemende partijen aan het convenant hebben concrete afspraken gemaakt over de implementatie van het pseudoniem/ketenID en over de aanvullende persoonsgegevens die verstrekt mogen worden voor de toegang tot en het gebruik van digitaal leermateriaal en het digitaal afnemen van toetsen en examens. Daarbij is het doel het zoveel mogelijk terugbrengen van het aantal persoonsgegevens dat hiervoor nodig is, terwijl het verzorgen van onderwijs zo efficiënt mogelijk kan verlopen. Binnen Edu-K is hiertoe een attributenbeleid vastgesteld, waarin de uitgangspunten staan beschreven op basis waarvan onderwijsinstellingen en private partijen omgaan met aanvullende persoonsgegevens (attributen). In het kader daarvan is een standaardattributenset afgesproken, waarin de aanvullende gegevens zijn opgenomen die gebruikt kunnen worden tussen onderwijsinstellingen en private partijen voor de toegang tot en het gebruik van digitale leermiddelen en toetsen. 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). De 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.[8] Uit deze juridische analyse komt ook naar voren dat het op overkoepelend niveau vaststellen van een attributenbeleid er naar verwachting toe zal leiden dat het overgrote deel van de markt zich zal gaan conformeren aan de standaarden die in dit beleid zijn gezet en dat leveranciers bij de inrichting van hun diensten rekening zullen houden met dit beleid. Deze ontwikkeling komt tegemoet aan de vereisten van privacy by design en privacy by default. Het vaststellen van een standaardattributenset, in combinatie met het invoeren van één persisterend kenmerk (pseudoniem/ketenID) voor de koppeling tussen ketenpartners, zal naar verwachting leiden tot een afname van het aantal persoonsgegevens dat op dit moment «standaard» door een onderwijsinstelling wordt doorgegeven. Het attributenbeleid zal stelselmatig onderwerp van evaluatie en zo nodig aanpassing zijn binnen Edu-K. Het attributenbeleid, de standaardattributenset, de juridische analyse en andere relevante documenten zijn openbaar en voor eenieder te raadplegen via de website van Edu-K (www.edu-k.nl).

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

De standaardattributenset geeft de onderwijsinstelling heldere richtlijnen en biedt haar tegelijkertijd de ruimte om daar in voorkomend geval gemotiveerd van af te kunnen wijken. Die ruimte is ook wenselijk. Een leverancier van digitale leermiddelen kan bijvoorbeeld een adaptief leermiddel ontwikkelen waarbij ook het geslacht van een leerling wordt gebruikt, omdat daarmee ingespeeld kan worden op verschillen tussen jongens en meisjes. 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 ouders en de medezeggenschapsraad, een zorgvuldige afweging maakt over de persoonsgegevens die zij van onderwijsdeelnemers ter beschikking stelt en voor welke doeleinden. Het wetsvoorstel draagt met het kunnen gebruiken van een pseudoniem (op basis van het persoonsgebonden nummer) bij aan een verbetering van zowel de privacy van onderwijsdeelnemers als het effectief functioneren van digitale leermiddelen.

1.7. Nut en noodzaak wetsvoorstel

De onderwijsinstelling staat in het hart van de netwerksamenleving en heeft met veel organisaties contact over haar onderwijsdeelnemers. Zoals met samenwerkingsverbanden passend onderwijs om te bepalen of een onderwijsdeelnemer in aanmerking komt voor extra ondersteuning. Hiervoor is het nodig dat onderwijsinstellingen gegevens kunnen uitwisselen over onderwijsdeelnemers. Er is een groeiende behoefte om dit efficiënt, veilig en met de nodige privacywaarborgen via de digitale weg te kunnen doen. Het is omwille van koppelbaarheid met andere gegevens niet wenselijk het PGN in dergelijke gevallen te gebruiken, omdat dit risico's voor de privacy van onderwijsdeelnemers met zich mee zou brengen. Het gebruik van ketenID's die voor specifieke gevallen gegenereerd en gebruikt worden, kent deze nadelen niet.

Het ligt voor de hand om het PGN te gebruiken om het pseudoniem op te baseren. De redenen hiervoor zijn:
– 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.

Ook uit het privacy impact assessment blijkt dat het PGN het voor de hand liggende nummer is om als basis voor het pseudoniem van onderwijsdeelnemers te gebruiken (zie paragraaf 6).

Om het pseudoniem te kunnen baseren op het PGN, is het noodzakelijk een doelbepaling voor het gebruik van het PGN in de wet op te nemen. Omdat het gebruik van het PGN extra risico's met zich kan brengen voor de bescherming van de persoonlijke levenssfeer, is in artikel 24 van de Wbp bepaald dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij de wet is bepaald. Aldus is een afweging op het niveau van de formele wet in beginsel gegarandeerd. Aan dit vereiste wordt met dit wetsvoorstel voldaan.

In de digitale uitwisseling van gegevens met andere partijen loopt de onderwijsinstelling telkens tegen dezelfde problemen aan. Er is een behoefte aan unieke, persistente identiteiten, zodat de uitwisseling goed

verloopt en er niet meer persoonsgegevens worden gebruikt dan noodzakelijk. De behoefte hieraan groeit, aangezien de samenleving steeds verder digitaliseert. De verscheidenheid aan partijen die onderwijsinstellingen uit de verschillende sectoren kennen, maakt dat een toekomstbestendige en flexibele oplossing nodig is. Om de huidige problemen het hoofd te bieden, hebben partijen hun eigen systematiek in het leven geroepen, met eigen nummers en veelal het gebruik van persoonsgegevens. Door een stelsel van ketenID's te creëren, waarbij het pseudoniem op het PGN is gebaseerd, kunnen voor specifieke uitwisselingen deze problemen worden opgelost en onder betere en transparante voorwaarden tot stand komen. Door alleen het pseudoniem op het PGN te baseren (in plaats van de afzonderlijke ketenID's) wordt het PGN niet in meer gevallen gebruikt dan strikt noodzakelijk. Dit wetsvoorstel vraagt slechts éénmaal een afweging op het niveau van de wet en is daarmee ook toekomstbestendig. Het wetsvoorstel voorziet erin dat de nadere aanwijzing van specifieke gevallen waarvoor een ketenID gegenereerd mag worden bij algemene maatregel van bestuur zal plaatsvinden, waarbij eveneens de categorieën van ontvangers worden benoemd die van het ketenID gebruik mogen maken. De voorwaarden waaronder het pseudoniem en het ketenID gebruikt mogen worden, zullen bij ministeriële regeling worden vastgesteld. Deze voorwaarden hebben betrekking op de duur van het pseudoniem/ketenID – hierbij gaat het om de vraag hoe lang hetzelfde pseudoniem voor een onderwijsdeelnemer gebruikt mag worden – en de beveiliging, waaronder gescheiden opslag van de pseudoniemen.

De regering heeft een bijzondere verantwoordelijkheid voor het genereren en gebruiken van pseudoniemen, omdat deze hun oorsprong vinden in het persoonsgebonden nummer; het gebruik van dit nummer is aan strenge wettelijke regels gebonden. De regering wil voorkomen dat pseudoniemen alsnog herleid kunnen worden tot het persoonsgebonden nummer, of dat het pseudoniem door langdurig gebruik de facto een nieuw persoonsgebonden nummer wordt. Daarvoor is het nodig nadere voorwaarden te stellen aan de beveiliging en het gebruik van pseudoniemen, 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).

Ten aanzien van de duur van het ketenID dat gebruikt wordt voor de toegang tot en het gebruik van digitale leermiddelen en het digitaal afnemen van toetsen en examens zal de duur van het pseudoniem aanvankelijk worden beperkt tot de onderwijssector. Wanneer een leerling van het primair onderwijs naar het voortgezet onderwijs gaat, zal er een ander pseudoniem voor deze leerling moeten worden gegenereerd. Daar is voor gekozen omdat vrijwel het gehele aanbod van leermiddelen per onderwijssector is vormgegeven. De ontwikkelingen binnen het onderwijs en de leermiddelenmarkt gaan echter toe naar een situatie waarin maatwerk per leerling en doorlopende leerlijnen beter gefaciliteerd worden. Het aanbod van sectoroverstijgende leermiddelen zal daarmee groeien. Op termijn ontstaat hierdoor een situatie waarbij een andere indeling van de duur van pseudoniemen wenselijk is om het onderwijs aan leerlingen op een goede manier te kunnen faciliteren. Hoe deze ontwikkelingen zullen uitpakken is nog niet te voorzien, wel is helder dat dit een dynamisch proces is. Dat betekent dat de administratieve voorschriften ten aanzien van de duur van pseudoniemen naar verwachting dikwijls wijziging zullen behoeven, waarmee delegatie naar ministeriële regeling op dit punt aangewezen is.

Om in adequate beveiligingsvoorschriften te voorzien, worden bij ministeriële regeling nadere voorwaarden gesteld ten aanzien van de beveiliging, waaronder gescheiden opslag van de pseudoniemen. Delegatie naar ministeriële regeling wordt noodzakelijk geacht, omdat het administratieve voorschriften betreft en deze voorwaarden naar verwachting dikwijls zullen wijzigen. De voorwaarden die zien op de beveiliging hangen immers sterk samen met de snel voortschrijdende ontwikkelingen in de techniek. Het niveau van de ministeriële regeling biedt de nodige flexibiliteit om deze nadere voorwaarden actueel te houden en daarmee ook daadwerkelijk in de beveiliging van pseudoniemen te kunnen voorzien. Voor het formuleren van de beveiligingseisen zullen de normen die in de Algemene verordening gegevensbescherming en de Baseline Informatiebeveiliging Rijk zijn geformuleerd als uitgangspunt worden genomen. Zoals ook is gebeurd voor de leermiddelenketen, zullen voor andere specifieke gevallen eveneens onderzoeken en privacy impact assessments ten grondslag liggen aan de voorwaarden die gesteld worden aan het gebruik van een ketenID. Op deze wijze wordt, in combinatie met het begrenzen van het gebruik, het benoemen van de partijen die het ketenID mogen gebruiken en het stellen van nadere voorwaarden, gewaarborgd dat er de facto geen nieuw persoonsgebonden nummer geïntroduceerd wordt. Door deze opzet kunnen de publieke kaders op een goede manier worden geborgd en voorziet het wetsvoorstel tegelijkertijd in de gewenste flexibiliteit en toekomstbestendigheid. Er kan zodoende adequaat worden ingespeeld op toekomstige ontwikkelingen.

2. Doel van het wetsvoorstel

2.1. Doel

Het doel van het wetsvoorstel is om tot een adequate en toekomstbestendige oplossing voor digitale gegevensuitwisseling in het onderwijs te komen, die bijdraagt aan het verbeteren van de privacy van onderwijsdeelnemers en die het digitaal uitwisselen van gegevens veiliger en efficiënter maakt.

Een eerste specifieke doelstelling waarvoor dit mogelijk gemaakt wordt, richt zich op het gebruik van digitale leermiddelen, digitale toetsen en digitale examens. Het is belangrijk dat onderwijsdeelnemers toegang hebben tot de juiste digitale leermiddelen, toetsen en examens en deze ook kunnen gebruiken, met inachtneming van de Wbp. Daarnaast wordt in het wetsvoorstel voorzien in de mogelijkheid om bij algemene maatregel van bestuur vast te stellen dat onderwijsinstellingen andere pseudoniemen (ketenID's) voor onderwijsdeelnemers kunnen creëren, gebaseerd op het eenmalige pseudoniem, die kunnen worden gebruikt in de uitwisseling tussen de onderwijsinstelling en leveranciers.
Het gebruik van een ketenID is in ieder geval voorzien voor de toegang tot en het gebruik van digitale leermiddelen en het digitaal afnemen van toetsen en examens. Onder toegang wordt verstaan:
– het geleverd krijgen, dan wel in gebruik kunnen nemen, van digitale leermiddelen conform de afspraken die zijn gemaakt tussen de onderwijsinstelling en de leverancier. Hieronder valt ook het bestellen van leermiddelen;
– het kunnen inloggen op de digitale (leer)omgeving van een leverancier, waaronder de identificatie (wie ben je), authenticatie (klopt het dat je bent wie je zegt) en autorisatie (welke gebruiksrechten heb je).

Onder gebruik wordt verstaan: het geven en volgen van onderwijs en het begeleiden en volgen van onderwijsdeelnemers, waaronder:
– de opslag van leer- en toetsresultaten door leveranciers;

– het kunnen uitwisselen van leer- en toetsresultaten tussen leveranciers van digitale leermiddelen en het schoolinformatiesysteem;
– de analyse en interpretatie van leer- en toetsresultaten door leveranciers om leerstof en toetsmateriaal te kunnen aanbieden dat is afgestemd op de specifieke leerbehoefte van een onderwijsdeelnemer.

Ook wordt met dit voorstel beoogd dat dit ketenID kan worden gebruikt in de benodigde gegevensuitwisseling voor het digitaal afnemen van examens en toetsen, waaronder de wettelijk vastgelegde.

Door gebruik te maken van dit ketenID zijn een aantal andere identificerende gegevens niet langer noodzakelijk om een onderwijsdeelnemer te herkennen (zoals geboortedatum of geslacht). Dit leidt tot dataminimalisatie en een minder omvangrijke opslag van persoonsgegevens door de leveranciers. Op deze wijze wordt voorkomen dat onnodig persoonsgegevens worden verwerkt door leveranciers en ontwikkelaars van digitaal leermateriaal.

Het gebruik van een ketenID heeft als voordelen:
– het kunnen garanderen van een kwalitatief hoogwaardig proces van uitgifte van persistente digitale identiteiten;
– het voorkomen van matchingsproblemen bij het gebruik van verschillende identiteiten;
– het reduceren of voorkomen van verlies van onderwijstijd door problemen met identiteiten;
– een betere bescherming van persoonsgegevens door gebruik van een minimale set persoonskenmerken in de keten.

2.2. Bescherming van persoonsgegevens

Onderwijsinstellingen maken steeds meer gebruik van digitale leermiddelen bij het geven van onderwijs. Gebleken is dat daarbij regelmatig onnodig veel persoonsgegevens worden uitgewisseld tussen onderwijsinstellingen en leveranciers: gegevens die niet strikt noodzakelijk zijn voor het geven van goed onderwijs. Ouders moeten ervan uit kunnen gaan dat de onderwijsinstelling zorgvuldig omgaat met de gegevens van hun kinderen. Onderwijsdeelnemers verdienen de best mogelijke privacybescherming. Dit vloeit ook voort uit de Wbp. Ingevolge deze wet mogen verantwoordelijken (degenen die doel en middelen van de verwerking vaststellen) alleen persoonsgegevens verwerken voor zover dit noodzakelijk is voor het doel. Onderwijsinstellingen zijn 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. Het eerder genoemde privacyconvenant en de bijbehorende modelbewerkersovereenkomst ondersteunen de onderwijsinstelling hierbij (zie paragraaf 1.5).

Met het introduceren van een pseudoniem en ketenID's voor onderwijsdeelnemers wordt beoogd aan de onwenselijke situatie van onnodige gegevensuitwisseling een einde te maken. Naar verwachting levert het gebruik van pseudoniemen een wezenlijke bijdrage aan de bescherming van de persoonsgegevens van de onderwijsdeelnemer.

Er is uiteraard ook gekeken naar alternatieven. In de eerste plaats is de mogelijkheid van anonimisering 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.

In de tweede plaats is onderzocht of in plaats van het PGN een vaste set persoonsgegevens (bijvoorbeeld volledige naam, geboortedatum, geboorteplaats), die al bekend zijn bij de onderwijsinstelling, kan worden gebruikt als basis voor het pseudoniem. Hieraan kleeft echter een belangrijk bezwaar. Hoe meer gegevens, hoe zekerder de identiteit, maar des te groter de kans op fouten (bijvoorbeeld omdat een naam van een onderwijsdeelnemer op twee onderwijsinstellingen verschillend wordt gespeld), waardoor handmatige correcties nodig zijn bij alle partijen in de keten.

Aangezien bij het omzetten naar een pseudoniem gebruik wordt gemaakt van het PGN in het onderwijs, is aanpassing van de wet nodig. Ingevolge artikel 24 van de Wbp mag een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens immers slechts worden gebruikt ter uitvoering van de betreffende wet, dan wel voor doeleinden bij de wet bepaald. In overeenstemming met deze bepaling is het gebruik van het PGN in de onderwijswetten strikt gereguleerd: er is in de artikelen 178a WPO, 164a WEC, 103b WVO, 2.3.6a en 2.5.5a WEB en artikel 7.52 WHW, precies beschreven voor welke situaties en door wie het gebruik van het nummer is toegestaan en ten behoeve van welke doeleinden. De WPO BES, WVO BES en de WEB BES kennen vergelijkbare bepalingen voor het gebruik van het persoonsgebonden nummer BES. Het wetsvoorstel voorziet in de mogelijkheid voor het bevoegd gezag of het instellingsbestuur het PGN (of in voorkomend geval het PGN BES) van onderwijsdeelnemers te gebruiken voor het creëren van een pseudoniem, dat de basis vormt voor het genereren van andere pseudoniemen (ketenID's). Het eerste ketenID dat is voorzien wordt gebruikt in het kader van (het bieden van voorzieningen voor) de toegang tot en het gebruik van digitale leermiddelen en het digitaal afnemen van toetsen en examens.

In 2014 is over de betekenis van pseudonimiseren een belangrijke opinie verschenen van de artikel 29 Werkgroep van Europese privacytoezichthouders. De artikel 29 Werkgroep geeft in deze opinie aan dat pseudonimiseren een beveiligingsmethode is om privacyrisico's te verkleinen. Het is echter op zichzelf geen anonimiseringsmethode. In de opinie wordt tevens aangegeven dat pseudonimisering niet mag worden gezien als synoniem van anonimisering. Pseudonimisering beperkt alleen de koppelbaarheid van een dataset aan de oorspronkelijke identiteit van een betrokkene en is bijgevolg een nuttige maatregel om gegevens te beveiligen. Een belangrijke factor bij anonimiseren is dat de verwerking onomkeerbaar moet zijn. Bij pseudonimisering worden persoonsgegevens zodanig bewerkt dat de herleidbaarheid tot het individu weliswaar wordt beperkt, maar niet voorgoed onmogelijk wordt gemaakt. Pseudonimisering alleen is dus niet voldoende om een dataset volledig anoniem te maken. Daarmee blijven het persoonsgegevens en is de Wbp van toepassing. Het College bescherming persoonsgegevens (de voorganger van de AP) heeft deze zienswijze bevestigd in het onderzoek dat het in december 2015 heeft aangekondigd naar de verstrekking door de Nederlandse Zorgautoriteit (NZa) van gegevens uit het Diagnose Informatie Systeem (DIS).[9]

Aangezien pseudoniemen persoonsgegevens blijven, moet pseudonimiseren plaatsvinden in overeenstemming met de Wbp. Een persoonsgegeven is in de Wbp gedefinieerd als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1, sub a, Wbp). Om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij

[9] https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-doet-onderzoek-dis-gegevens-bij-nza.

redelijkerwijs door degene die voor de verwerking verantwoordelijk is, dan wel door enig ander persoon, zijn in te zetten om genoemde persoon te identificeren. Gepseudonimiseerde gegevens leiden weliswaar niet direct tot identificatie van een bepaalde persoon, maar door combinatie met andere gegevens, kunnen ze wel in verband worden gebracht met een bepaalde persoon. In dat geval is sprake van indirect identificerende gegevens.

Digitale leermiddelen vragen voor een goede werking en vanuit het onderwijsbelang om het gebruik van een aantal persoonskenmerken, bijvoorbeeld de voornaam, de groep of het niveau van de onderwijsdeelnemer. Dit is ook nodig opdat leraren direct kunnen zien welke onderwijsdeelnemer (en niet welk ketenID) welke resultaten behaalt. Gebruik van het ketenID betekent dus niet dat er geen persoonsgegevens meer uitgewisseld worden. Het is aan de onderwijsinstelling als verantwoordelijke om daar zorgvuldige keuzes in te maken. Zodra een leverancier van digitale leermiddelen stopt met het aanbieden daarvan, bijvoorbeeld omdat de contractuele relatie met de onderwijsinstelling eindigt, dient hij binnen het daarvoor geldende regime van de Wbp zorg te dragen voor verwijdering van alle persoonsgegevens, inclusief de ketenID's van de betreffende onderwijsdeelnemers.

Door het toepassen van encryptie (dataversleuteling) op zowel het PGN, als op het pseudoniem en ketenID's, wordt het risico op identificeerbaarheid van onderwijsdeelnemers tot een minimum gereduceerd. De leveranciers zijn gehouden om pseudoniemen op een zodanig beveiligde wijze in hun administratie te bewaren, dat er geen koppeling kan plaatsvinden met gegevenssets van onderwijsdeelnemers die voor andere doeleinden zijn verkregen.

2.3. Reikwijdte van pseudoniemen

Het is niet de bedoeling dat het pseudoniem of één van de ketenID's een persoonsnummer wordt en de functie van het PGN in het onderwijs overneemt. Het pseudoniem wordt niet gebruikt in de digitale uitwisseling van gegevens tussen de onderwijsinstelling en een derde partij. KetenID's worden alleen geïntroduceerd wanneer het gebruik daarvan een beperkte reikwijdte heeft. Voorafgaand aan het introduceren van een nieuw ketenID zal onderzoek en een privacy impact assessment worden verricht om zeker te stellen dat de reikwijdte beperkt is en blijft. Het eerste ketenID is op dit moment voorzien bij de uitwisseling van gegevens tussen de onderwijsinstelling en haar leveranciers in het kader van de toegang tot en het gebruik van digitale leermiddelen en voor het digitaal afnemen van toetsen en examens. Dit ketenID heeft daardoor een beperkte reikwijdte. Het pseudoniem wordt ook in reikwijdte beperkt doordat het wijzigt zodra een onderwijsdeelnemer overstapt naar een andere sector. In de uitgevoerde Privacy Impact Assessment (PIA) wordt deze conclusie onderschreven.

In het wetsvoorstel wordt voorzien om bij algemene maatregel van bestuur vast te leggen voor welke specifieke gevallen een ander pseudoniem (ketenID) gebruikt mag worden. Dit betekent dat voor elk geval een ander ketenID gegenereerd wordt, waardoor er geen risico op koppelbaarheid ontstaat en de reikwijdte van elk ketenID per definitie al beperkt is. Om zeker te stellen dat de reikwijdte beperkt genoeg is zal een PIA worden uitgevoerd voor de introductie van een nieuw ketenpseudoniem. Een specifieke beschrijving van het geval bij algemene maatregel van bestuur en het stellen van nadere voorwaarden bij ministeriële regeling borgen op transparante wijze dat deze reikwijdte beperkt is en blijft.

Het gebruik van pseudoniemen wordt niet voorgeschreven. Aangezien onderwijsinstellingen zorgdragen voor het geven van 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. Zo sluiten onderwijsinstellingen bijvoorbeeld bewerkersovereenkomsten met leveranciers van digitale leermiddelen die zij zelf kunnen kiezen. Deze eigen verantwoordelijkheid van de onderwijsinstelling is een belangrijke reden om niet tot het gebruik van pseudoniemen te verplichten. Bovendien zal het gebruik van pseudoniemen voor onderwijsinstellingen in de praktijk standaard worden, aangezien leveranciers afspraken maken met onderwijsinstellingen over het gebruik van pseudoniemen en daar hun systemen op aanpassen. Dit wetsvoorstel verplicht dan ook niet tot het gebruik van pseudoniemen, maar stelt onderwijsinstellingen in staat een ketenID te hanteren als zij gegevens uitwisselen met andere partijen voor welomschreven, specifieke gevallen die bij algemene maatregel van bestuur worden aangewezen, zoals voor het gebruik van digitale leermiddelen, digitaal toetsen of digitaal afnemen van examens in dit wetsvoorstel geschiedt. Door het juridisch mogelijk maken en borgen van dit stelsel van pseudoniemen, faciliteert de overheid de onderwijsinstellingen zodat zij dataminimalisatie kunnen toepassen. Met de afspraken in het privacyconvenant en de bepalingen in de modelbewerkersovereenkomst wordt een zo goed mogelijk gebruik van het ketenID voor digitale leermiddelen bereikt. Een onderwijsinstelling kan gegronde redenen hebben om geen gebruik te maken van het ketenID. Bijvoorbeeld omdat de onderwijsinstelling zelf al andere maatregelen heeft getroffen om persoonsgegevens te beschermen. Gelet op de norm van dataminimalisatie geldt op grond van de Wbp dat partijen in alle gevallen moeten aangeven voor welk doel de verwerking van die persoonsgegevens noodzakelijk is en welke waarborgen zijn getroffen om de privacy van betrokkenen op adequate wijze te waarborgen.

De keuze voor zelfregulering kan op gespannen voet 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. Daarbij zal onderzocht worden of onderwijsinstellingen 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 de aanvullende persoonsgegevens die mogen worden verstrekt.

2.4. Hoe komt een pseudoniem en ketenID tot stand?

Om een pseudoniem en ketenID's te genereren is er een centraal georganiseerde nummervoorziening gerealiseerd. Dit is een voorziening voor het aanmaken, wijzigen en verwijderen van een pseudoniem en ketenID's. Het proces om te komen tot een pseudoniem en vervolgens een ketenID voor toegang tot en gebruik van digitale leermiddelen, toetsen en examens ziet er als volgt uit:

1. De onderwijsinstelling kan het PGN bij DUO verifiëren, om zeker te stellen dat de juiste identiteit van een onderwijsdeelnemer gebruikt wordt om een pseudoniem op te baseren. De onderwijsinstelling geeft het schoolinformatiesysteem de opdracht om het PGN onomkeerbaar te versleutelen voordat dit door het schoolinformatiesysteem naar de nummervoorziening wordt verstuurd om een pseudoniem te genereren. Dit wordt gedaan ter beveiliging, om te

voorkomen dat het PGN als PGN naar de nummervoorziening verzonden wordt. In de nummervoorziening zelf worden geen andere persoonsgegevens verwerkt dan het versleutelde PGN en het naar de onderwijsinstelling terug te sturen pseudoniem. In de nummervoorziening worden geen gegevens opgeslagen.

2. Het pseudoniem wordt binnen de nummervoorziening gegenereerd op basis van het versleutelde PGN. Het pseudoniem wordt geretourneerd naar de onderwijsinstelling en bewaard in het schoolinformatiesysteem.
3. Het pseudoniem wordt naar de nummervoorziening gestuurd, op basis daarvan wordt een ketenID gegenereerd op basis van een combinatie van a) het pseudoniem, b) een aanduiding van het geval waarvoor het ketenID wordt gebruikt (in dit geval de toegang tot en het gebruik van digitale leermiddelen, toetsen en examens) en c) de onderwijssector. Door deze meervoudige basis is het ketenID niet meer aan te merken als een «een-op-een» pseudoniem van (enkel) het pseudoniem. Het ketenID varieert daarmee, ook al is dit steeds gebaseerd op hetzelfde pseudoniem van de onderwijsdeelnemer en per geval waarvoor het pseudoniem gebruikt wordt.
4. Op het moment dat onderwijsdeelnemers digitale leermiddelen gaan gebruiken of digitale toetsen of examens afnemen, wordt dit ketenID gebruikt in de uitwisseling tussen het schoolinformatiesysteem en de leverancier(s) van de betreffende leermiddelen, dan wel toetsen of examens, om de toegang te regelen en het gebruik mogelijk te maken.
5. Het pseudoniem en de ketenID's zijn door hun verschijningsvorm geschikt voor verwerking door computers en vrijwel niet door mensen. Deze zijn namelijk niet leesbaar op een scherm of simpel over te schrijven. In die zin wijken het pseudoniem en ketenID's wezenlijk af van het PGN zelf. Om het risico van inbreuk op de bescherming van persoonsgegevens van onderwijsdeelnemers als gevolg van datalekken te minimaliseren, worden het pseudoniem en de ketenID's versleuteld vastgelegd in de schoolinformatiesystemen.

De nummervoorziening is centraal ontwikkeld door Stichting Kennisnet voor het gehele onderwijs. Het voornemen is om de nummervoorziening voor het po, vo en mbo onder te brengen in de ICT-basisinfrastructuur die Stichting Kennisnet beheert. Door middel van een derdenverklaring kan de kwaliteitsborging voor onderwijsinstellingen en leveranciers worden geregeld.[10] Onderwijsinstellingen sluiten met de beheerder van de nummervoorziening een bewerkersovereenkomst waarin de gegevensuitwisseling tussen de onderwijsinstelling en de nummervoorziening is vastgelegd. Het gebruik van pseudoniemen moet op een goede manier bij de leveranciers ingevoerd worden, zodat de scholen er zonder problemen mee kunnen werken. Om dit te borgen zijn bestuurlijke afspraken gemaakt met leveranciers en is een apart programma ingericht dat de implementatie coördineert en zorgdraagt voor een geruisloze invoering op scholen.

De Wbp stelt dat maatregelen genomen dienen te worden om de beveiliging van persoonsgegevens op een passend niveau te brengen en houden. De nieuwe mogelijkheden die technologische ontwikkelingen meebrengen, maken dat hier een continue verbetering in wordt aangebracht. In de ministeriële regeling zullen de actuele beveiligingsmaatregelen worden beschreven, zodat transparant is op welke manier een veilige omgang met de pseudoniemen en ketenID's zekergesteld wordt. Tot slot participeert de onderwijssector met het oog op de voortschrijdende techniek en de veranderende eisen aan privacy en beveiliging in de

[10] Een derdenverklaring is een verklaring die afgegeven wordt door een onafhankelijke auditpartij over de kwaliteit van de ICT-dienstverlening en -beheersing van een organisatie.

ontwikkeling van de Generieke Digitale Infrastructuur (GDI) van de overheid.[11] Het is voor de onderwijssector van belang om te borgen dat de stappen die gezet worden in lijn zijn met het rijksbrede initiatief om tot een standaard voor de toegang tot online dienstverlening te komen.

2.5. Aanvullende maatregelen

Naast de introductie van het pseudoniem en ketenID's wordt in het onderwijs een aantal andere maatregelen getroffen, die gezamenlijk tot de beoogde verbetering van de privacy en de omgang met persoonsgegevens moeten leiden:
– de invoering van het hierboven beschreven convenant «Digitale Onderwijsmiddelen en Privacy – Leermiddelen en Toetsen» voor po en vo en het gebruik van de modelbewerkersovereenkomst door partijen;
– de sectorraden in po, vo en mbo en Kennisnet ondersteunen onderwijsinstellingen en instellingen op het gebied van informatiebeveiliging en privacy. Door middel van concrete producten wordt gewerkt aan de bewustwording van en ondersteuning bij deze onderwerpen bij onderwijsinstellingen en aan gedragsverbetering;
– bij de totstandkoming van sectorale inkoopvoorwaarden in het po en vo wordt een relatie gelegd met de modelbewerkersovereenkomst;
– er is binnen Edu-K een aangescherpt attributenbeleid vastgesteld, waarin is vastgelegd welke gegevens op welk moment tussen welke partijen worden gedeeld. Dit leidt ertoe dat er minder gegevens worden gedeeld tussen onderwijsinstellingen en leveranciers. Dit beleid wordt binnen Edu-K stelselmatig geëvalueerd en zonodig aangescherpt.

3. Samenwerking Inspectie van het Onderwijs met de AP

De Inspectie van het Onderwijs (hierna: inspectie) en de AP werken sinds 1 januari 2016 samen aan een efficiënt en effectief toezicht op de verwerking van persoonsgegevens door onderwijsinstellingen. Deze organisaties hebben in een samenwerkingsovereenkomst afgesproken hoe zij elkaar informeren. De overeenkomst houdt samengevat het volgende in:
– 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.

4. Reactie onderwijsorganisaties en uitkomst internetconsultatie

Het conceptwetsvoorstel is tussen 18 mei en 16 juni 2016 in een openbare internetconsultatie voorgelegd aan belanghebbenden en geïnteresseerden. Er zijn veertien reacties binnengekomen.

[11] De GDI bestaat uit herbruikbare digitale basisvoorzieningen, standaarden en producten die het overheden, publieke organisaties en private partijen mogelijk maken om hun primaire processen doelmatig in te richten en te blijven ontwikkelen.

De noodzaak van het aanpassen van de wet wordt door niemand ter discussie gesteld. De sectororganisaties in het po, vo en mbo benadrukken allemaal het belang van een unieke, persistente identiteit van onderwijsdeelnemers voor toegang en gebruik van digitale leermiddelen. Tevens benadrukken zij dat er een bredere behoefte is om ook voor andere gevallen gebruik te kunnen maken van een (ander) pseudoniem. Gebleken is dat deze behoefte ook bestaat in het hoger onderwijs. Naar aanleiding van de internetconsultatie en overleg met de sector hoger onderwijs wordt dan ook voorgesteld om de relevante artikelen in de WHW op vergelijkbare wijze aan te passen.

Pseudonimiseren wordt door vrijwel iedereen als (onderdeel van) de gewenste oplossing voor het verbeteren van de privacy van onderwijsdeelnemers gezien. Vier indieners geven in hun reactie aan dat de wijze van pseudonimiseren hen niet ver genoeg gaat en dat er alternatieven zijn die de privacy van de onderwijsdeelnemers nog beter beschermen. De in de reacties aangedragen alternatieven zijn echter onderzocht en bekend bij de ontwikkelaars. De keuze voor de wijze waarop de pseudoniemen tot stand komen en de bijbehorende beveiligingseisen (waaronder de mate van encryptie van gegevens) zijn gebaseerd op twee overwegingen. De eerste is de huidige stand van de techniek. 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 teveel onzekerheden met zich meebrengen. De tweede overweging is de snelheid waarmee alle leveranciers de benodigde aanpassingen in hun systemen kunnen aanbrengen. Hoe moderner de techniek, hoe langer het duurt voordat alle partijen zijn aangesloten.

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 niveau van een ministeriële regeling nadere voorwaarden te stellen aan het pseudoniem en ketenID's.

De memorie van toelichting is op basis van de reacties op enkele punten verduidelijkt.

5. Reactie Autoriteit Persoonsgegevens (AP)

Op 8 november 2016 heeft de AP haar advies uitgebracht over een eerdere versie van dit wetsvoorstel. De AP heeft daarin het volgende geadviseerd:

a. De AP adviseert om in de toelichting op het wetsvoorstel nader te motiveren waarom een pseudoniem noodzakelijk is en op welke wijze een pseudoniem tot dataminimalisatie leidt.
b. De AP adviseert om nader toe te lichten door wie, wanneer en op welke wijze pseudoniemen aan elkaar kunnen worden gekoppeld.
c. De AP constateert dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. De AP adviseert om deze bedreiging te betrekken in de onderbouwing van de noodzaak voor de voorgestelde pseudonimisering.
d. De AP constateert dat het PGN kan worden aangemerkt als een identificerend nummer dat bij wet is voorgeschreven als bedoeld in artikel 24 van de Wbp. Dit betekent dat niet bij ministeriële regeling mag worden bepaald dat het PGN mag worden gebruikt om een

pseudoniem te genereren voor andere gevallen. De AP adviseert om expliciet in het wetsvoorstel of in de toelichting daarop aan te geven dat andere pseudoniemen niet worden gebaseerd op het PGN, tenzij zulks geschiedt bij formele wet.

De adviezen van de AP hebben geleid tot aanpassing van het wetsvoorstel. De adviezen zijn als volgt verwerkt:

a. In de toelichting is nader gemotiveerd hoe de invoering van pseudoniemen tot dataminimalisatie leidt. In de huidige situatie worden veelal persoonsgegevens gebruikt voor de identificatie van onderwijsdeelnemers. Met de invoering van een ketenID hoeven alleen nog maar die persoonsgegevens uitgewisseld te worden die nodig zijn voor het beoogde doel. Bij het gebruik van digitale leermiddelen hoeft dan bijvoorbeeld de geboortedatum of het geslacht van een leerling niet langer meegestuurd te worden om zeker te weten dat de school en de leverancier het over dezelfde leerling hebben, het ketenID zorgt daarvoor.
b. De onderwijsinstelling beschikt in juridische zin als verantwoordelijke over het PGN, het pseudoniem en ketenID's. In de praktijk krijgen de partijen waarmee de school gegevens uitwisselt enkel een ketenID. Voor zover dat verschillende gevallen betreft, is dat elke keer een ander ketenID. In het administratiesysteem van de school worden het PGN, pseudoniem en de ketenID's zowel gescheiden van elkaar als gescheiden van de (ten opzichte van het pseudoniem) aanvullende persoonsgegevens van de onderwijsdeelnemer bewaard, zoals wordt vereist op grond van de Algemene verordening gegevensbescherming. Het pseudoniem en ketenID's zijn unieke identiteiten in de computersystemen van de school, verschijnen niet op het scherm en zijn in die zin niet door mensen te verwerken. Alleen in het geval dat de onderwijsinstelling als verantwoordelijke aan het administratiesysteem als bewerker de opdracht geeft om de koppeling tussen deze gegevens te maken, zullen deze aan elkaar gekoppeld worden.
c. Zoals onder b beschreven is de onderwijsinstelling de enige die over het pseudoniem en de ketenID's beschikt en rechtmatig een koppeling zou kunnen leggen. Het risico op een onrechtmatige koppeling van gegevens is tot een minimum beperkt. Alleen in het – zeer onwaarschijnlijke – geval dat zowel binnen administratiesystemen de beveiliging het op meerdere plekken laat afweten (omdat de gegevens gescheiden worden opgeslagen in de administratie van de school) en dit gelijktijdig bij systemen van leveranciers gebeurt, kunnen onbevoegden de gegevens koppelen. In de huidige situatie is dat ook het geval, het gebruik van een pseudoniem en ketenID's brengt geen aanvullend risico mee. Omdat door een ketenID minder persoonsgegevens beschikbaar zijn bij leveranciers van digitaal leermateriaal betekent dit zelfs een verlaging van het risico dat identificerende persoonsgegevens met leerresultaten in onbevoegde handen komen (zie ook conclusie van de PIA onder paragraaf 6).
d. In de versie van het wetsvoorstel dat de AP heeft beoordeeld, was voorzien in het gebruik van het PGN voor elk ketenID. De gevallen waarvoor en voorwaarden waaronder andere ketenID's gegenereerd en gebruikt konden worden, zouden bij ministeriële regeling worden vastgesteld. De AP constateert terecht dat dit zou betekenen dat het gebruik van het PGN voor andere gevallen niet bij wet zou worden vastgesteld, hetgeen in strijd is met artikel 24 van de Wbp. Dit heeft tot een belangrijke herziening van het wetsvoorstel en de techniek van pseudonimiseren geleid. In het onderhavige wetsvoorstel is de mogelijkheid voorzien voor onderwijsinstellingen om een pseudoniem op het PGN te baseren. KetenID's die voor specifieke gevallen kunnen worden gebruikt, worden op het pseudoniem gebaseerd. Dit heeft een aantal belangrijke voordelen. Zo wordt het PGN niet voor

meer gevallen gebruikt dan strikt noodzakelijk, slechts voor het eenmalig genereren van een pseudoniem. Het pseudoniem is naar zijn aard geen persoonsnummer als bedoeld in artikel 24 van de Wbp. Bovendien wordt het pseudoniem niet voorgeschreven en alleen binnen het administratiesysteem van de school bewaard, gescheiden van andere (persoons)gegevens. Door ketenID's op het pseudoniem te baseren worden alle technische voordelen behouden: een identiteit die kwalitatief hoogwaardig en persistent is, waarmee dataminimalisatie, vermindering van administratieve lasten op onderwijsinstellingen en het uitoefenen van het toekomstig recht op dataportabiliteit van onderwijsdeelnemers geborgd wordt. Door de andere gevallen waarvoor een ketenID gebruikt mag worden bij algemene maatregel van bestuur te regelen en de voorwaarden waaronder vervolgens in een ministeriële regeling vast te leggen, wordt het gebruik hiervan op een betere manier dan in de huidige situatie gereguleerd, met behoud van de benodigde flexibiliteit zodat adequaat op toekomstige ontwikkelingen kan worden ingespeeld.

6. Uitkomsten Privacy Impact Assessment (PIA)

Er is een PIA uitgevoerd over het gebruik van de nummervoorziening in de leermiddelenketen. Met het PIA is getoetst of de voorgenomen gegevensverwerking doorgang dient te vinden, welke gegevensverwerkingen dan noodzakelijk zijn en, vervolgens, hoe deze gegevensverwerkingen met inachtneming van de Wbp plaats kunnen vinden. Daarmee brengt het PIA de risico's op het gebied van privacy en gegevensverwerking in kaart en bevat deze een voorstel voor passende beveiligingsmaatregelen. Op basis van het PIA kan gesteld worden dat het gebruik van een ketenID als vervanger van een uitgebreidere dataset, leidt tot dataminimalisatie en daarmee tot het reduceren van de kans op koppelbaarheid van gegevens van onderwijsdeelnemers. Ook constateert het PIA dat het gebruik van het PGN als basis voor het pseudoniem niet leidt tot extra risico's op koppelbaarheid van de gegevens van onderwijsdeelnemers. De voorgestelde passende beveiligingsmaatregelen zijn onverkort overgenomen in de realisatie en invoering van het pseudoniem.

Hieronder volgen de belangrijkste conclusies van het PIA.

6.1. Toets op de doelen, noodzakelijkheid en passend gebruik

Ten aanzien van de doelen van gegevensverwerking en de noodzakelijkheid van het gebruik van gegevens, concludeert het PIA dat:
– om onderwijsdeelnemers te identificeren zonder gebruik te maken van datasets met daarin direct identificerende gegevens (zoals naam en adres) een identificator noodzakelijk is.

Ten aanzien van de noodzakelijkheid van een identificator en de noodzakelijkheid van een nummer als identificator, concludeert het PIA dat:
– een ketenID de voorkeur verdient als identificator binnen de leermiddelenketen boven datasets met NAW-gegevens en boven direct identificerende nummers, zoals het PGN;
– de identificator (het ketenID) met name een administratieve functie vervult en, bij het gebruik van bepaalde digitale leermiddelen, de bevoegdheid representeert om die leermiddelen te gebruiken. De identificator is geen nummer dat het resultaat is van een voorafgaande identiteitscontrole.

Belangrijke constateringen ten aanzien van het passend gebruik zijn:
– Het privacyconvenant en de bijbehorende bewerkersovereenkomst zijn essentiële voorwaarden om de machtsverhouding tussen onderwijs-

instellingen en leermiddelenproducenten (distributeurs en uitgevers) in balans te krijgen.
– Ook de beheerder van de nummervoorziening en de beheerders van de inlogfaciliterende applicaties zijn aan te merken als Wbp-bewerkers voor de onderwijsinstellingen;
– Het PGN is het eerst voor de hand liggende nummer om als basis voor het ketenID van onderwijsdeelnemers te gebruiken.

6.2. Risicoanalyse

In de risicoanalyse die door middel van het PIA is uitgevoerd, worden zes privacyrisico's geduid:
1. Verspreiding van direct identificerende gegevens over/binnen de leermiddelenketen;
2. Distributeurs en uitgevers verwerken gegevens (als bewerker) op een manier die zich aan het zicht van onderwijsinstellingen onttrekt ofwel waar de onderwijsinstellingen zich niet (volledig) bewust van zijn;
3. Distributeurs en uitgevers gebruiken de gegevens – waarover zij in het kader van hun rol in de leermiddelenketen beschikken – voor de eigen bedrijfsvoering of voor commerciële benadering van onderwijsdeelnemers of ouders;
4. Rechtmatigheidsproblemen die ontstaan doordat het gebruik van nummers breder is dan met betrekking tot persoonsidentificerende nummers binnen de wet is toegestaan;
5. Gegevenssets die op basis van verschillende doelen zijn verkregen worden op basis van het ketenpseudoniem aan elkaar gekoppeld waardoor een grotere gegevensset ontstaat;
6. Resultaten van onderwijsdeelnemers worden gebruikt als personeelsvolgsysteem van de docent.

Met de invoering van het pseudoniem, de wijze waarop de nummervoorziening is ontworpen en de totstandkoming van het privacyconvenant worden bovenstaande risico's 1 en 2 adequaat ondervangen. Voor risico 6 is de conclusie dat dit niet speelt bij de nummervoorziening. Risico's 3, 4 en 5 worden (groten)deels aangepakt en het PIA stelt een aantal aanvullende maatregelen voor. Deze maatregelen zijn:
– voorafgaande toestemming van de onderwijsinstelling voor hergebruik van gegevens door leveranciers. Daarnaast zal er in de praktijk ook en vooral aandacht dienen te zijn voor de vraag of en welk hergebruik rechtmatig en toelaatbaar is. Hierover zijn afspraken gemaakt in het privacyconvenant;
– datascheiding tussen de gegevens van distributeurs en uitgevers om te voorkomen dat gegevenssets die op basis van verschillende doelen zijn verkregen op basis van het pseudoniem aan elkaar worden gekoppeld waardoor een grotere gegevensset ontstaat (koppelingsrisico, ook bij eventuele datalekken);
– datascheiding bij gegevensbestanden die distributeurs gebruiken, tussen het pseudoniem, ketenID's en NAW-gegevens betreffende de aflevering en betaling van leermiddelen. Deze scheiding kan worden doorgevoerd zodra de aflevering en de betaling van de leermiddelen hebben plaatsgevonden;
– encryptie van het pseudoniem, ketenID's (en het PGN) in de systemen van de leveranciers.

Deze aanbevelingen zijn onverkort overgenomen en worden meegenomen in de realisatie en invoering van het pseudoniem en ketenID's.

7. Positie Caribisch Nederland

Het uitgangspunt bij de onderwijswetgeving in Caribisch Nederland is dat deze niet onnodig uit de pas loopt met de wetgeving in Europees Nederland.[12] Daarom wordt voorgesteld om de wetgeving ook voor Caribisch Nederland aan te passen. Uiteraard wordt er rekening gehouden met het feit dat de lokale context op de eilanden anders is. De Rijksdienst Caribisch Nederland heeft een concept van het wetsvoorstel ter consultatie voorgelegd in Caribisch Nederland. Naar aanleiding van de consultatie zijn geen vragen en opmerkingen ontvangen en is het wetsvoorstel ten gevolge daarvan niet meer aangepast.

De wijziging van de artikelen in de WPO BES, de WVO BES en de WEB BES (artikelen II, V en VII) heeft betrekking op artikelen die nog niet in werking zijn getreden. Het betreft de artikelen 147 WPO BES, 179 WVO BES en 2.3.4 WEB BES.[13] Dit betekent dat de desbetreffende wijzigingsvoorstellen pas van kracht worden op het tijdstip waarop de genoemde artikelen in werking treden. Het is nog niet bekend wanneer dat gaat gebeuren.

Dit wetsvoorstel zal naar verwachting niet al op korte termijn gevolgen hebben voor Caribisch Nederland. In beginsel kunnen alle scholen en instellingen die over het PGN BES beschikken, gebruik maken van de nummervoorziening om een pseudoniem en ketenID's te laten genereren. Voorwaarde is wel dat de leveranciers hun systemen daarop aangepast hebben.

8. Uitvoering en handhaving

Stichting Kennisnet is verantwoordelijk voor de realisatie van de nummervoorziening. Voordat het ketenID voor de leermiddelenketen daadwerkelijk gebruikt kan worden, zullen de leveranciers hun systemen moeten aanpassen. De betrokken partijen (PO-Raad, VO-raad, MBO Raad, Kennisnet) en leveranciers werken samen aan een zorgvuldige invoering. Voor het toezicht op de naleving is in het privacyconvenant vastgelegd dat zowel het Platform Edu-K als de Autoriteit Persoonsgegevens een rol hebben bij het houden van toezicht op de naleving van het convenant en de Wbp. Daarnaast werken de Inspectie van het Onderwijs en de Autoriteit Persoonsgegevens samen aan een efficiënt en effectief toezicht op de verwerking van persoonsgegevens door onderwijsinstellingen (zie ook hoofdstuk 3).

9. Administratieve lasten

De invoering van het pseudoniem en ketenID's zal voor onderwijsinstellingen een administratieve lastenvermindering opleveren. De gegevensuitwisseling tussen het schoolinformatiesysteem en de nummervoorziening en de uitwisseling met bevoegde partijen zal volledig geautomatiseerd plaatsvinden. Dit vergt geen additionele handelingen van de onderwijsinstelling in vergelijking met de huidige praktijk. Door de invoering van ketenID's zal de foutgevoeligheid van gegevensuitwisselingen afnemen. De fouten maken nu administratieve correcties door de onderwijsinstelling noodzakelijk en leiden in het geval van digitale leermiddelen tot ongewenste lesverstoringen op momenten dat onderwijsdeelnemers geen toegang hebben tot hun leermiddelen. De huidige praktijk laat zien dat deze fouten vooral in het voortgezet onderwijs een probleem zijn en geschat wordt dat een gemiddelde onderwijsinstelling

[12] Kamerstukken I 2011/12 33 000 VII, nr. C, p. 2.
[13] Tweede Aanpassingswet openbare lichamen Bonaire, Sint Eustatius en Saba-B, Stb. 2011, 33.

minimaal drie uur per jaar met correcties bezig is. Dat aantal loopt snel op als er serieuze problemen zijn.

Het digitaal afnemen van toetsen en examens met behulp van een pseudoniem betekent voor onderwijsinstellingen dat zij niet langer zelf een administratieve handeling hoeven te verrichten om de resultaten te koppelen aan hun onderwijsdeelnemers. De vertaalslag van pseudoniem naar onderwijsdeelnemer vindt geautomatiseerd plaats in het administratiesysteem van de school.

De omvang van de administratieve lastenvermindering voor het gebruik van ketenID's voor andere gevallen is nu niet bekend, evenwel is helder dat daar ook een vermindering van de administratieve last mee zal worden bereikt.

10. Financiële gevolgen

De invoering van het pseudoniem en ketenID's heeft geen directe financiële gevolgen voor onderwijsinstellingen. De incidentele, centrale ontwikkelkosten (ca. € 500.000) van de nummervoorziening en het beheer daarvan worden gefinancierd door de Minister van OCW. Leveranciers maken kosten om de aanpassingen in hun systemen te kunnen doen.

B. Artikelsgewijs

Artikelen I, III, IV, VI en VIII

Met de wijziging van de artikelen 178a van de WPO, 164a van de WEC, 103b van de WVO, 2.3.6a en 2.5.5a van de WEB, en 7.52 van de WHW wordt voor het bevoegd gezag een grondslag gecreëerd om het PGN van een onderwijsdeelnemer eenmalig te gebruiken ten behoeve van het genereren van een pseudoniem voor een onderwijsdeelnemer met het oog op het bieden van voorzieningen in het kader van het geven van onderwijs en de begeleiding van leerlingen, deelnemers, studenten en extraneï. Het bevoegd gezag draagt er zorg voor dat dit pseudoniem en het andere pseudoniem, waarop hieronder verder wordt ingegaan, uitsluitend wordt bewaard in de systemen van de leveranciers waarin de onderwijsdeelnemers zijn geregistreerd. Dit pseudoniem kan vervolgens worden gebruikt voor het genereren van een ander pseudoniem (ketenID) voor gegevensuitwisseling met leveranciers in het kader van de toegang tot en het gebruik van de digitale leermiddelen of in het kader van het digitaal afnemen van toetsen, examens, of in het hoger onderwijs ook tentamens, waaronder de wettelijk verplichte toetsen en examens. Het gaat hierbij om een ketenID gekoppeld aan het gebruik van digitale leermiddelen en het digitaal afnemen van toetsen en examens. Dit andere pseudoniem wordt uitsluitend verstrekt aan een leverancier die een digitaal product of een digitale dienst aanbiedt bestaande uit leerstof of toetsen en de daarmee samenhangende digitale diensten. Hierbij kan worden gedacht aan een centraal examensysteem dat toetsen en examens digitaal afneemt. Tevens kan het pseudoniem worden gebruikt voor het genereren van een ander pseudoniem voor een ander geval bepaald bij algemene maatregel van bestuur, waarbij in elk geval de categorieën van ontvangers worden aangewezen. Op deze mogelijkheid wordt hieronder verder ingegaan. Onder digitaal afnemen wordt begrepen: het volledige proces van plannen, inroosteren, afnemen, verwerken en terugkoppelen van de resultaten van toetsen en examens.

Deze bepaling geldt alleen voor zover toetsen en examens daadwerkelijk digitaal worden afgenomen; op het analoog afnemen van toetsen en examens is deze bepaling niet van toepassing. De wettelijk verplichte

toetsen en examens in het funderend onderwijs zijn: de eindtoets (artikel 9b van de WPO), het eindexamen (v)so (artikel 47 van de WEC) en het eindexamen vo, waarvan de rekentoets een onderdeel vormt (artikel 29 van de WVO).[14] In het mbo zijn dit de examens, bedoeld in de artikelen 7.4.2 (beroepsopleidingen) en 7.4.11 van de WEB (opleidingen vavo en opleidingen Nederlands als tweede taal). In het ho gaat het om de tentamens en examens, bedoeld in artikel 7.10 van de WHW. De WEB kent overigens twee bepalingen voor het gebruik van het PGN door het bevoegd gezag: artikel 2.5.5a regelt het gebruik van dit nummer voor het beroepsonderwijs en artikel 2.3.6a regelt dit voor opleidingen educatie, waaronder het voortgezet algemeen volwassenenonderwijs. In paragraaf 2.4 is ingegaan op de wijze waarop het pseudoniem tot stand komt. Het wetsvoorstel voorziet daarnaast in de mogelijkheid om bij algemene maatregel van bestuur andere gevallen aan te wijzen dan de wettelijke opgesomde gevallen van het bieden van voorzieningen in het kader van de toegang tot en het gebruik van digitale leermiddelen of het digitaal afnemen van toetsen. Hierbij geldt dat per geval, bepaald bij algemene maatregel van bestuur, een afzonderlijk pseudoniem wordt gegenereerd. Zoals hierboven aangegeven, wordt hiervoor het pseudoniem, genereerd op basis van het eenmalig gebruikte PGN van de leerling, deelnemer, student of extraneus, gebruikt. Er zijn immers ook andere situaties denkbaar waarin onderwijsinstellingen behoefte kunnen hebben aan een unieke digitale identiteit, bijvoorbeeld bij de gegevensuitwisseling tussen scholen en samenwerkingsverbanden in het kader van passend onderwijs (zie paragraaf 1.3). Tevens worden in deze algemene maatregel van bestuur de categorieën van ontvangers van dit andere pseudoniem aangewezen. Over de voorwaarden waaronder de pseudoniemen (met inbegrip van de ketenID's) kunnen worden gebruikt, worden bij ministeriële regeling nadere regels gesteld. Deze voorwaarden hebben in ieder geval betrekking op de duur en de beveiliging, waaronder de gescheiden opslag van de pseudoniemen. Met de duur van het pseudoniem wordt geregeld dat deze wordt beperkt tot de desbetreffende onderwijssector. Dit betekent dus bijvoorbeeld dat als een leerling van het primair onderwijs overgaat naar het voortgezet onderwijs, dat er voor deze leerling een ander pseudoniem zal worden gegeneerd. Dit om te voorkomen dat een pseudoniem door langdurig gebruik de facto een nieuw persoonsgebonden nummer wordt. In de artikelen 188d van de WPO, 173d van de WEC, 123c van de WVO, 12.5.1a van de WEB, en 19.1a van de WHW is een evaluatiebepaling opgenomen. De effecten van de maatregelen in het kader van de pseudonimisering worden binnen vijf jaar geëvalueerd. De regering besteedt zoals gebruikelijk het onderzoek aan bij een wetenschappelijk onderzoeksbureau en zal zich laten adviseren over bijvoorbeeld de opzet van het onderzoek en populatie door onafhankelijke wetenschappelijke deskundigen. Op deze wijze wordt geborgd dat een zo objectief mogelijke en onafhankelijke maatstaf zal worden gekozen. De precieze uitwerking van de opzet van het onderzoek wordt te zijner tijd nog verder uitgewerkt. Vijf jaar na inwerkingtreding van deze wet wordt de evaluatie naar de Staten-Generaal gestuurd.

Artikelen II, V en VII

Ook de bepalingen over het gebruik van het persoonsgebonden nummer BES worden aangepast. Deze bepalingen (artikelen 147 van de WPO BES, 179 van de WVO BES en 2.3.4 van de WEB BES) komen overeen met de bepalingen over het gebruik van het PGN in de WPO, WVO en WEB (artikel 2.5.5a van de WEB). In beginsel kunnen dus ook alle scholen en instellingen in Caribisch Nederland die over het PGN BES beschikken

[14] De diagnostische toetsen Nederlandse taal en rekenen (artikelen 28b WVO en 7.2.11 WEB) zijn nog niet tot stand gekomen, omdat daarvoor een AMvB noodzakelijk is.

eenmalig een pseudoniem laten genereren met het oog op het bieden van voorzieningen in het kader van het geven van onderwijs en de begeleiding van leerlingen. Dit pseudoniem kan vervolgens worden gebruikt voor het genereren van een ander pseudoniem (ketenID) in het kader van gegevensuitwisseling met leveranciers in het kader van de toegang tot en het gebruik van de digitale leermiddelen of in het kader van het digitaal afnemen van toetsen en examens, waaronder de wettelijk verplichte toetsen en examens, zoals het eindexamen, bedoeld in artikel 72 van de WVO BES of de examens, bedoeld in de artikelen 7.4.2 en 7.4.13 van de WEB BES. Voor beide soorten pseudoniemen is in het wetsvoorstel geregeld om welke categorieën van ontvangers het gaat. Deze zijn hierboven bij de artikelsgewijze toelichting op de artikelen I, III, IV, VI en VIII nader toegelicht. Tevens kan dit pseudoniem worden gebruikt voor het genereren van een ander pseudoniem in het kader van een ander geval bepaald bij algemene maatregel van bestuur. Inwerkingtreding van deze bepalingen is niet op korte termijn voorzien. Dit heeft er onder meer mee te maken dat nog niet alle scholen en instellingen op de BES over een persoonsgebonden nummer BES beschikken.[15] De wijzigingen in dit voorstel zullen pas van kracht worden op het tijdstip waar de genoemde bepalingen in de BES-wetten in werking zullen treden (zie ook in paragraaf 7).

In de artikelen 167e van de WPO BES, 218c van de WVO BES en 11.6f van de WEB BES is een evaluatiebepaling opgenomen. Voor een toelichting op deze bepalingen wordt verwezen naar de artikelsgewijze toelichting bij de artikelen I, III, IV, VI en VIII.

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

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

[15] Zie de memorie van toelichting bij de Tweede aanpassingswet openbare lichamen Bonaire Sint Eustatius en Saba-B, Kamerstukken II 2009/10, nr. 3.