WIJ WILLEM-ALEXANDER,
BIJ DE GRATIE GODS,
KONING DER NEDERLANDEN,
PRINS VAN ORANJE-NASSAU,
ENZ. ENZ. ENZ.

Voorstel van wet tot wijziging van de Wet op het primair onderwijs, de Wet primair onderwijs BES, de Wet op de expertisecentra, de Wet op het voortgezet onderwijs, de Wet voortgezet onderwijs BES, de Wet educatie en beroepsonderwijs en de Wet educatie en beroepsonderwijs BES in verband met het pseudonimiseren van leerling- of deelnemergegevens ten behoeve van de toegang tot en het gebruik van digitale leermiddelen

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het gelet op het belang van een zorgvuldige omgang met persoonsgegevens van leerlingen en deelnemers wenselijk is om in het kader van de toegang tot en het gebruik van digitale leermiddelen een pseudoniem van een leerling of deelnemer te kunnen gebruiken dat is gebaseerd op het persoonsgebonden nummer, en dat het in verband hiermee noodzakelijk is de Wet op het primair onderwijs, de Wet primair onderwijs BES, de Wet op de expertisecentra, de Wet op het voortgezet onderwijs, de Wet voortgezet onderwijs BES, de Wet educatie en beroepsonderwijs en de Wet educatie en beroepsonderwijs BES te wijzigen.;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Artikel I. Wijziging Wet op het primair onderwijs

Aan artikel 178a van de Wet op het primair onderwijs worden na het tiende lid twee leden toegevoegd, luidende:

11. Het bevoegd gezag kan het persoonsgebonden nummer van een leerling gebruiken ten behoeve van het genereren van een pseudoniem voor een leerling. Dit pseudoniem wordt gebruikt in het kader van de toegang tot en het gebruik van digitale leermiddelen.
12. Bij ministeriële regeling kunnen andere doeleinden worden aangewezen waarvoor een pseudoniem kan worden gebruikt. Daarbij kunnen tevens nadere regels worden gesteld over de voorwaarden waaronder dit pseudoniem kan worden gebruikt.

Artikel II. Wijziging Wet primair onderwijs BES

Aan artikel 147 van de Wet primair onderwijs BES worden na het zevende lid twee leden toegevoegd, luidende:

8. Het bevoegd gezag kan het persoonsgebonden nummer BES van een leerling gebruiken ten behoeve van het genereren van een pseudoniem voor een leerling. Dit

pseudoniem wordt gebruikt in het kader van de toegang tot en het gebruik van digitale leermiddelen.
9. Bij ministeriële regeling kunnen andere doeleinden worden aangewezen waarvoor een pseudoniem kan worden gebruikt. Daarbij kunnen tevens nadere regels worden gesteld over de voorwaarden waaronder dit pseudoniem kan worden gebruikt.

Artikel III. Wijziging Wet op de expertisecentra

Aan artikel 164a van de Wet op de expertisecentra worden na het elfde lid twee leden toegevoegd, luidende:

12. Het bevoegd gezag kan het persoonsgebonden nummer van een leerling gebruiken ten behoeve van het genereren van een pseudoniem voor een leerling. Dit pseudoniem wordt gebruikt in het kader van de toegang tot en het gebruik van digitale leermiddelen.
13. Bij ministeriële regeling kunnen andere doeleinden worden aangewezen waarvoor een pseudoniem kan worden gebruikt. Daarbij kunnen tevens nadere regels worden gesteld over de voorwaarden waaronder dit pseudoniem kan worden gebruikt.

Artikel IV. Wijziging Wet op het voortgezet onderwijs

In artikel 103b van de Wet op het voortgezet onderwijs worden onder vernummering van het twaalfde lid tot het veertiende lid twee leden ingevoegd, luidende:

12. Het bevoegd gezag kan het persoonsgebonden nummer van een leerling gebruiken ten behoeve van het genereren van een pseudoniem voor een leerling. Dit pseudoniem wordt gebruikt in het kader van de toegang tot en het gebruik van digitale leermiddelen.
13. Bij ministeriële regeling kunnen andere doeleinden worden aangewezen waarvoor een pseudoniem kan worden gebruikt. Daarbij kunnen tevens nadere regels worden gesteld over de voorwaarden waaronder dit pseudoniem kan worden gebruikt.

Artikel V. Wijziging Wet voortgezet onderwijs BES

Aan artikel 179 van de Wet voortgezet onderwijs BES worden na het achtste lid twee leden toegevoegd, luidende:

9. Het bevoegd gezag kan het persoonsgebonden nummer BES van een leerling gebruiken ten behoeve van het genereren van een pseudoniem voor een leerling. Dit pseudoniem wordt gebruikt in het kader van de toegang tot en het gebruik van digitale leermiddelen.
10. Bij ministeriële regeling kunnen andere doeleinden worden aangewezen waarvoor een pseudoniem kan worden gebruikt. Daarbij kunnen tevens nadere regels worden gesteld over de voorwaarden waaronder dit pseudoniem kan worden gebruikt.

Artikel VI. Wijziging Wet educatie en beroepsonderwijs

De Wet educatie en beroepsonderwijs wordt als volgt gewijzigd:

A

In artikel 2.3.6a worden onder vernummering van het negende lid tot het elfde lid twee leden ingevoegd, luidende:

9. Het bevoegd gezag kan het persoonsgebonden nummer van een deelnemer gebruiken ten behoeve van het genereren van een pseudoniem voor een deelnemer. Dit pseudoniem wordt gebruikt in het kader van de toegang tot en het gebruik van digitale leermiddelen.

10. Bij ministeriële regeling kunnen andere doeleinden worden aangewezen waarvoor een pseudoniem kan worden gebruikt. Daarbij kunnen tevens nadere regels worden gesteld over de voorwaarden waaronder dit pseudoniem kan worden gebruikt.

B

In artikel 2.5.5a worden onder vernummering van het twaalfde lid tot het veertiende lid twee leden ingevoegd, luidende:

12. Het bevoegd gezag kan het persoonsgebonden nummer van een deelnemer gebruiken ten behoeve van het genereren van een pseudoniem voor een deelnemer. Dit pseudoniem wordt gebruikt in het kader van de toegang tot en het gebruik van digitale leermiddelen.
13. Bij ministeriële regeling kunnen andere doeleinden worden aangewezen waarvoor een pseudoniem kan worden gebruikt. Daarbij kunnen tevens nadere regels worden gesteld over de voorwaarden waaronder dit pseudoniem kan worden gebruikt.

Artikel VII. Wijziging Wet educatie en beroepsonderwijs BES

Aan artikel 2.3.4 van de Wet educatie en beroepsonderwijs BES worden na het achtste lid twee leden toegevoegd, luidende:

9. Het bevoegd gezag kan het persoonsgebonden nummer BES van een deelnemer gebruiken ten behoeve van het genereren van een pseudoniem voor een deelnemer. Dit pseudoniem wordt gebruikt in het kader van de toegang tot en het gebruik van digitale leermiddelen.
10. Bij ministeriële regeling kunnen andere doeleinden worden aangewezen waarvoor een pseudoniem kan worden gebruikt. Daarbij kunnen tevens nadere regels worden gesteld over de voorwaarden waaronder dit pseudoniem kan worden gebruikt.

Artikel VIII. Inwerkingtreding

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen verschillend kan worden vastgesteld.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister van Onderwijs, Cultuur en Wetenschap,

dr. Jet Bussemaker

Memorie van toelichting

A. Algemeen

Dit wetsvoorstel stelt onderwijsinstellingen in staat om leerlinggegevens (of deelnemergegevens) te pseudonimiseren ten behoeve van het gebruik en de ontwikkeling van digitale leermiddelen. Het wetsvoorstel bevat voorstellen tot wijziging van de Wet op het primair onderwijs (WPO), de Wet primair onderwijs BES, de Wet op de expertisecentra (WEC), de Wet op het voortgezet onderwijs (WVO), de Wet voortgezet onderwijs BES, de Wet educatie en beroepsonderwijs (WEB) en de Wet educatie en beroepsonderwijs BES. Nadere uitwerking voor wat betreft de condities waaronder het pseudoniem gebruikt mag worden zal plaatsvinden in lagere regelgeving.

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

Inhoudsopgave

A. Algemeen 4
1. Inleiding 5
1.1. Kern van het wetsvoorstel 5
1.2. Leeswijzer 5
1.3. Probleemanalyse 5
1.4. Aanleiding en achtergrond 6
1.5. Convenant privacy en digitale onderwijsmiddelen: onderwijsinstellingen voeren de regie 7
1.6. Pseudoniem maakt dataminimalisatie mogelijk 8
1.7. Nut en noodzaak wetsvoorstel 8
2. Doel van het wetsvoorstel 9
2.1. Doel 9
2.2. Bescherming van persoonsgegevens 10
2.3. Reikwijdte van het pseudoniem 12
2.4. Hoe komt het pseudoniem tot stand? 13
2.5. Aanvullende maatregelen 14
3. Samenwerking Inspectie van het Onderwijs met de AP 14
4. Reactie onderwijsorganisaties en uitkomst internetconsultatie 14
5. Reactie Autoriteit Persoonsgegevens 14
6. Uitkomsten Privacy Impact Assessment (PIA) 15
6.1. Toets op de doelen, noodzakelijkheid en passend gebruik 15
6.2. Risicoanalyse 15
7. Positie Caribisch Nederland 16
8. Uitvoering en handhaving 16
9. Administratieve lasten 17
10. Financiële gevolgen 17
B. Artikelsgewijs 17

1. Inleiding

1.1. Kern van het wetsvoorstel

Met het wetsvoorstel wordt het voor onderwijsinstellingen mogelijk om voor de uitwisseling van leerlinggegevens of deelnemersgegevens met derde partijen een pseudoniem te gebruiken, waarbij het pseudoniem gebaseerd is op het persoonsgebonden nummer. Dit ten behoeve van de toegang tot en het gebruik van digitale leermiddelen.

1.2. Leeswijzer

In deze memorie van toelichting worden de wijzigingen en voordelen van de nieuwe situatie 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 Persoonsgegevens (5), de uitkomsten van het uitgevoerde privacy impact assessment (6), de positie van Caribisch Nederland (7), de uitkomst van de uitvoerings- en handhaafbaarheidstoets (8), administratieve lasten (9) en financiële gevolgen (10).

Daar waar in deze toelichting wordt gesproken over leerlingen (of leerlinggegevens), worden ook deelnemers in het middelbaarberoepsonderwijs (of de gegevens van die deelnemers) 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. Zo gebruiken steeds meer leraren apps die hen helpen om kinderen taal of rekenen te leren. Onderwijsinstellingen in het primair onderwijs (po), (voortgezet) speciaal onderwijs ((v)so), voortgezet onderwijs (vo) en middelbaar beroepsonderwijs (mbo) maken in toenemende mate gebruik van dergelijke digitale leermiddelen. Of het nu gaat om onderwijsinstellingen die alle leerlingen met behulp van een laptop of tablet onderwijs geven, of onderwijsinstellingen die voor sommige klassen of enkele vakken digitale hulpmiddelen gebruiken, het gebruik van digitale leermiddelen neemt in het Nederlandse onderwijs gestaag toe. Onder digitale leermiddelen wordt hier verstaan: digitale producten of digitale diensten, bestaande uit leerstof en/of toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens onderwijsinstellingen.

Digitale leermiddelen brengen nieuwe mogelijkheden met zich mee, die veel kunnen betekenen voor de kwaliteit van het onderwijs. Zo kunnen digitale leermiddelen helpen om oefenstof in het tempo en op het niveau van de leerling aan te bieden. Dat maakt het voor leraren mogelijk om meer te differentiëren tussen leerlingen. Directe feedback en automatisch nakijken zijn voordelen waarmee leraren tijd besparen, die weer benut kan worden voor interactie met de leerlingen. Ook worden digitale leermiddelen veel gebruikt bij het aanleren van 21e-eeuwse vaardigheden zoals digitale geletterdheid, mediawijsheid en *computational thinking*.

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

Om te bereiken dat leerlingen probleemloos gebruik kunnen maken van digitale leermiddelen is het nodig dat zij door alle betrokken partijen, 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), uniek geïdentificeerd kunnen worden (hierna gezamenlijk: leveranciers). Hiervoor hebben de onderwijsinstelling en de desbetreffende leverancier een unieke identiteit nodig, zoals een nummer. Doordat onderwijsinstellingen nu niet kunnen beschikken over zo'n 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 bij onderwijsinstellingen en leveranciers. Dit heeft tot gevolg dat leveranciers hun eigen maatregelen nemen, waarbij vaak gebruik wordt gemaakt van persoonsgegevens, om ervoor te zorgen dat er een correcte koppeling gelegd kan worden tussen aangeschafte leermiddelen en de leerlingen voor wie deze leermiddelen bestemd zijn. Door deze 'matchingsproblematiek' worden er onnodig veel persoonsgegevens uitgewisseld.

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 leerlingen 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 (Wbp), dienen er minder persoonsgegevens uitgewisseld te worden;
2. Met het toenemend gebruik van digitale leermiddelen en de wens van onderwijsinstellingen en leraren om hun onderwijs beter te laten aansluiten op het tempo en niveau van de afzonderlijke leerling, neemt het belang van een goed functionerende leermiddelenketen toe. Om van de meerwaarde van digitale leermiddelen gebruik te kunnen maken, moeten leerlingen gedurende een bepaalde periode door de leermiddelen herkend kunnen worden. Alleen dan kunnen de vorderingen van een leerling worden gevolgd. De toegang tot en het gebruik van digitale leermiddelen moeten soepel verlopen, zonder onnodige administratieve lasten voor onderwijsinstellingen en zodanig dat de leerresultaten snel en gemakkelijk toegankelijk zijn voor de leerling en leraar.

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 betreft de introductie van een pseudoniem voor leerlingen om de toegang tot en het gebruik van digitale leermiddelen te optimaliseren.[1] Een pseudoniem is een unieke identiteit voor leerlingen die door elke leverancier kan worden gebruikt, zonder dat direct te herleiden is om welke specifieke leerling 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 leerlingen 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.[2] De motie Rog[3] vraagt de regering te realiseren dat persoonsgegevens van leerlingen alleen nog maar gepseudonimiseerd worden verstrekt aan leveranciers en ontwikkelaars van digitaal leermateriaal. De motie Jasper van Dijk[4] verzoekt de regering ervoor te zorgen dat de persoonlijke gegevens van leerlingen in handen van commerciële bedrijven worden vernietigd (overwegende dat er gewerkt wordt aan pseudonimisering).

1.5. Convenant privacy en digitale onderwijsmiddelen: onderwijsinstellingen voeren de regie

In april 2015 hebben de PO-Raad, de VO-raad, de Groep Educatieve Uitgeverijen (GEU), de Vereniging Digitale Onderwijs Dienstverleners (VDOD) en de leden van de sectie Educatief van de Koninklijke Boekverkopersbond het convenant 'Digitale Onderwijsmiddelen en Privacy – Leermiddelen en Toetsen' gesloten.[5] De individuele partijen die dit convenant hebben ondertekend, dekken op dit moment gezamenlijk zo'n 95 procent van de markt van leermiddelen en leerlinginformatiesystemen.

Het convenant regelt onder meer dat de onderwijsinstellingen, en niet de uitgevers of distribiteurs van digitale leermiddelen, de regie hebben over wat er gebeurt met de gegevens van leerlingen 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 leerlingen informeren over het gebruik van persoonsgegevens en hoe ouders en leerlingen gebruik kunnen maken van hun rechten, zoals inzage en correctie. Het convenant concretiseert hiermee de naleving van de verplichtingen van onderwijsinstellingen en hun leveranciers die uit de Wbp voortvloeien.

Het convenant gaat vergezeld van een modelbewerkersovereenkomst en een privacybijsluiter die door onderwijsinstellingen en leveranciers kunnen worden gebruikt 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 aangegeven. 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.

---

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

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

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

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

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

De modelovereenkomst ondersteunt onderwijsinstellingen bij het sluiten van contracten. Door het grote aantal leveranciers dat 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 haar hierbij, maar een onderwijsinstelling kan ook zelf, zonder modelovereenkomst, mits binnen de kaders van wet, goede afspraken maken met leveranciers. De AP houdt hier toezicht op.

1.6. Pseudoniem maakt dataminimalisatie mogelijk

Op dit moment wisselen onderwijsinstellingen en leveranciers nog een set aan persoonsgegevens uit om zich ervan te vergewissen dat ze het over dezelfde leerling hebben. In plaats van deze set aan persoonsgegevens is het ook mogelijk om hiervoor een nummer te gebruiken dat voor iedere leerling 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 voor dit doel 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 van koppelbaarheid van gegevens vergroten.

Om die reden wordt het PGN omgezet naar een pseudoniem, zodat dit pseudoniem kan worden ingezet voor de toegang tot en het gebruik van digitale leermiddelen en de risico's op koppelbaarheid geminimaliseerd worden. Het pseudoniem leidt ertoe dat onderwijsinstellingen en leveranciers van digitaal leermateriaal weten dat ze het over dezelfde leerling hebben. De onderwijsinstelling weet welke leerling dit is; het pseudoniem is voor anderen niet te herleiden naar een individuele leerling.

Door het pseudoniem te baseren op het PGN is één pseudoniem voor dezelfde leerling te creëren voor de toegang en het gebruik van digitale leermiddelen. Dit biedt mogelijkheden voor ondersteuning van doorlopende leerlijnen, sectorovergangen en (voornamelijk in het mbo) het meenemen van zelf aangeschafte leermiddelen voor gebruik binnen andere instellingen. Het pseudoniem maakt dataminimalisatie mogelijk. Onderwijsinstellingen behoeven alleen die gegevens uit te wisselen die nodig zijn voor een gebruiksvriendelijke inzet van digitale leermiddelen. Te denken valt aan een voornaam, zodat leerlingen 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 het contract dat de onderwijsinstelling sluit met de leverancier. Het eerder hierboven beschreven privacyconvenant en de bijbehorende modelbewerkersovereenkomst ondersteunen onderwijsinstellingen hierbij.

1.7. Nut en noodzaak wetsvoorstel

Nut en noodzaak van het gebruik van het PGN voor dit doel 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;
- er is in ieder geval ergens in de keten een koppeling tussen het pseudoniem en het PGN nodig om de leerresultaten van het pseudoniem te kunnen vertalen naar echte leerlingen. Regulering hiervan maakt het mogelijk om transparant te zijn naar alle betrokken partijen (zoals leveranciers, ouders) en duidelijk te maken wat wel en niet is toegestaan;
- door het PGN als basis te gebruiken voor het pseudoniem is, los van de onderwijsinstelling en aanbieder, hetzelfde pseudoniem voor dezelfde leerling te

genereren. Dit maakt het mogelijk dat leerlingen over een bepaalde periode door de leermiddelen worden herkend.

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

Aangezien onderwijsinstellingen zorgdragen voor het geven van goed onderwijs en bepalen welke leermiddelen worden gebruikt, 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 aanbieders van digitale leermiddelen die zij zelf kunnen kiezen. Deze eigen verantwoordelijkheid van de onderwijsinstelling is een belangrijke reden om het gebruik van een pseudoniem niet verplicht voor te schrijven. Bovendien zal het gebruik van het pseudoniem voor onderwijsinstellingen in de praktijk de standaard zijn, aangezien de leveranciers afspraken hebben gemaakt met onderwijsinstellingen over het gebruik van het pseudoniem en daar hun systemen op hebben aangepast. Dit wetsvoorstel verplicht dan ook niet tot het gebruik van een pseudoniem, maar stelt onderwijsinstellingen in staat een pseudoniem te hanteren als zij digitale leermiddelen gebruiken en om in het kader van het genereren van dat pseudoniem het persoonsgebonden nummer te gebruiken. Op die manier 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 breed mogelijk gebruik van het pseudoniem bereikt. Een onderwijsinstelling kan gegronde redenen hebben om geen gebruik te maken van het pseudoniem. Bijvoorbeeld omdat de onderwijsinstelling zelf al andere maatregelen heeft getroffen om persoonsgegevens te beschermen. Met het oog 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.

Om het pseudoniem te kunnen baseren op het PGN, is het noodzakelijk deze doelbepaling voor het gebruik van het PGN wettelijk te verankeren. In artikel 24, eerste lid, van de Wbp is het volgende geregeld: een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. Dat betekent dat een wettelijk voorgeschreven persoonsnummer kan worden verwerkt ter uitvoering van de wet waarin het voorschrift over het nummer is opgenomen. De praktijk leert evenwel dat dergelijke nummers ook voor andere doeleinden worden verwerkt. Onder omstandigheden is dit gerechtvaardigd, in andere gevallen echter niet. Algemene randvoorwaarde is dat persoonsgegevens niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (artikel 9 van de Wbp). Uiteraard geldt dit ook voor persoonsnummers. Omdat het gebruik van persoonsnummers 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. Hieraan wordt met dit wetsvoorstel voldaan.

2. Doel van het wetsvoorstel

2.1. Doel

Het doel van het wetsvoorstel is het voorzien in de mogelijkheid voor onderwijsinstellingen om een pseudoniem voor leerlingen te creëren, gebaseerd op het

PGN, dat kan worden gebruikt in de uitwisseling tussen de onderwijsinstelling en de leveranciers, zodat de leerlingen toegang hebben tot de juiste digitale leermiddelen en deze ook kunnen gebruiken. Onder toegang wordt hier 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, voor zover in dat proces persoonsgegevens van leerlingen gebruikt worden;
- het kunnen inloggen op de digitale leeromgeving 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 leerlingen, waaronder:

- de opslag van leer- en toetsresultaten door leveranciers;
- het kunnen uitwisselen van leer- en toetsresultaten tussen leveranciers van digitale leermiddelen en het schoolinformatiesysteem; en
- 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 leerling.

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

Een pseudoniem dat door alle leveranciers gebruikt wordt, heeft als voordelen:

- een kwalitatief hoogwaardig proces van uitgifte van digitale identiteiten te kunnen garanderen;
- het reduceren c.q. voorkomen van matchingsproblemen bij het gebruik van verschillende identiteiten;
- het reduceren c.q. voorkomen van verlies van onderwijstijd door problemen met identiteiten;
- betere bescherming van persoonsgegevens door gebruik van een minimale set persoonskenmerken in de keten;
- het bieden van continuïteit voor de leerling bij een overstap naar een andere onderwijsinstelling;
- het faciliteren van een doorlopende leerlijn bij de overstap tussen sectoren.

Het pseudoniem is de unieke digitale identiteit die nodig is om te komen tot een duurzaam afsprakenstelsel voor identificatie, authenticatie en autorisatie. Het is essentieel dit goed te regelen om de toegang tot en het gebruik van leermiddelen soepel te laten verlopen. De onderwijssector participeert in de ontwikkeling van Idensys[6], het rijksbrede initiatief om tot een standaard voor de toegang tot online dienstverlening te komen. Op die manier wordt geborgd dat de stappen die in de onderwijssector gezet worden, aansluiten bij rijksbrede ontwikkelingen op dit gebied.

2.2. Bescherming van persoonsgegevens

Onderwijsinstellingen maken steeds meer gebruik van digitale leermiddelen in het onderwijs. Gebleken is dat daarbij onnodig persoonsgegevens worden uitgewisseld tussen onderwijsinstellingen en leveranciers: gegevens die niet strikt noodzakelijk zijn voor het geven van goed onderwijs. Ouders moeten er vanuit kunnen gaan dat de onderwijsinstelling zorgvuldig omgaat met de gegevens van hun kinderen. Leerlingen

[6] www.idensys.nl, Idensys maakt het mogelijk dat burgers, consumenten en ondernemers op termijn beter online zaken kunnen doen met overheid en bedrijfsleven en wordt onder regie van de ministers van BZK en EZ ontwikkeld.

verdienen als kwetsbare groep in de samenleving extra privacybescherming. Dit vloeit ook voort uit de Wbp. Volgens 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 voor leerlingen wordt beoogd aan de onwenselijke situatie van onnodige gegevensuitwisseling definitief een einde te maken. Naar verwachting levert het gebruik van pseudoniemen een wezenlijke bijdrage aan de bescherming van de persoonsgegevens van de leerling.

Er is ook zorgvuldig gekeken naar alternatieven. In de eerste plaats is de mogelijkheid van anonimisering onderzocht. Bij anonimisering is de leerling 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 leerlingen over een bepaalde periode kunnen herkennen. Anonimisering is daarom geen geschikt alternatief.

In de tweede plaats is onderzocht om in plaats van het PGN een vaste set persoonsgegevens (bijvoorbeeld volledige naam, geboortedatum, geboorteplaats) die al bekend zijn bij de onderwijsinstelling, te gebruiken 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 leerling op twee onderwijsinstellingen verschillend wordt geschreven), waardoor handmatige correcties nodig zijn bij alle partijen in de keten. Bovendien wordt het pseudoniem straks, beveiligd, samen met het PGN, in het schoolinformatiesysteem opgeslagen, zodat deze gegevens praktisch gezien gekoppeld zullen zijn. Deze koppeling heeft tot doel voor de onderwijsinstelling en de leraren duidelijk te maken welke leerling achter welk pseudoniem schuilgaat. Omdat die koppeling er toch zal zijn, is het vanuit het oogpunt van bescherming van persoonsgegevens minder bezwaarlijk dat het pseudoniem op het PGN wordt gebaseerd.

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 en de artikelen 2.3.6a en 2.5.5a WEB precies aangegeven voor welke situaties en door wie het gebruik van het nummer is toegestaan en ten behoeve van welke doeleinden. De Wet primair onderwijs BES (WPO BES), Wet voortgezet onderwijs BES (WVO BES) en de Wet educatie en beroepsonderwijs BES (WEB BES) kennen vergelijkbare bepalingen voor het gebruik van het persoonsgebonden nummer BES. Het wetsvoorstel voorziet in de mogelijkheid voor het bevoegd gezag het PGN (of het PGN BES) van leerlingen te gebruiken voor het creëren van een pseudoniem, dat in het kader van de toegang tot en het gebruik van digitale leermiddelen kan worden gebruikt.

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 (voorganger 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).[7]

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 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.

Sommige digitale leermiddelen vragen voor een goede werking en vanuit het onderwijsbelang om het gebruik van een aantal persoonskenmerken, bijvoorbeeld de naam of initialen, de groep of het niveau van de leerling. Dit is ook nodig opdat leraren direct kunnen zien welke leerling (en niet welk pseudoniem) welke resultaten behaalt. Gebruik van het pseudoniem 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 aanbieder van digitale leermiddelen stopt met het aanbieden daarvan, bijvoorbeeld omdat de contractrelatie met de onderwijsinstelling eindigt, dient hij binnen het daarvoor geldende regime van de Wbp zorg te dragen voor verwijdering van alle persoonsgegevens, inclusief de pseudoniemen van de betreffende leerlingen.

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

2.3. Reikwijdte van het pseudoniem

Het is niet de bedoeling dat een pseudoniem de functie van het PGN in het onderwijs overneemt. Het gebruik van een pseudoniem is op dit moment enkel 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. Dit pseudoniem heeft daardoor een beperkte reikwijdte. De betrokken leveranciers mogen bovendien voor andere doelen onderling geen andere persoonsgegevens van leerlingen uitwisselen.

Tegelijkertijd staat de onderwijsinstelling in het hart van de netwerksamenleving en heeft deze met veel organisaties contact over haar leerlingen. Bijvoorbeeld met samenwerkingsverbanden passend onderwijs om te bepalen of een leerling in aanmerking komt voor extra ondersteuning. Hiervoor is het nodig dat

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

onderwijsinstellingen gegevens kunnen uitwisselen over leerlingen. Er is een groeiende behoefte om dit veilig en efficiënt via de digitale weg te kunnen doen.

Het is omwille van koppelbaarheid met andere gegevens niet wenselijk het PGN voor dergelijke doelen te gebruiken, omdat dit risico's voor de privacy van leerlingen met zich mee zou brengen. Het gebruik van een pseudoniem doet dat niet, mits voor elk doel een ander pseudoniem wordt gehanteerd. Door gebruik te maken van verschillende pseudoniemen voor verschillende doeleinden, wordt dataminimalisatie mogelijk in de processen waarin geen gebruik gemaakt mag worden van het PGN.

Digitale gegevensuitwisseling tussen onderwijsinstellingen en hun omgeving wordt steeds meer de norm. Ook gaan de ontwikkelingen op het gebied van privacy en beveiliging snel. Daarom voorziet het wetsvoorstel in de mogelijkheid om bij ministeriële regeling vast te leggen voor welke andere doeleinden en onder welke voorwaarden een pseudoniem (het gaat hier om een ander pseudoniem dan het pseudoniem dat in het kader van de uitwisseling van digitale leermiddelen wordt gegenereerd) gebruikt mag worden. Deze voorwaarden kunnen bijvoorbeeld betrekking hebben op de partijen die over het pseudoniem mogen beschikken, de bewaartermijn van het pseudoniem, eventueel andere persoonsgegevens die in combinatie met het pseudoniem gebruikt mogen worden, de manier waarop het pseudoniem tot stand komt, beveiligingseisen, etc. Hiermee voorziet het wetsvoorstel in de gewenste flexibiliteit en toekomstbestendigheid. Er kan zodoende adequaat worden ingespeeld op toekomstige ontwikkelingen.

2.4. Hoe komt het pseudoniem tot stand?

Om een pseudoniem te genereren is er een centraal georganiseerde nummervoorziening nodig. Dit is een voorziening voor het aanmaken, wijzigen en verwijderen van pseudoniemen. Het proces ziet er als volgt uit:

1. De onderwijsinstelling geeft het schoolinformatiesysteem opdracht om het PGN onomkeerbaar te versleutelen voordat dit door het schoolinformatiesysteem naar de nummervoorziening wordt verstuurd om een pseudoniem te genereren. Dit ter beveiliging, om te voorkomen dat het PGN als PGN naar de nummervoorziening verzonden wordt. In de nummervoorziening zelf worden geen andere persoonsgegevens verwerkt (dus ook niet opgeslagen) dan het versleutelde PGN en het naar de onderwijsinstelling terug te sturen pseudoniem.

2. Het pseudoniem wordt binnen de nummervoorziening gegenereerd op basis van een combinatie van a) het versleutelde PGN, b) een aanduiding van het doel waarvoor het pseudoniem gebruikt wordt (in dit geval de toegang tot en het gebruik van digitale leermiddelen) en c) de onderwijssector. Door deze meervoudige basis is het pseudoniem niet meer aan te merken als een "een-op-een" pseudoniem van (enkel) het PGN. Het pseudoniem kan, ook al is dit steeds gebaseerd op hetzelfde PGN van de leerling, daarmee variëren per onderwijssector en per doel waarvoor het pseudoniem gebruikt wordt.

3. Het pseudoniem wordt geretourneerd naar de onderwijsinstelling en opgeslagen in het schoolinformatiesysteem.

4. Op het moment dat leerlingen digitale leermiddelen gaan gebruiken, wordt het pseudoniem gebruikt in de uitwisseling tussen het schoolinformatiesysteem en de leverancier(s) van de betreffende leermiddelen om de toegang te regelen en het gebruik mogelijk te maken.

5. Het pseudoniem is door zijn verschijningsvorm alleen geschikt voor verwerking door computers en niet door mensen. Het pseudoniem is namelijk niet leesbaar op

een scherm of simpel over te schrijven. In die zin wijkt het pseudoniem wezenlijk af van het PGN of BSN zelf. Om het risico op inbreuk op persoonsgegevens van leerlingen als gevolg van datalekken te minimaliseren, wordt het pseudoniem versleuteld vastgelegd in de schoolinformatiesystemen.

Het voornemen is om de centraal te organiseren nummervoorziening onder te brengen in de ICT-basisinfrastructuur die Stichting Kennisnet beheert voor het po, vo, (v)so en mbo. Door middel van een derdenverklaring kan Kennisnet de kwaliteitsborging regelen voor onderwijsinstellingen en leveranciers.[8] Onderwijsinstellingen sluiten met Kennisnet een bewerkersovereenkomst waarin de gegevensuitwisseling tussen de onderwijsinstelling en de nummervoorziening is vastgelegd.

2.5. Aanvullende maatregelen

Naast de introductie van het pseudoniem wordt 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' en het gebruik van de modelbewerkersovereenkomst door partijen;
- de sectorraden ondersteunen onderwijsinstellingen en instellingen op het gebied van privacy en beveiliging. Door middel van concrete producten wordt gewerkt aan de bewustwording op deze onderwerpen bij onderwijsinstellingen en aan gedragsverbetering;
- bij de totstandkoming van sectorale inkoopvoorwaarden wordt een relatie gelegd met de modelbewerkersovereenkomst;
- er wordt gewerkt aan een aangescherpt attributenbeleid. Dat is het beleid waarin is vastgelegd welke gegevens op welk moment door welke partij worden gedeeld. Dit leidt ertoe dat er minder gegevens worden gedeeld tussen onderwijsinstellingen en leveranciers.

3. Samenwerking Inspectie van het Onderwijs met de AP

De Inspectie van het Onderwijs 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 alle informatie die relevant kan zijn voor ieders taak;
- 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 liggen.

4. Reactie onderwijsorganisaties en uitkomst internetconsultatie

PM

5. Reactie Autoriteit Persoonsgegevens

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

PM

6. Uitkomsten Privacy Impact Assessment (PIA)

Er is een PIA uitgevoerd op het gebruik van de nummervoorziening in de leermiddelenketen. Met de 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 de PIA de risico's op het gebied van privacy en gegevensverwerking in kaart en doet deze een voorstel voor passende beveiligingsmaatregelen. Op basis van de PIA kan gesteld worden dat het risico op koppelbaarheid van de gegevens van leerlingen door gebruik van het PGN als basis voor het pseudoniem verwaarloosbaar zijn. De voorgestelde passende beveiligingsmaatregelen zijn onverkort overgenomen in de realisatie en invoering van het pseudoniem.

Hieronder volgen de belangrijkste conclusies uit de 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 de PIA dat:

- om leerlingen 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 de PIA dat:

- een pseudoniem de voorkeur verdient als identificator binnen de leermiddelenketen boven datasets met NAW-gegevens en boven direct identificerende nummers, zoals het PGN;
- de identificator (het pseudoniem) 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 onderwijsinstellingen 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 pseudoniem van leerlingen te gebruiken.

6.2. Risicoanalyse

In de risicoanalyse die door middel van de 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 leerlingen 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 leerlingen 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 de PIA stelt een aantal aanvullende maatregelen voor. Deze maatregelen zijn:

- voorafgaande toestemming van de onderwijsinstelling bij 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 enerzijds het pseudoniem en anderzijds 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 (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.

7. Positie Caribisch Nederland

Het uitgangspunt bij de onderwijswetgeving in Caribisch Nederland is dat deze niet onnodig uiteenloopt met de wetgeving in Europees Nederland.[9] 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 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.[10] Dit betekent dat de desbetreffende wijzigingsvoorstellen pas van kracht worden op het tijdstip waarop de artikelen 147 WPO BES, 179 WVO BES en 2.3.4 WEB BES in werking treden. Het is nog niet bekend wanneer dat gaat gebeuren.

Dit wetsvoorstel zal daarom naar verwachting weinig 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 te laten genereren in kader van het gebruik van digitale leermiddelen. Voorwaarde is wel dat de leveranciers hun systemen daarop aangepast hebben. Nederlandse leveranciers bieden straks die dienstverlening, leveranciers uit andere landen (nog) niet.

8. Uitvoering en handhaving

Stichting Kennisnet is verantwoordelijk voor de realisatie van de nummervoorziening. Kennisnet is betrokken bij de totstandkoming van het wetsvoorstel en voorziet geen

[9] Kamerstukken I 2011/12 33000 VII, nr. C, p.2.
[10] Tweede Aanpassingswet openbare lichamen Bonaire, Sint Eustatius en Saba-B, Stb. 2011, 33.

problemen in de realisatie. Voordat het pseudoniem daadwerkelijk gebruikt kan worden, zullen de leveranciers hun systemen moeten aanpassen. De betrokken publieke partijen (PO-raad, VO-raad, MBO-raad, Kennisnet) en leveranciers werken samen aan een zorgvuldige invoering.

9. Administratieve lasten

De invoering van het pseudoniem zal voor onderwijsinstellingen een beperkte administratieve lastenvermindering opleveren. De gegevensuitwisseling tussen het schoolinformatiesysteem en de nummervoorziening en de uitwisseling met leveranciers zal volledig geautomatiseerd plaatsvinden. Dit vergt geen additionele handelingen van de onderwijsinstelling in vergelijking met de huidige praktijk. Door de invoering van het unieke nummer zal de foutgevoeligheid van het bestel- en toegangsproces afnemen. De fouten leiden nu tot noodzakelijke administratieve correcties door de onderwijsinstelling en ongewenste lesverstoringen op momenten dat leerlingen niet kunnen inloggen op 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 minimaal 3 uur per jaar met correcties bezig is. Dat aantal loopt snel op als er serieuze problemen zijn.

10. Financiële gevolgen

De invoering van het pseudoniem 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 en VI

Met de wijziging van de artikelen 178a van de WPO, 164a van de WEC, 103b van de WVO en de artikelen 2.3.6a en 2.5.5a van de WEB, wordt voor het bevoegd gezag een grondslag gecreëerd om het PGN van een leerling te gebruiken ten behoeve van het genereren van een pseudoniem voor een leerling. Dit pseudoniem kan worden gebruikt bij de gegevensuitwisseling met leveranciers in het kader van de toegang tot en het gebruik van de digitale leermiddelen. De WEB kent 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 het voortgezet algemeen volwassenenonderwijs. 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. Hieraan wordt met dit wetsvoorstel voldaan. In paragraaf 2.4 is ingegaan op de wijze waarop het pseudoniem tot stand komt. Het wetsvoorstel voorziet daarnaast in de mogelijkheid om bij ministeriële regeling te bepalen voor welke andere doeleinden en onder welke voorwaarden een ander pseudoniem dan het pseudoniem dat ten behoeve van de uitwisseling van digitale leermiddelen wordt gegenereerd, gebruikt mag worden. Deze voorwaarden kunnen bijvoorbeeld betrekking hebben op welke partijen over het pseudoniem mogen beschikken, de bewaartermijn van het pseudoniem, eventueel andere persoonsgegevens die in combinatie met het pseudoniem gebruikt mogen worden, de manier waarop het pseudoniem tot stand komt, beveiligingseisen, etc.

Artikelen II, V en VII

Ook de bepalingen over het gebruik van het persoonsgebonden nummer BES worden aangepast. Deze bepalingen (artikelen 147 WPO BES, 179 WVO BES en 2.3.4 WEB BES) komen overeen met de bepalingen over het gebruik van het PGN in de WPO, WVO en WEB (artikel 2.5.5a WEB). 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.[11] 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 onder 7).

De Minister van Onderwijs, Cultuur en Wetenschap,

dr. Jet Bussemaker

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