PBLQ
HEC

voor een sterke
publieke sector

DEFINITIEF

Privacy Impact Assessment Nummervoorziening in de Leermiddelenketen

Rapport

DEFINITIEF

Privacy Impact Assessment Nummervoorziening in de Leermiddelenketen

Eindrapportage

project 4798
versie 1.0
datum 27 mei 2015

DEFINITIEF

Inhoudsopgave

Samenvatting

Kennisnet is in opdracht van het Doorbraak-project onderwijs & ICT een ontwerptraject gestart voor een nummervoorziening. De Nummervoorziening is een dienst waarmee in de leermiddelenketen in het primair onderwijs (PO), het voorgezet onderwijs (VO) en het middelbaar beroepsonderwijs (MBO) leerlingen en docenten uniek geïdentificeerd kunnen worden met een pseudoniem. Voordat de Nummervoorziening gerealiseerd gaat worden wil de stuurgroep van het Doorbraak-project de zekerheid hebben dat de privacy en de gegevensbescherming met de Nummervoorziening goed geregeld zijn. Kennisnet heeft PBLQ in dat verband de opdracht verstrekt om een Privacy Impact Assessment (PIA) uit te voeren op het gebruik van de Nummervoorziening in de leermiddelenketen, ook wel de Educatieve Content Keten (ECK) genoemd.

De opdracht is als volgt geformuleerd:

- Voer een Privacy Impact Assessment uit op het gebruik van de Nummervoorziening in de leermiddelenketen.
- Breng de compliance van de Nummervoorziening toegepast in de leermiddelenketen in kaart op het gebied van privacy en gegevensverwerking.
- Breng de (extra) risico's op het gebied van privacy en gegevensverwerking van het gebruik van de Nummervoorziening in de leermiddelenketen in kaart. Geef een beoordeling van de risico's en specificeer wat de bijbehorende beveiligingsmaatregelen zijn op basis van toepasselijke normenstelsel(s).

Een PIA toetst, kort gezegd, óf de voorziene gegevensverwerking inderdaad doorgang dient te vinden, welke gegevensverwerkingen dan noodzakelijk zijn en vervolgens hoe deze gegevensverwerkingen plaats mogen vinden.

Huidige situatie

In de bestaande praktijk wordt een viertal specifieke privacy-issues onderkend:

1. de verspreiding van direct identificerende gegevens binnen c.q. over de leermiddelenketen;
2. de in de praktijk vrij zelfstandige positie van distributeurs en uitgevers en (mogelijke) gegevensverwerkingen door die partijen, die zich aan het zicht van de scholen onttrekken dan wel waar de scholen zich niet (volledig) bewust van zijn;
3. de mogelijkheid dat distributeurs en uitgevers de gegevens waarover zij in het kader van hun rol in de leermiddelenketen beschikken, gebruiken voor de eigen bedrijfsvoering en zouden (gaan) gebruiken voor commerciële benadering van leerlingen of ouders;
4. de strikte regulering van het gebruik van bij wet ter identificatie aan personen toegekende nummers zoals het burgerservicenummer (BSN) en het persoonsgebonden nummer in het onderwijs (PGN).

Toets op de compliance

Ten aanzien van doelen van gegevensverwerking en de noodzakelijkheid van gegevens concluderen wij dat:

- om leerlingen te identificeren zonder gebruik te maken van datasets met daarin direct identificerende gegevens (zoals naam en adres) een identificator noodzakelijk is;
- voor de gegevens benodigd voor het bestellen, leveren en gebruiken van verplichte leermiddelen en het indien nodig terugleveren van de resultaten aan de school, geldt dat:

- alleen de distributeur zou hoeven te beschikken over de NAW-gegevens en betaalgegevens van de besteller en over de NAW-gegevens van het afleveradres (en de uitgever dus niet);
- de distributeur bij een gecombineerde levering van digitale en folio leermiddelen dient te beschikken over zowel het ketenpseudoniem als de NAW gegevens van de besteller en de NAW gegevens van het afleveradres. In bepaalde gevallen zal, afhankelijk van de inrichting van de bestelomgeving, ook daarbij het ketenpseudoniem gebruikt worden;
- alleen de uitgever zou hoeven te beschikken over de resultaten van leerlingen (en de distributeur dus niet).

Ten aanzien van de noodzakelijkheid van een identificator en de noodzakelijkheid van een nummer als identificator concluderen wij dat:

- een ketenpseudoniem de voorkeur verdient als identificator binnen de leermiddelenketen boven datasets met NAW-gegevens en boven direct identificerende nummers zoals het PGN of bijvoorbeeld het personeelsnummer voor docenten;
- de identificator (het ketenpseudoniem) met name een administratie functie vervult en, bij het gebruik van bepaalde digitale leermiddelen, de bevoegdheid representeert om die leermiddelen te gebruiken. Binnen de leermiddelenketen heeft de identificator geen functie als nummer dat het resultaat is van een voorafgaande identiteitsvaststelling.

Voor de reikwijdte van het voorziene ketenpseudoniem komen we, strikt juridisch bezien, tot de bevindingen:

- Vanuit de scholen bezien is een sectorale identificator (het ketenpseudoniem) en de thans voorziene uitgifte per sector (PO, VO en MBO), als juridisch mogelijk aan te merken is, voor zover dit enkel en alleen het ketenpseudoniem zelf betreft. Een aandachtspunt daarbij is dat er - met een gelijkblijvend ketenpseudoniem bij een overstap binnen een sector - mogelijkheden ontstaan waarbij de oude of de nieuwe school kennisneemt van vastgelegde gegevens en resultaten die zijn of worden gegenereerd tijdens het verblijf op de andere school.
- Vanuit de leerling bezien achten wij het kunnen volgen van leerlijnen en het kunnen blijven gebruiken van persoonlijk aangeschafte autorisaties voor digitale leermiddelen de inhoudelijke criteria voor de bepaling van de reikwijdte van het ketenpseudoniem. Het is daarbij juridisch aanvaardbaar dat het pseudoniem behouden blijft bij verhuizing naar een andere school binnen dezelfde sector (PO, VO of MBO).
- Vanuit de leermiddelenproducenten (distributeurs en uitgevers) bezien is het voorstelbaar dat er meerdere of verschillende identificatoren zouden (kunnen) zijn voor een bepaalde leerling. Er is echter geen strikt juridische noodzaak om meerdere pseudoniemen te hanteren.

Belangrijke constateringen ten aanzien van het passend gebruik zijn:

- Het Privacy Convenant en de bijbehorende bewerkersovereenkomst zijn essentiële voorwaarden om de machtsverhouding tussen scholen en leermiddelenproducenten (distributeurs en uitgevers) in balans te krijgen. Wij achten het daarom de moeite waard om, op termijn en indien het door het Convenant beoogde resultaat onvoldoende bereikt wordt, in overweging te nemen om het Convenant en (in het bijzonder) de bewerkersovereenkomst van een nadere en aanvullende wettelijke basis te voorzien.
- Ook de beheerder van de Nummervoorziening en de beheerders van de inlogfaciliterende applicaties zijn aan te merken als Wbp-bewerkers voor de scholen.

- Het PGN/ BSN is het als eerst voor de hand liggende nummer om als basis voor het ketenpseudoniem van leerlingen te gebruiken. Daarbij kan niet met zekerheid gesteld worden dat het PGN (juridisch gezien) inderdaad als basis gebruikt *mag* worden. Tegelijkertijd kan eveneens niet gesteld worden dat het PGN *niet* als basis gebruikt zou *mogen* worden. Desalniettemin zijn er aanknopingspunten op basis waarvan gebruik van het PGN verdedigbaar is.

Risicoanalyse

In de risicoanalyse worden zes privacyrisico's geduid. Bij twee van deze risico's wordt het risico al (middels de Nummervoorziening, het ketenpseudoniemen en/ of het Privacy Convenant) adequaat aangepakt.
Van één risico (resultaten van leerlingen worden gebruikt als personeelsvolgsysteem van docent) wordt geconcludeerd dat het risico niet speelt bij de Nummervoorziening. Voor de overige drie risico's worden aanvullende maatregelen voorgesteld. Deze maatregelen zijn:

- voorafgaand akkoord van de school bij hergebruik van gegevens door distributeurs en uitgevers. Daarnaast zal er in de praktijk ook en vooral aandacht dienen te zijn voor de vraag of en welk hergebruik inderdaad rechtmatig en toelaatbaar is;
- 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 ketenpseudoniem aan elkaar worden gekoppeld waardoor een grotere gegevensset ontstaat (koppelingsrisico, ook bij eventuele datalekken);
- datascheiding bij gegevensbestanden die distributeurs gebruiken, tussen enerzijds het ketenpseudoniem en anderzijds NAW-gegevens betreffende de aflevering en betaling van leermiddelen. Deze scheiding kan doorgevoerd worden zodra de aflevering en de betaling van de leermiddelen hebben plaatsgevonden;
- encryptie van het ketenpseudoniem (en het PGN) in vooral de systemen van de scholen (LAS etc.).

Verder achten wij het voorstelbaar dat aanvullende regelgeving wordt gemaakt om duidelijk aan te geven dat het PGN als basis voor het ketenpseudoniem gebruikt mag worden.

Drietal centrale ontwerpvragen

Bij de opdracht is gevraagd expliciet in te gaan op een drietal centrale ontwerpvragen. De antwoorden op deze ontwerpvragen worden in dit rapport op verschillende plaatsen gegeven. In deze samenvatting worden de antwoorden bij deze vragen gegeven (- *cursief*) waarbij eventueel wordt verwezen naar de paragrafen in het rapport waar het aspect wordt behandeld.

1. Waarom gebruikt de Nummervoorziening het PGN / BSN bij de versleuteling daarvan tot een ketenpseudoniem?
   - *Wij constateren (net als in het ontwerp van de Nummervoorziening) dat het PGN/ BSN het als eerst voor de hand liggende nummer is om als basis voor het ketenpseudoniem van leerlingen te gebruiken (zie bovenstaande constatering bij passend gebruik en paragraaf 3.3.4).*
2. Waarom wordt het ketenpseudoniem decentraal opgeslagen in de leerling administratiesystemen (LAS) van de scholen?
   - *In alle gevallen zijn de scholen de Wbp-verantwoordelijken. Het maakt juridisch niet uit op welke plek het ketenpseudoniem wordt opgeslagen.*
   - *Door het toepassen van encryptie op het ketenpseudoniem (en het PGN) in vooral de systemen van de scholen (LAS etc.) (aanbevolen maatregel in paragraaf 4.2) wordt het risico op misbruik van het ketenpseudoniem na een datalek in een LAS verkleind.*

3. Wat is een juiste reikwijdte van het ketenpseudoniem? Dit uit zich bijvoorbeeld in de vraag waarom hetzelfde ketenpseudoniem voor alle distributeurs en uitgevers van leermiddelen gebruikt wordt. Bij deze reikwijdte spelen de volgende aspecten:
    - De scope / breedte van het gebruik van het ketenpseudoniem;
    - De levensduur van het ketenpseudoniem;
    - De herleidbaarheid van het ketenpseudoniem tot de desbetreffende leerling of docent.

- *Vanuit de scholen bezien is een sectorale identificator als juridisch mogelijk aan te merken, voor zover dit enkel en alleen het ketenpseudoniem zelf betreft. Wij bevelen daarbij aan om nader aandacht te besteden aan de mogelijkheden die - bij een overstap binnen een sector met een gelijkblijvend ketenpseudoniem - ontstaan dat de ene school kennisneemt van vastgelegde gegevens en resultaten die zijn of worden gegenereerd tijdens het verblijf op de andere school en de relatie daarvan met de reeds bestaande regeling over overdrachtsdossiers bij wijziging van school binnen een bepaalde sector. Daarbij kan ook aandacht besteed worden aan de overgang van Wbp-verantwoordelijkheid als een leerling naar een andere school gaat en gebruik blijft maken van dezelfde leermiddelen. Vanuit de leerling bezien achten wij een sectorale identificator juridisch aanvaardbaar. En vanuit de leermiddelenproducenten bezien is het voorstelbaar dat er meerdere of verschillende identificatoren zouden (kunnen) zijn voor een bepaalde leerling. Er is echter geen strikt juridische noodzaak om meerdere pseudoniemen te hanteren (zie bovenstaande bevindingen ten aanzien van de reikwijdte van het voorziene ketenpseudoniem en paragraaf 3.3.3).*
- *De levensduur van een ketenpseudoniem (de leerlijn in een sector) is direct gerelateerd aan de reikwijdte van de (sectorale) identificator.*
- *De reikwijdte van een ketenpseudoniem heeft in juridische zin geen invloed op de herleidbaarheid van het pseudoniem. Dit omdat het altijd zal gaan om persoonsgegevens. Wel wordt met het gebruik van het ketenpseudoniem de feitelijke herkenbaarheid voor distributeurs en uitgevers sterk gereduceerd ten opzichte van de huidige uitwisseling van datasets met direct identificerende gegevens.*

1. Inleiding

1.1 Aanleiding

Kennisnet is in opdracht van het Doorbraak-project onderwijs & ICT een ontwerptraject gestart voor een nummervoorziening. De Nummervoorziening is een dienst waarmee in de leermiddelenketen in het primair onderwijs (PO), het voorgezet onderwijs (VO) en het middelbaar beroepsonderwijs (MBO) leerlingen en docenten uniek geïdentificeerd kunnen worden met een pseudoniem. De Nummervoorziening moet voorzien in een aantal functionele ketenbehoeftes zoals een oplossing voor het matchingprobleem wat ziet op een juiste koppeling van bepaalde leermiddelen aan de personen (leerlingen) voor wie deze leermiddelen bestemd zijn en bij overstapissues die kunnen ontstaan als een school overstapt naar een ander ICT-platform of wanneer de leerling zelf verandert van school.

Voordat de Nummervoorziening gerealiseerd gaat worden wil de stuurgroep van het Doorbraak-project de zekerheid hebben dat de privacy en de gegevensbescherming met de Nummervoorziening goed geregeld zijn. Kennisnet heeft PBLQ in dat verband de opdracht verstrekt om een Privacy Impact Assessment (PIA) uit te voeren op het gebruik van de Nummervoorziening in de leermiddelenketen, ook wel de Educatieve Content Keten (ECK) genoemd.

Een PIA toetst, kort gezegd, óf de voorziene gegevensverwerking inderdaad doorgang dient te vinden, welke gegevensverwerkingen dan noodzakelijk zijn en vervolgens hoe deze gegevensverwerkingen plaats mogen vinden.

1.2 Opdrachtformulering

De opdracht is als volgt geformuleerd:

- Voer een Privacy Impact Assessment uit op het gebruik van de Nummervoorziening in de leermiddelenketen.
- Breng de compliance van de Nummervoorziening toegepast in de leermiddelenketen in kaart op het gebied van privacy en gegevensverwerking.
- Breng de (extra) risico's op het gebied van privacy en gegevensverwerking van het gebruik van de Nummervoorziening in de leermiddelenketen in kaart. Geef een beoordeling van de risico's en specificeer wat de bijbehorende beveiligingsmaatregelen zijn op basis van toepasselijke normenstelsel(s).

Deze PIA is uitgevoerd in opdracht van Kennisnet, door PBLQ in samenwerking met Net2Legal Consultants.

De PIA stelt Kennisnet, de programmagroep van het Doorbraak project, het ministerie van OCW en veldpartijen zoals programmaraden, distributeurs en uitgevers in staat te bezien of er vanuit privacy oogpunt aanpassingen van het ontwerp of aanvullende maatregelen nodig zijn om aan de toepasselijke privacywetgeving en eventuele privacybezwaren te voldoen. De partijen zijn daarmee de doelgroep waarop de PIA zich richt.

1.3 Werkwijze

De PIA is uitgevoerd door de documentatie te bestuderen die door Kennisnet is verstrekt en interviews te houden met medewerkers van Kennisnet die bij de Nummervoorziening zijn betrokken (de projectleider, de privacyjurist en de architect). Daarnaast is een interview gehouden met betrokkenen vanuit het ministerie van OCW.

1.4 Indeling rapport

In hoofdstuk 2 zijn het object van de PIA (de Nummervoorziening toegepast in de leermiddelenketen) en de bijbehorende context beschreven. In hoofdstuk 3 is de toets op de compliance uitgewerkt. De op de toets gebaseerde risicoanalyse is opgenomen in hoofdstuk 4. Daarbij worden ook de mogelijke maatregelen beschreven. Het rapport bevat een viertal achtergrondbijlagen:

- een algemene beschrijving van de Privacy Impact Assessment in bijlage A;
- een overzicht van de bepalingen die van toepassing zijn bij het gebruik van het Persoonsgebonden nummer (PGN) in bijlage B;
- een verhandeling over persoonsgegevens, datasets en soorten bestanden in bijlage C;
- een korte beschrijving van de Wet op de Ondernemingsraden in bijlage D.

De geïnterviewde personen en de bestudeerde documentatie zijn gespecificeerd in de bijlagen E en F.

2. Object van de PIA

Het object van deze PIA is de Nummervoorziening en het gebruik van pseudoniemen toegepast in de leermiddelenketen. Daarbij gaat het zowel om de compliance met regelgeving over het verwerken van persoonsgegevens als om de privacyrisico's. In deze PIA wordt specifieke aandacht besteed aan het gebruik van nummers en de rol en positie van partijen.

In de PIA wordt verder ingegaan op een drietal centrale ontwerpvragen[1]:

1. Waarom gebruikt de Nummervoorziening het PGN / BSN bij de versleuteling daarvan tot een ketenpseudoniem?
2. Waarom wordt het ketenpseudoniem decentraal opgeslagen in de leerling administratiesystemen (LAS) van de scholen?
3. Wat is een juiste reikwijdte van het ketenpseudoniem? Dit uit zich bijvoorbeeld in de vraag waarom hetzelfde ketenpseudoniem voor alle distributeurs en uitgevers van leermiddelen gebruikt wordt. Bij deze reikwijdte spelen de volgende aspecten:
   - De scope / breedte van het gebruik van het ketenpseudoniem;
   - De levensduur van het ketenpseudoniem;
   - De herleidbaarheid van het ketenpseudoniem tot de desbetreffende leerling of docent.

2.1 Privacy-issues in de leermiddelenketen in de huidige situatie

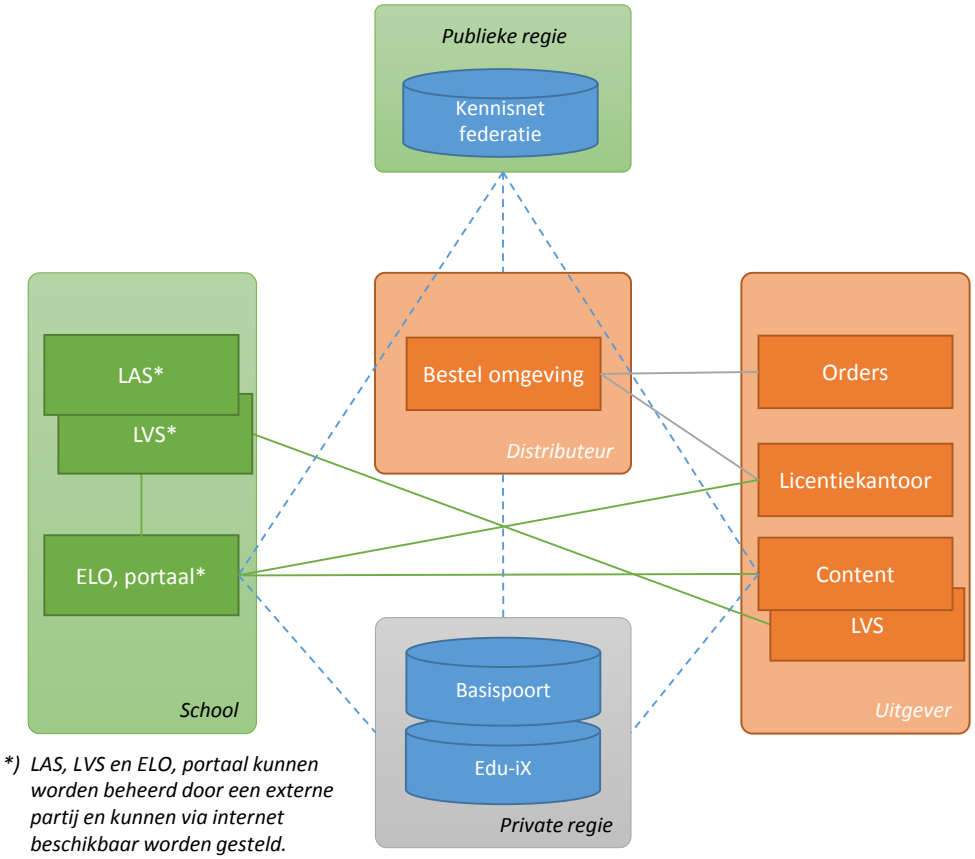
Leermiddelen zijn er in vele soorten en maten, van papieren boeken tot interactieve elektronische leeromgevingen. Afhankelijk van de antwoorden die een leerling geeft kan de leerstof soms verder gepresenteerd worden op basis van de gegeven antwoorden (gepersonaliseerde leermiddelen).
De volgende functies spelen bij leermiddelen en gepersonaliseerde leermiddelen in meer of mindere mate een rol:

A. een elektronische omgeving met inlogfaciliteit;
B. de identiteit van de leerling moet soms bekend zijn;
C. een leermiddel (leermiddelensysteem) moet de mogelijkheid bieden om prestatiegegevens op individueel niveau te verwerken.

In de huidige situatie worden bij het gebruik van ICT-voorzieningen binnen de leermiddelenketen voor deze functies persoonsgegevens van leerlingen en docenten verwerkt en verspreid binnen de leermiddelenketen.

---

[1] De antwoorden op deze ontwerpvragen worden in dit rapport op verschillende plaatsen gegeven. In de samenvatting van dit rapport wordt expliciet antwoord gegeven op deze vragen. Daarbij wordt eventueel verwezen naar de paragrafen in het rapport waar het aspect wordt behandeld.



Figuur 1: Schematische weergave huidige situatie

Scholen hebben - uiteraard en wettelijk voorgeschreven – de beschikking over personalia en andere identificerende gegevens van leerlingen en docenten. Voor het bestellen van leermateriaal en het gebruiken van leermiddelen worden identificerende gegevens vastgelegd voor het verwerken van orders, de distributie, het verkrijgen en gebruiken van licenties, het gebruik van leermiddelensystemen zelf (content), het vastleggen van resultaten van leerlingen in leermiddelensystemen en de opname van deze resultaten in leerlingvolgsystemen van de scholen.

Het is binnen die leermiddelenketen ook noodzakelijk dat bij het bestellen, het gebruik van licenties en systemen (content) en het vastleggen van resultaten al deze handelingen toegeschreven (kunnen) worden aan de juiste persoon. Soms dient daarbij de identiteit van die persoon bekend te zijn, soms ook niet. Voor het toeschrijven van handelingen aan de juiste persoon is een unieke identificator nodig. Een identificator is hierbij of één gegeven (een nummer of pseudoniem) of een set van gegevens (zoals NAW-gegevens). De functie van de identificator is om binnen de leermiddelenketen allerlei handelingen eenduidig te koppelen aan de juiste persoon.
Het toeschrijven van handelingen aan de juiste persoon wordt wel aangeduid als het matchingissue. De handelingen dienen immers gematched (gekoppeld) te worden aan de juiste persoon.

Door de noodzaak van de aangegeven matching is de vraag óf de gegevensverwerking (lees: het gebruik van een identificator) plaats dient te vinden in feite beantwoord. **Een identificator is inderdaad noodzakelijk.** Deze constatering zegt echter nog niets over welke identificator gebruikt wordt en hoe het gebruik daarvan ingeregeld wordt.

Bij het toeschrijven van handelingen aan de juiste persoon en bij het matchingissue wordt in de praktijk gebruik gemaakt van applicaties die toegang tot systemen en de juiste autorisaties daarbij regelen en ondersteunen. Er zijn dergelijke applicaties die zijn ontwikkeld en worden beheerd door de Kennisnet-federatie en er zijn meer privaat ontwikkelde en beheerde applicaties zoals Basispoort en Edu-iX. Deze applicaties zorgen ervoor dat bij gebruik van meerdere systemen van met name distributeurs en uitgevers niet iedere keer apart ingelogd hoeft te worden, maar dat inloggen automatisch (als het ware onder water) plaats kan vinden middels de Elektronische leeromgeving (ELO) en andere portalen die scholen gebruiken. In die zin worden deze inlogfaciliterende applicaties wel aangeduid als ‘single sign on’ (SSO).

In de huidige situatie wordt (nog) geen eenduidige en unieke identificator gebruikt en worden verschillende datasets als identificator gebruikt. Door deze verschillende datasets die als identificator dienen, ontstaan verschillende matchingproblemen. Bij de datasets als identificator en voor het oplossen van de matchingproblemen, worden daarbij veelal gegevens gebruikt die de leerling of docent direct identificeren. Daarbij valt te denken aan personalia, adresgegevens, gegevens over een specifieke klas van een bepaalde school, nummers zoals leerling- of personeelsnummers en inloggegevens.
Het gebruik van direct identificerende datasets als identificator heeft tot gevolg dat de diverse partijen binnen de leermiddelenketen over direct identificerende persoonsgegevens beschikken. Er is in die zin een brede verspreiding van direct identificerende gegevens. Daardoor is het (in beginsel) mogelijk dat bijvoorbeeld distributeurs gegevens over resultaten aan een bepaalde leerling zouden kunnen koppelen en dat bijvoorbeeld uitgevers de resultaten van bepaalde leerlingen zouden kunnen gebruiken om die leerlingen direct te benaderen om extra (niet verplichte) producten onder de aandacht te brengen.
Het zijn deze verspreiding van direct identificerende gegevens en het mogelijke gebruik daarvan door distributeurs en uitgevers die aanleiding geven tot privacybezwaren en situaties die als onnodig of zelfs als onwenselijk ervaren worden. Hierbij gaat het nog niet eens zozeer om de vraag of die gegevensverwerkingen juridisch gezien toegestaan zijn of zouden kunnen zijn, maar meer nog om de vraag of het allemaal wel strikt noodzakelijk en wenselijk is.

Daarnaast was er in de bestaande situatie, zeker tot enige tijd geleden, onduidelijkheid en discussie over de juridische posities van de diverse partijen en over de zeggenschap over de persoonsgegevens die door de diverse partijen werden verwerkt of waarover de diverse partijen feitelijk beschikken omdat die partijen systemen beheren waarin persoonsgegevens zijn vastgelegd. In juridische zin gaat het bij het verwerken van persoonsgegevens om de vraag welke partij de Wbp-verantwoordelijke is en of een bepaalde partij een bewerker voor de Wbp-verantwoordelijke is. Algemeen gezegd, werd daarbij aan de distributeurs en uitgevers, mede gelet op de handelwijze van de scholen, een vrij zelfstandige positie toegekend dan wel hadden distributeurs en uitgevers in de praktijk (de facto) een vrij zelfstandige positie.

Samenvattend gezegd zijn/ waren er (in de bestaande praktijk) een viertal specifieke privacy-issues:

1. de verspreiding van direct identificerende gegevens binnen c.q. over de leermiddelenketen;
2. de in de praktijk vrij zelfstandige positie van distributeurs en uitgevers en (mogelijke) gegevensverwerkingen door die partijen die zich aan het zicht van de scholen onttrekken dan wel waar de scholen zich niet (volledig) bewust van zijn;
3. de mogelijkheid dat distributeurs en uitgevers de gegevens waarover zij in het kader van hun rol in de leermiddelenketen beschikken, zouden (gaan) gebruiken voor de eigen bedrijfsvoering en zouden (gaan) gebruiken voor commerciële benadering van leerlingen of ouders;
4. de strikte regulering van het gebruik van bij wet ter identificatie aan personen toegekende nummers zoals het burgerservicenummer (BSN) en het persoonsgebonden nummer in het onderwijs (PGN).

2.2 Twee oplossingen

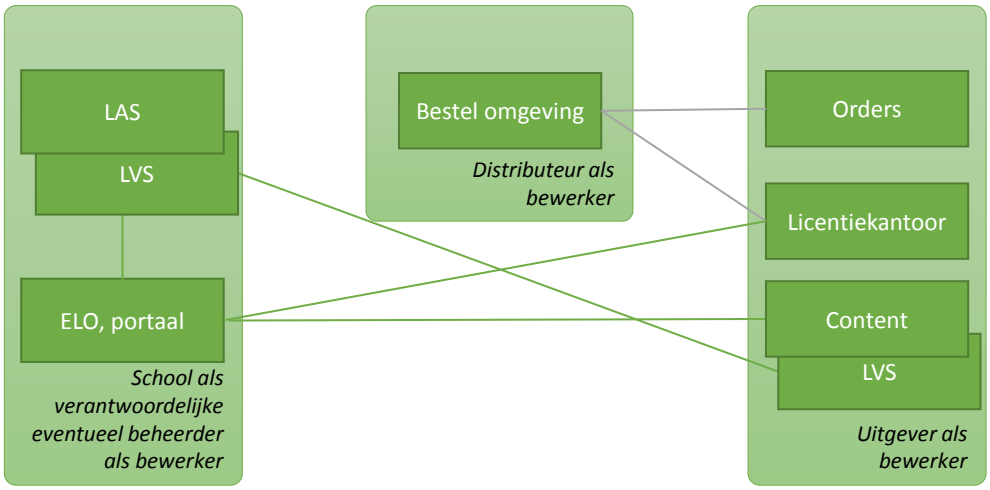
Om de vier geschetste privacy-issues aan te pakken, zijn twee ‘oplossingen’ ontstaan en ontwikkeld. Beide oplossingen adresseren daarbij (enkel) een deel van de privacy-issues. Deze twee ‘oplossingen’ zijn de Nummervoorziening met pseudoniemen en het Privacy Convenant.

Nummervoorziening met pseudoniemen
Om de geschetste privacy-issues aan te pakken is een nieuwe nummervoorziening en het gebruik van pseudoniemen als identificator ontstaan. De ontwikkeling van de Nummervoorziening was daarbij in oorsprong in het bijzonder ingegeven voor het oplossen van de bestaande matchingproblemen. De huidige verschillende datasets die als identificator gebruikt werden, worden daarbij vervangen door een nieuw uniek en eenduidig ketenpseudoniem. De Nummervoorziening en de ketenpseudoniemen zien daarbij zowel op leerlingen als op docenten.
Als gevolg hiervan zou de verspreiding van direct identificerende gegevens verminderd worden en zouden met name distributeurs en uitgevers niet meer - of in ieder geval in mindere mate - over direct identificerende gegevens van met name leerlingen beschikken. Een gevolg daarvan is weer dat distributeurs en uitgevers minder mogelijkheden overhouden om de gegevens - waarover zij in het kader van hun rol in de leermiddelenketen beschikken - te hergebruiken voor de eigen bedrijfsvoering en commerciële benadering van leerlingen of ouders. De nieuwe nummervoorziening en de ketenpseudoniemen waren (van oorsprong) niet gericht op het issue van de in de praktijk vrij zelfstandige positie van de distributeurs en uitgevers. Ook was de ontwikkeling van de Nummervoorziening en de introductie van pseudoniemen (in eerste instantie) niet zozeer gericht op een antwoord of maatregel voor de - vanuit privacybeleving ervaren onnodige of onwenselijke - verspreiding van gegevens van leerlingen (in de zin van verspreiding van gegevens over verschillende partijen). Wel beperkt het pseudoniem het aantal gegevens dat uitgewisseld wordt. Daarbij wordt de verspreiding van de eerdere datasets teruggebracht tot uitwisseling van het pseudoniem.

In paragraaf 2.3 wordt de werking van de Nummervoorziening in de leermiddelenketen verder beschreven.

Een Privacy Convenant
Een andere oplossing is het Privacy Convenant voor de leermiddelenketen of, beter gezegd: voor de distributeurs en uitgevers van leermiddelen.
Het convenant is nadrukkelijk ontstaan om de vanuit privacybeleving ervaren onnodige of onwenselijke situaties aan te pakken. Tevens is het convenant ontstaan om de in de praktijk bestaande vrij zelfstandige positie van de distributeurs en uitgevers op te lossen en de zeggenschap over de gegevensverwerking (weer) duidelijk neer te leggen bij de scholen zelf.
De insteek van het convenant is daarbij dat de scholen de rol van Wbp-verantwoordelijke hebben en deze rol ook, met steun van de onderwijsraden, oppakken en vormgeven. De distributeurs en zeker de uitgevers van leermiddelen handelen dan als Wbp-bewerker voor de scholen. Het convenant is daarvoor aangevuld met een zogenaamde - op grond van de Wet bescherming persoonsgegevens verplichte - bewerkersovereenkomst.
Het convenant richt zich daarbij niet op de gegevensverwerking in het kader van de nieuwe Nummervoorziening en is tevens beperkt tot de gegevensverwerking ter uitvoering van de taken en werkzaamheden van de scholen (les geven en het door leerlingen les volgen). In die zin is het Privacy Convenant niet zozeer gericht op het verminderen van de verspreiding van persoonsgegevens, maar veeleer gericht op het verzekeren dat de persoonsgegevens enkel ten behoeve van de scholen en onder regie en aansturing van de scholen verwerkt worden. Het Convenant concentreert zich daarbij op de verwerking van gegevens over leerlingen en bevat geen specifieke bepalingen over gegevens betreffende docenten.

Uitgaande van de weergave (zie hierboven) van de bestaande situatie, ziet de voorziene situatie met het Privacy Convenant en de bijbehorende bewerkersovereenkomsten er als volgt uit.



Figuur 2: Situatie na toepassing van het Privacy Convenant en de bewerkersovereenkomsten

De twee oplossingen in het licht van de vraag: Wbp-verantwoordelijke en/ of bewerker?
De Wbp-verantwoordelijke is de partij die het doel en de middelen van de gegevensverwerking bepaalt. Deze doelen hangen daarbij samen met de taken en werkzaamheden van de Wbp-verantwoordelijke. De bewerker is een externe partij die de Wbp-verantwoordelijke ondersteunt bij de gegevensverwerking. In algemene zin kunnen drie typen activiteiten en diensten onderscheiden worden die door bewerkers uitgevoerd worden. Dit zijn:

1. De hosting van ICT-systemen
   De rol van de bewerker is hierbij in feite beperkt tot het leveren van ruimten en hardware die de Wbp-verantwoordelijke zelfstandig kan gebruiken. De Wbp-verantwoordelijke beheert de systemen en applicaties in beginsel zelf en regelt ook zelf het technisch beheer van de applicaties. De partij die de hostingdienst levert, heeft in het algemeen geen of slechts beperkt toegang tot de persoonsgegevens die opgenomen zijn in de systemen en applicaties van de Wbp-verantwoordelijke.
2. Het technisch beheer van de ICT-systemen en de applicaties
   Hierbij beheert de bewerker de systemen en applicaties in technische zin. De technisch beheerder kan ook de partij zijn die een bepaalde applicatie ontwikkeld heeft. De producenten van leermiddelen die als technische beheerder optreden zijn vaak ook de partij die de applicatie voor de leermiddelen ontwikkeld heeft. Bij het technisch beheer heeft de bewerker in beginsel toegang tot de persoonsgegevens die met de systemen en applicaties verwerkt worden. Deze toegang is nodig voor het kunnen uitvoeren van het technisch beheer. In het algemeen behoren de ontwikkeling van applicaties zelf en ook de verdere doorontwikkeling daarvan niet tot de Wbp-bewerkerswerkzaamheden. Daarbij hebben applicatieontwikkelaars een zelfstandige rol.
3. De inhoudelijke verwerking van persoonsgegevens
   Hierbij voert de bewerker een aantal inhoudelijke taken voor de Wbp-verantwoordelijke uit en verwerkt daarbij persoonsgegevens. Een klassiek voorbeeld is een partij die voor de Wbp-verantwoordelijke de salarisadministratie voert. De bewerker heeft hierbij voor het uitvoeren van de inhoudelijke werkzaamheden voor de Wbp-verantwoordelijke – uiteraard – toegang tot de persoonsgegevens. Leermiddelenproducten kunnen in de praktijk ook inhoudelijke werkzaamheden uitvoeren. Hierbij valt te denken aan het bewerken en terugleveren aan scholen van resultaten van leerlingen om in bijv. leerlingvolgsystemen vast te leggen. Ook distributeurs zullen inhoudelijk gegevens verwerken voor bijvoorbeeld de levering van leermiddelen.

In de praktijk kunnen bij het verwerken van persoonsgegevens binnen de leermiddelenketen door producenten van leermiddelen (uitgevers) en distributeurs diverse bewerkersscenario's van toepassing zijn. Het is zelfs mogelijk dat een verwerker activiteiten en diensten aan een andere partij uitbesteedt. Zo is het mogelijk dat leermiddelenproducenten enkele inhoudelijke werkzaamheden en het technisch beheer uitvoeren, maar de hosting zelf weer uitbesteden aan een andere partij.

Bij de vraag welke partij de Wbp-verantwoordelijke (de scholen) en welke partij een bewerker (zoals leermiddelenproducenten) is en of de beheerder van de ICT-systemen die gebruikt worden eventueel toch aangemerkt dient te worden als bijvoorbeeld een (mede-)verantwoordelijke in de zin van de Wbp, staat de vraag centraal of de invloed en zeggenschap van de Wbp-verantwoordelijke (de scholen) zodanig is dat deze

ook daadwerkelijk als verantwoordelijke aangemerkt kunnen worden.[2]

Bij de beantwoording van de vraag of de invloed en zeggenschap van de scholen voldoende groot is om aangemerkt te (blijven) worden als Wbp-verantwoordelijke, kan een aantal onderwerpen onderscheiden worden om aan de hand daarvan de invloed en zeggenschap vast te stellen. Deze onderwerpen[3] zijn:

- Wie bepaalt de vast te leggen gegevens?
- Wie mag de gegevens raadplegen en wie geeft daar toestemming voor en voort daarop controle uit?
- Wie is verantwoordelijk voor en belast met controle op de juistheid en actualiteit van de gegevens?
- Wie bepaalt het bewaren c.q. verwijderen van gegevens?
- Wie voert de overige zorgplichten uit de Wbp uit, zoals een adequate beveiliging, het informeren van betrokkenen de mogelijkheid voor betrokkenen om hun rechten uit te oefenen?
- Wie bepaalt of eventueel een dienstverlener (ICT-bedrijf) voor het beheer wordt ingehuurd en aan welke voorwaarden deze dienstverlener dient te voldoen?

Als het voor één of meer van bovenstaande onderwerpen niet duidelijk is wat in de praktijk de precieze rolverdeling is of als een Wbp-verantwoordelijke onvoldoende zicht heeft op wat een bewerker doet, dan bestaat het risico dat de bewerker als Wbp-verantwoordelijke of als medeverantwoordelijke aangemerkt wordt enkel en alleen om het feit dat er, kort gezegd, te weinig duidelijkheid is. Kern bij invloed en zeggenschap is dat deze toekomt aan de Wbp-verantwoordelijken (hier: de scholen). De partij die de diensten levert en in beginsel de bewerker is of zou moeten zijn, wordt hierbij als dienstenleverancier toch Wbp-verantwoordelijke. Strikt genomen heeft een dergelijke dienstenleverancier die vanwege onduidelijkheid of een scheve machtsverhouding toch aangemerkt wordt als Wbp-verantwoordelijke geen deugdelijke juridische basis om als Wbp-verantwoordelijke persoonsgegevens te verwerken. In die zin is het veeleer een Wbp-verantwoordelijke "bij gebrek aan beter".

Op basis van de ontvangen documenten en de gevoerde gesprekken, komen wij tot de observatie dat, zeker in het verleden, de leermiddelenproducten (uitgevers) en de distributeurs juist vanwege onduidelijkheid over een aantal essentiële onderwerpen en een slechts marginale betrokkenheid en aansturing door de scholen, de facto als Wbp-verantwoordelijke opereerden.
Een andere observatie bij deze PIA is dat er bij het ontwerpen van de Nummervoorziening en zeker bij de discussie daarover soms, veelal impliciet, uitgegaan lijkt te worden van de opvatting dat de leermiddelenproducten en distributeurs als Wbp-verantwoordelijke aan te merken zijn. Ook in het politieke debat en bij de privacybezwaren tegen het verwerken van persoonsgegevens door bijvoorbeeld uitgevers, lijken de uitgevers veeleer als zelfstandige Wbp-verantwoordelijken beschouwd te worden dan als Wbp-bewerkers voor de scholen.

Het zijn het Privacy Convenant en de daarbij behorende bewerkersovereenkomst die de eerdere problemen met de rol en positie van leermiddelenproducten en –distributeurs regelen. Daarmee worden onduidelijkheden en scheve machtsverhoudingen tussen de scholen als Wbp-verantwoordelijken en de uitgevers en

---

[2] *Het criterium invloed en zeggenschap sluit aan bij de feitelijke invloed als bedoeld in het Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker" van de zogenaamde artikel 29 groep van 6 februari 2010, p.13-14. Het sluit tevens aan bij de in het Advies gememoreerde autonome beslisbevoegdheid, p.38. In dit Advies 1/2010 wordt (wat verwarrend) met het begrip "verwerker" de "bewerker" volgens de Wbp aangeduid.*

[3] *Zie ook de Memorie van Toelichting bij de Wbp, nr. 3, pp. 61-62 en het Advies van de artikel 29 Groep 1/2010, p.17.*

distributeurs aangepakt. Juridisch gezien leidt de aanpak met het Privacy Convenant en de bijbehorende bewerkersovereenkomst tot een belangrijke omslag. Eerder hadden uitgevers en distributeurs in feite geen of nauwelijks een deugdelijke juridische basis om als zelfstandig Wbp-verantwoordelijke persoonsgegevens van - in het bijzonder - leerlingen te verwerken. Daar waar zij eerder (onterecht) als Wbp-verantwoordelijke opereerden of (onterecht) als Wbp-verantwoordelijke werden gezien, worden ze nu - door hen expliciet de rol van bewerker toe te kennen - (ineens) wel bevoegd om persoonsgegevens voor de scholen als Wbp-verantwoordelijke te verwerken. Immers: een bewerker is bevoegd om voor de Wbp-verantwoordelijke de persoonsgegevens te verwerken die de Wbp-verantwoordelijke zelf ook mag verwerken.

Het is goed om te benadrukken dat deze verschillende posities van uitgevers en distributeurs en de juridische omslag en verduidelijking met het Privacy Convenant en de bewerkersovereenkomst, van specifiek belang is voor de PIA. Het is immers van belang om te voorkomen en te vermijden dat argumenten en bezwaren die horen bij de eerdere Wbp-verantwoordelijke-rol van de uitgevers, een rol pelen bij de huidige (nieuwe) rol als bewerkers voor de scholen. In die zin kan gesteld worden dat de juridische achtergrond bij de Nummervoorziening en de pseudoniemen als het ware verschoven is. Was de juridische noodzaak van pseudoniemen bij uitgevers en distributeurs eerder veeleer gelegen in de vraag of zijn überhaupt wel persoonsgegevens mochten verwerken, thans is de juridische vraag veeleer gelegen in welke mate zij persoonsgegevens dienen te verwerken en ook of met minder persoonsgegevens dan voorheen volstaan kan worden. Anders gezegd: de juridische discussie is als het ware verschoven van een nadruk op toelaatbaarheid c.q. rechtmatigheid (mag het?) naar een nadruk op toereikendheid en dataminimalisatie (welke gegevens zijn noodzakelijk?).

Een zeer specifiek issue waarvoor deze omslag met het convenant en de bijbehorende bewerkersovereenkomsten van belang is, is de vraag of het voorziene ketenpseudoniem en het gebruik daarvan zodanig dient te zijn, dat er geen sprake meer is van persoonsgegevens aan de kant van de distributeurs en uitgevers van leermiddelen. Bij gegevensverwerking waarbij de scholen de Wbp-verantwoordelijke zijn en de distributeurs en uitgevers optreden als Wbp-bewerker, is het vanuit de Wbp bezien echter niet nodig om pseudoniemen te gebruiken waardoor er geen sprake meer zou zijn van persoonsgegevens aan de kant van de Wbp-bewerkers. Nog los van de vraag of het inderdaad mogelijk is om pseudoniemen te gebruiken op een wijze waarbij er geen sprake meer is van persoonsgegevens, is het uitgangspunt bij deze PIA dat distributeurs en uitgevers als Wbp-bewerkers gerechtigd zijn om persoonsgegevens te verwerken. Voor een uitgebreide uiteenzetting over het juridisch lastige begrip persoonsgegevens wordt verwezen naar Bijlage C. Hier wordt enkel benadrukt dat het bij persoonsgegevens niet de vraag is of een bepaald gegeven op zich een persoonsgegeven is, maar dat het beoordelingscriterium is of alle gegevens die beschikbaar zijn (de gehele set van gegevens) in hun samenhang bezien persoonsgegevens - in de zin van de Wbp - opleveren. In die zin is dan ook niet relevant of het voorziene pseudoniem geheel op zichzelf en losstaand beschouwd, wel of geen persoonsgegeven is. Het gaat immers om de combinatie van het voorziene pseudoniem met alle andere gegevens waarover beschikt kan worden. Hierbij zal het pseudoniem dat vastgelegd is in de leerlingenadministratiesystemen van de scholen altijd een persoonsgegeven zijn. Dit enkel en alleen al omdat in die systemen ook de personalia en het PGN vastgelegd zijn. En - vanuit de Wbp bezien - zal het pseudoniem bij de Wbp-bewerkers in juridische zin ook altijd als persoonsgegeven aangemerkt dienen te worden. Dit dan enkel en alleen al vanwege het feit dat het pseudoniem voor de Wbp-verantwoordelijke (de scholen) een persoonsgegeven is.

Uitgangspunten voor de PIA
Op basis van de hierboven beschreven twee oplossingen en de opmerkingen over Wbp-verantwoordelijke en/ of bewerker, worden bij deze PIA de volgende uitgangspunten gehanteerd:

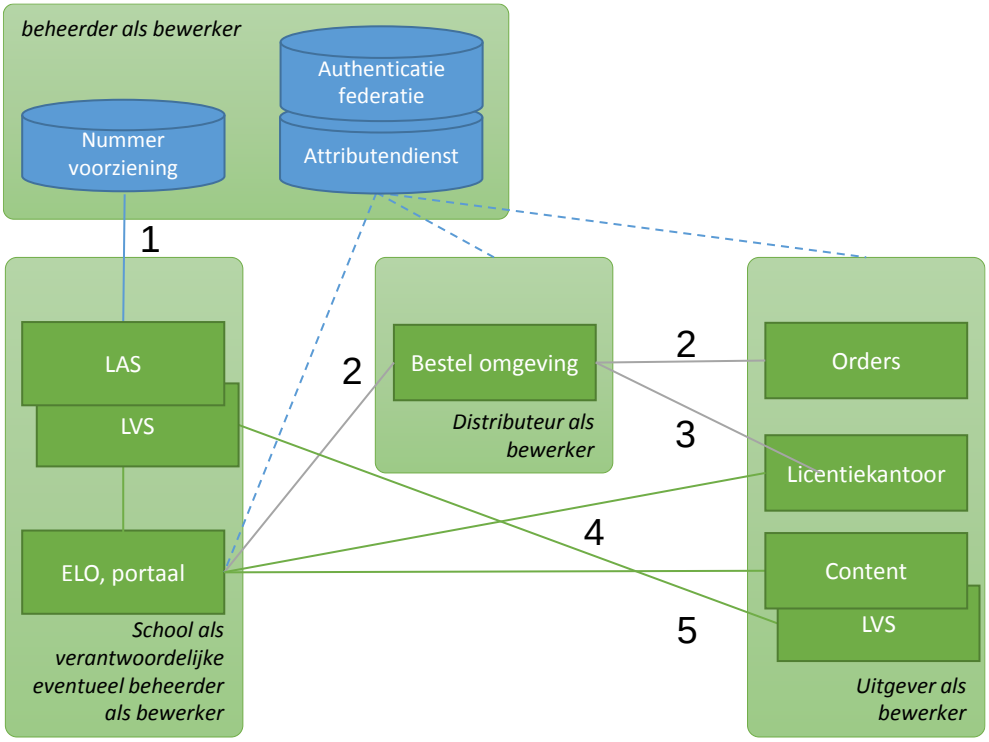
- Vanuit juridisch oogpunt bezien is het Privacy Convenant met bijbehorende bewerkersovereenkomst een essentiële voorwaarde om de Nummervoorziening en de voorziene pseudoniemen rechtmatig en in overeenstemming met de Wbp te kunnen gebruiken binnen de leermiddelenketen.
- Vanuit praktisch en juridisch oogpunt bezien ondersteunen de Nummervoorziening en de voorziene pseudoniemen het oplossen van eerdere matchingproblemen (praktisch) en dataminimalisatie en informatiebeveiliging waar dit mogelijk is (juridisch).
- Vanuit juridisch oogpunt bezien kunnen de Nummervoorziening en de voorziene pseudoniemen een technische bijdrage leveren aan een juiste balans in de verhouding tussen scholen als Wbp-verantwoordelijken en uitgevers en distributeurs als bewerkers. Dit in aanvulling op het Convenant en de bewerkersovereenkomst die meer de juridische en organisatorische bijdrage leveren voor deze balans. Door gebruik van het ketenpseudoniem kan immers bewerkstelligd worden dat de herleidbaarheid en de mogelijkheden voor distributeurs en uitgevers van leermiddelen om leerlingen en docente te identificeren (beduidend) verminderd worden.

2.3 Werking van de Nummervoorziening in de leermiddelenketen

In deze paragraaf wordt de werking van de Nummervoorziening in de leermiddelenketen beschreven. Het betreft een beschrijving op hoofdlijnen, opgesteld met het oog op het kunnen beoordelen van privacyaspecten in de leermiddelenketen.
De Nummervoorziening is een voorziening voor het aanmaken, wijzigen en (in de toekomst) verwijderen van pseudoniemen. Met de Nummervoorziening kan een unieke identificator (ketenpseudoniem) voor leerlingen en docenten worden gecreëerd. Dit pseudoniem is, zoals hierboven is aangegeven, aan te merken als een persoonsgegeven in de zin van de Wbp.
In het ontwerp van de Nummervoorziening is een aantal bepalende keuzes gemaakt die voor deze PIA de uitgangspunten vormen voor de werking van de Nummervoorziening in de leermiddelenketen:

- Een onderwijsdeelnemer heeft één ketenpseudoniem voor de gehele leermiddelenketen (ook wel de Educatieve Contentketen genoemd).
- Het PGN (het BSN of het Onderwijsnummer) van de leerling wordt gebruikt als basis voor het ketenpseudoniem.
- Het ketenpseudoniem is hetzelfde gedurende het verblijf van de leerling in een sector (PO, VO, MBO).
- Voor de leermiddelenketen wordt het ketenpseudoniem opgeslagen in de leerlingenadministratiesystemen.
- Ook voor de docent dient een ketenpseudoniem beschikbaar te zijn. In het Ontwerpbesluit wordt geen uitsluitsel gegeven over de wijze waarop het ketenpseudoniem voor docenten wordt gegenereerd en opgeslagen. In dit rapport wordt het uitgangspunt gehanteerd dat het ketenpseudoniem voor docenten hetzelfde dient te zijn per school c.q. per werkgever.

Onderstaande figuur geeft een schematische weergave van de leermiddelenketen en de plek die de Nummervoorziening daarbij inneemt. De nummers in de figuur refereren aan de processen (use cases) die daarna zijn beschreven.



Figuur 3: Schematische weergave van de Nummervoorziening in de leermiddelenketen

1. Eenmalig aanvragen van ketenpseudoniem en opslaan in het leerlingenadministratiesysteem

De school registreert het persoonsgebonden nummer (PGN) van een leerling in het leerlingenadministratiesysteem (LAS). Naast het persoonsgebonden nummer bevat het leerlingenadministratiesysteem ook de personalia en onderwijsgegevens van de leerling en – vanaf de inschrijving – de persoonsgegevens van de ouders of verzorgers van de leerling.
De Nummervoorziening is een op zichzelf staand systeem dat functies voor het aanmaken, wijzigen en (in de toekomst) verwijderen van ketenpseudoniemen beschikbaar stelt. Vanuit het leerlingenadministratiesysteem wordt een ketenpseudoniem aangevraagd bij de Nummervoorziening. Voordat het PGN wordt doorgegeven aan de Nummervoorziening wordt het gehasht (versleuteld). In het Ontwerpbesluit wordt niet expliciet vermeld waar en hoe het PGN wordt gehasht. In dit rapport wordt het uitgangspunt gehanteerd dat het PGN door het leerlingenadministratiesysteem wordt gehasht en vervolgens aan de Nummervoorziening wordt gestuurd.

De Nummervoorziening beschikt voor het samenstellen van het ketenpseudoniem over a) het gehashte PGN, b) een aanduiding van de keten (in dit geval de leermiddelenketen) en c) de onderwijssector (PO, VO of MBO). Deze drie elementen worden gezamenlijk gebruikt om een ketenpseudoniem samen te stellen. In die zin is het gehashte PGN zeker niet dé enige basis voor het ketenpseudoniem. Door meerdere elementen als basis voor het ketenpseudoniemen te gebruiken, kan bijvoorbeeld bereikt worden dat als een leerling met hetzelfde gehashte PGN naar een andere sector (element c) gaat (van PO naar VO), ook een ander ketenpseudoniem

krijgt. Ook kan bijvoorbeeld bereikt worden dat als de Nummervoorziening voor andere onderwerpen dan de leermiddelenketen gebruikt zou worden, een afwijkend pseudoniem toegekend kan worden. Dit omdat daarbij de keten (element b) anders is.

Bij de eerste uitgifte van het ketenpseudoniem voert de Nummervoorziening een aantal controles uit waaronder de controle op de autorisatie van de aanvrager. In de Nummervoorziening zelf worden geen andere persoonsgegevens verwerkt (of opgeslagen) dan het gehashte PGN dat wordt gebruikt om het ketenpseudoniem op te baseren en het aan de scholen te verstrekken ketenpseudoniem zelf.
Het ketenpseudoniem voor de leerling wordt geretourneerd naar de school en opgeslagen in het leerlingenadministratiesysteem. Een belangrijk aspect daarbij is dat het ketenpseudoniem door de verschijningsvorm (een zeer lange reeks onsamenhangende karakters c.q. een reeks van “enen en nullen”) alleen voor computers (en dus niet voor de mens) te interpreteren is. Vanaf het moment dat het ketenpseudoniem is opgeslagen in het leerlingenadministratiesysteem kan het worden gebruikt voor transacties in de leermiddelenketen.

Gelet op deze wijze van samenstellen van het ketenpseudoniem - waarbij het ketenpseudoniem op basis van meerdere elementen wordt samengesteld - komen wij in het kader van de PIA tot de volgende observaties ten aanzien van het voorziene ketenpseudoniem:

- Het door de school hashen van het PGN geschiedt in feite enkel ter beveiliging van de verzending naar de Nummervoorziening en om te voorkomen dat het PGN als PGN naar de Nummervoorziening verzonden wordt;
- Het ketenpseudoniem is door de meervoudige basis niet meer aan te merken als een een-op-eenpseudoniem van (enkel) het PGN;
- Het ketenpseudoniem kan, ook al is dit steeds gebaseerd op hetzelfde PGN van de leerling, variëren per sector en kan variëren per keten;
- Het ketenpseudoniem is niet vatbaar voor menselijk gebruik. In die zin wijkt het ketenpseudoniem (wezenlijk) af van bijvoorbeeld het PGN/ BSN zelf;
- Het aanmerken van de distributeurs en uitgevers van leermiddelen als één en dezelfde keten, lijkt voornamelijk ingegeven door praktische overwegingen en overwegingen ten aanzien van de uitvoerbaarheid. Wat de technische opzet van de Nummervoorziening betreft, lijkt een detaillering binnen de leermiddelenketen in beginsel mogelijk;
- Een verdere detaillering van de keten zou voor wat de scholen betreft, tot de situatie (kunnen) leiden dat deze meerdere ketenpseudoniemen voor eenzelfde leerling of docent vast dienen te (kunnen) leggen.

2. Bestellen van leermiddelen (digitaal en folio)

Scholen, leerlingen en ouders kunnen leermiddelen bestellen bij de distributeur. Ook de leverancier van leermiddelen kan daarbij als distributeur optreden. Er zijn daarbij een drietal mogelijkheden:

a) De school doet de bestelling.
b) De leerling gaat naar de bestelomgeving van de distributeur en identificeert zichzelf bij bestelling met een schoolaccount.
c) De leerling logt in op het portaal van de school en gaat vervolgens naar de bestelomgeving van de distributeur.

a) School doet de bestelling
   In situaties waar de school de bestelling doet is identificatie van de leerling niet nodig voor de bestelling en is het voldoende als het ketenpseudoniem tijdens gebruik beschikbaar is.
b) Leerling start bestelling in de bestelomgeving van de distributeur
   De leerling (en/ of ouder) gaat naar de bestelomgeving van de distributeur en start een bestelactie. Gedurende deze bestelactie zal de bestelomgeving de leerling vragen om in te loggen op de schoolomgeving, zodat het ketenpseudoniem beschikbaar komt. Als de leerling alleen folio leermiddelen besteld heeft, heeft de distributeur het ketenpseudoniem mogelijk niet verder nodig voor de feitelijke levering, maar zal deze wel dienen te beschikken over de NAW-gegevens van het afleveradres. Als de bestelling een gecombineerde levering van digitale en folio leermiddelen betreft heeft de distributeur voor de feitelijke levering zowel het ketenpseudoniem als de NAW gegevens van het afleveradres nodig.
c) Leerling gaat via schoolportaal naar de bestelomgeving van de distributeur
   De leerling (en/ of ouder) logt in op de schoolomgeving en heeft vanuit de schoolomgeving (op basis van het principe single sign-on) toegang tot de bestelomgevingen van de door school geselecteerde distributeurs en uitgevers. Daarbij wordt het ketenpseudoniem vanuit de schoolomgeving meegegeven aan de bestelomgeving van de distributeur.
   De leerling (of ouder) plaatst de bestelling in de bestelomgeving waarbij, indien nodig, ook de betaling wordt afgehandeld. In geval van een digitaal leermiddel bericht de bestelomgeving aan het licentiesysteem om een licentie voor het materiaal klaar te zetten voor de besteller.

3. Leveren leermiddelen (digitaal en folio)

In geval van folio leermiddelen (zoals boeken) zorgt de distributeur dat de bestelde leermiddelen worden afgeleverd op het opgegeven adres.
Voor de levering van digitale leermiddelen zijn diverse methoden voorhanden zoals:

- Via een activatiecode die door de distributeur is verstrekt aan de school of de leerling zelf;
- Het autoriseren van het gebruik van het leermiddel voor een (groep)leerling(en) op basis van het ketenpseudoniem

4. Gebruik van digitale leermiddelen

In geval van digitale leermiddelen logt de leerling in op het portaal of ELO van de school. Vervolgens klikt de leerling op de toegangslink of surft zelf naar de toegangspagina van het betreffende leermateriaal. Daarbij wordt (op basis van het principe single sign-on) toegang verschaft tot de juiste digitale omgeving van de betreffende leverancier/ uitgever en de lijst van gelicenseerde materialen. De leverancier/uitgever autoriseert en verleent toegang tot de leermiddelen op basis van het ketenpseudoniem van de leerling. Het autoriseren gebeurt op basis van de eerder gedane levering (in 3) waarbij de relatie bestelling – levering – gebruik wordt gelegd.

Na toegang te hebben gekregen gaat de leerling aan de slag. Elke toepassing hanteert zijn eigen didactische aanpak en behandelt een set leerdoelen. Methodes en toetsen vragen in sommige gevallen om het gebruik van persoonskenmerken zoals:

- Naam of initialen;
- Groep en / of leeftijd;
- Niveau en/ of leerstijl.

5. Ter beschikking stellen van toets- en leerresultaten aan de docenten c.q. de school

Het doel van het ter beschikking stellen van resultaten van leerlingen is om de resultaten in één overzicht te krijgen, zodat een docent een platform heeft waarmee hij het leerproces kan volgen en zijn rapportages op kan baseren. Het leerresultaat wordt daarbij vanuit het leermiddelsysteem opgehaald of verzonden op basis van het ketenpseudoniem. De docent (die ook een ketenpseudoniem heeft) kan de resultaten, voor zover nodig, opnemen in het leerlingvolgsysteem (LVS) van de school.

3. Compliance gerichte toets

3.1 Opzet compliance toets

De toets op de compliance bestaat uit vier toetsonderdelen.

Toetsonderdeel 1
Dit onderdeel ziet op de taken en werkzaamheden die uitgevoerd worden en wat daarvoor de (wettelijke) basis is. Ook de juridische positie van de verschillende partijen (scholen, leveranciers van leermiddelen en de Nummervoorziening) komen daarbij aan de orde. Daarbij speelt het voorziene Privacy Convenant een rol.

Toetsonderdeel 2
Dit onderdeel ziet op het doel waarvoor, ter uitvoering van de taken en werkzaamheden, persoonsgegevens verwerkt worden. Hierbij kan zowel toegestaan als niet toegestaan gebruik van gegevens voor bepaalde doelen aan de orde komen. Regelgeving en zeker ook zelfregulering kunnen de doelen waarvoor wel en waarvoor geen persoonsgegevens verwerkt worden nader bepalen. Het voorziene Privacy Convenant speelt eveneens een rol bij de (nadere) bepalingen van de doelen waarvoor (scholen) persoonsgegevens verwerken.

Privacywetgeving stelt bij de vraag of gegevensverwerking toegestaan is altijd het doel centraal. Het gebruik van een identificator is dus altijd afhankelijk van het doel waarvoor de persoonsgegevens (de gehele set persoonsgegevens) verwerkt worden. Als doelen verschillen of gelegen zijn bij verschillende zelfstandige partijen, dan verschilt ook de juridische mogelijkheid om wel of geen identificator te gebruiken en de eisen die dan aan een identificator gesteld worden.

Toetsonderdeel 3
Dit onderdeel betreft een toets welke gegevens noodzakelijk zijn om de doelen te bereiken. Hierbij spelen nadrukkelijk de gewenste en te bereiken dataminimalisatie en het voorziene gebruik van pseudoniemen als identificator in de leermiddelenketen een rol.

Toetsonderdeel 4
Dit betreft de toets van de juridische basis met in dit geval:
- de in artikel 8 van de Wbp vermelde grondslag die voor het verwerken van persoonsgegevens van toepassing is;

- de regeling over het verwerken van de in artikel 16 van de Wbp bedoelde bijzondere persoonsgegevens, bijvoorbeeld in het kader van resultaten bij proeftoetsen. Op basis van de beschikbare gegevens ligt het verwerken van bijzondere gegevens niet meteen voor de hand. Echter, in bepaalde gevallen kan alleen al de school waar een leerling ingeschreven is, leiden tot bijvoorbeeld gegevens over de gezondheid;
- de regeling over het gebruik van de in artikel 24 Wbp bedoelde - bij wet voorgeschreven - nummers ter identificatie van een persoon, zoals het persoonsgebonden nummer in het onderwijs en het burgerservicenummer. Hierbij zal ook aan de orde komen of en in welke mate een op het BSN-gebaseerd pseudoniem nog wel of niet als een artikel 24 Wbp-nummer aangemerkt kan of zou moeten worden. In Bijlage B is een overzicht opgenomen van de voor het gebruik binnen de leermiddelenketen relevante bepalingen over het PGN en het gebruik van het PGN.

Daarbij zal er aandacht zijn voor de situaties waarbij persoonsgegevens gebruikt c.q. verstrekt worden aan andere organisaties (doelbinding) en situaties waarbij reeds aanwezige gegevens binnen een organisatie voor een ander doel hergebruikt worden. Bij dit hergebruik kan het gaan om gegevens die men eerder als Wbp-verantwoordelijke al verwerkte en ook kan het gaan om hergebruik van gegevens die men eerder enkel als bewerker ter beschikking had.

3.2 Taken, doelen en noodzakelijke gegevens

De gegevensverwerkende partijen - vooral die in het kader van de leermiddelenketen impact op de privacy kunnen hebben - zijn de scholen, de distributeurs en de uitgevers van leermiddelen. Daarnaast kunnen overigens ook de Nummervoorziening zelf (de beherende partij van de Nummervoorziening) en de partijen die de eerder beschreven inlogfaciliterende applicaties (SSO) beheren impact hebben op de privacy. Uiteraard hebben ook beheerders c.q. bewerkers die voor scholen de administraties zoals LAS, LVS en ELO beheren impact op de privacy. Deze laatste partijen vallen buiten het bestek van deze PIA.

De scholen
De primaire taak van een school is lesgeven. In de context van leermiddelen zijn hun belangrijkste taken het gebruiken van leermiddelen en het verwerken en analyseren van resultaten die met leermiddelen zijn bereikt. De school voert de verwerking van persoonsgegevens voortvloeiende uit deze taak uit vanuit de rol als zelfstandig Wbp-verantwoordelijke. Voorbeelden van doelstellingen voor het verwerken van gegevens zijn het gebruik van de leermiddelen en gepersonaliseerd leren aan de hand van het gebruik en vooral de resultaten bij het gebruik van leermiddelen. De doeleinden worden in het Privacy Convenant nader en gedetailleerd aangeduid. Hiermee wordt bijvoorbeeld artikel 7 van de Wbp ingevuld en geconcretiseerd. De grondslag voor gegevensverwerking door de scholen in verband met leermiddelen ligt hierbij in artikel 8, onder e, Wbp voor zover men aanneemt dat er sprake is van een publiekrechtelijke taak van een bestuursorgaan (voorstelbaar bij openbare scholen) en voor het overige ligt - specifiek voor de leermiddelenketen - de grondslag in artikel 8, onder f, Wbp dat ziet op de goede uitvoering van taken en werkzaamheden van de Wbp-verantwoordelijke. Hierbij is het goed om te benadrukken dat de Wet bescherming persoonsgegevens de gegevensverwerking in het kader van leermiddelen regelt en in die zin niet ziet op de keuze voor en aanschaf van leermiddelen als zodanig.

De uitgevers en distributeurs van leermiddelen
De taken en werkzaamheden van leveranciers van leermiddelen zijn het leveren van leermiddelen en het ontwikkelen en/ of leveren van aanpalende diensten (zoals aanvullend studiemateriaal of extra oefenstof). Daar waar de leermiddelenleveranciers optreden als partner van school (leveren leermiddelen en beheren van de ICT-omgeving voor die leermiddelen) vervullen zij (in beginsel) de rol van Wbp-bewerker. Het leveren en ontwikkelen van aanpalende diensten doen zij meer vanuit de rol als zelfstandig Wbp-verantwoordelijke.

In de rol van Wbp-bewerker hebben de leermiddelenproducenten (distributeurs en uitgevers) geen eigen doelen voor het verwerken van gegevens. Het gaat hierbij enkel om de doelen van de scholen als Wbp-verantwoordelijke die door de werkzaamheden van de bewerkers ondersteund worden.

Bij het ontwikkelen van verdere diensten zoals het aanbieden van eventueel extra niet-verplicht lesmateriaal, het verbeteren van leermiddelen of het gerichter adviseren voor het gebruik van aanvullende leermiddelen

(adviseren gelet op de resultaten bij het gebruik van verplichte leermiddelen die voor de school beheert worden), gaat het wel om doelen ten dienste van de (commerciële bedrijfsvoering) leermiddelenproducenten. Mogelijk is er daarbij, bijvoorbeeld bij het verbeteren van leermiddelen, een gezamenlijk belang of doel voor zowel scholen als producenten.

De beheerders van de Nummervoorziening en van de inlogfaciliterende applicaties (SSO)
De in het Privacy Convenant ingezette lijn dat de scholen Wbp-verantwoordelijke zijn en de distributeurs en uitgevers als Wbp-bewerker handelen, kan ook toegepast worden op de verhouding tussen de scholen en de (feitelijk) beheerder van de Nummervoorziening en de (feitelijk) beheerders van de inlogfaciliterende applicaties (SSO). Die partijen zijn, evenals de distributeurs en uitgevers, Wbp-bewerkers voor de scholen. Dat hiervoor nog nadere aandacht nodig is, komt in onderdeel B van paragraaf 3.3.4 verder aan de orde.

Doelen en noodzakelijke gegevens
Voor het specifieke gebruik van een identificator (een gegeven of een dataset met meerdere gegevens) die een unieke aanduiding van de leerling geven, wordt een aantal specifieke doelen onderscheiden. Dit zijn:

- Gebruik van leermiddelen waarbij met de identificator vastgesteld kan worden dat gebruiker bevoegd is en waarbij individualiseerbaarheid (om welke gebruiker gaat het?) niet noodzakelijk is;
- Gepersonaliseerd leren met eenvoudige en veilige toegang tot digitaal leermateriaal waarbij individualiseerbaarheid (en een individuele identificator) wel noodzakelijk zijn met daarbij:
  - De identiteit van de gebruiker (wie is de gebruiker precies) is noodzakelijk, bijvoorbeeld bij examens;
  - De identiteit van de gebruiker is niet noodzakelijk, maar de resultaten dienen wel aan de juiste gebruiker toegerekend dienen te worden (individualiseerbaarheid);
- Het feitelijk verminderen van de herleidbaarheid van leerlingen en studenten door het verkleinen van de set persoonsgegevens die - alleen ten behoeve van matching - moet worden gedeeld. In concreto: het vervangen van de huidige datasets met direct identificerende persoonsgegevens door het voorziene pseudoniem.

Bij het bepalen van doelen waarvoor gegevens benodigd zijn wordt onderscheid gemaakt tussen:

- Verplichte leermiddelen (die behoren tot het standaard lesmateriaal) en niet verplichte leermiddelen (kunnen aanvullend door de leerling worden besteld/ aangevraagd en gebruikt)
- Levering van leermiddelen aan of via de school of aan of via de leerling
- Elektronische leermiddelen en niet elektronisch leermiddelen
- Leermiddelen waarvoor wel gegevens van de leerling nodig zijn (bij de bestelling en/ of bij het gebruik van een leermiddel) en leermiddelen waarvoor geen gegevens van de leerling nodig zijn.

In onderstaande tabel zijn de mogelijke situaties bij de bestelling, levering en gebruik van verplichte leermiddelen en het terug leveren van leerresultaten weergegeven. Per mogelijke situatie zijn de werkwijze en de gegevens die de distributeur en de uitgever minimaal nodig hebben, beschreven. Ter verduidelijking wordt een voorbeeld gegeven. Een aantal situaties is niet mogelijk of onwaarschijnlijk. De kolom ‘wel/ geen gegevens van leerling nodig’ ziet op de positie van de leermiddelenproducent (distributeurs en uitgevers). Als een producent daarbij Wbp-bewerker is (en als bewerker mag wat de school als Wbp-verantwoordelijke mag) staan minder persoonsgegevens en het vervangen van datasets door een ketenpseudoniem in het licht van datamini-malisatie en verdere bescherming van gegevens. Als een producent daarbij meer een Wbp-verantwoordelijke is (verbeteren leermiddelen of aanbieden van extra niet-verplichte leermiddelen) staan minder of geen persoonsgegevens vooral (en wel degelijk) in het licht van de rechtmatigheid van de gegevensverwerking.

Mogelijke situaties			Werkwijze	Voorbeeld	Benodigde gegevens
Levering via/ aan de school	Elektronisch leermiddel	Wel gegevens van leerling nodig	Bestelling:school bestelt leermiddelen bij distributeur en geeft ketenpseudoniemen van leerlingen door aan de distributeur Levering: Uitgever autoristeert obv ketenpseudoniemen Gebruik: Leerling logt in met schoolaccount en krijgt obv ketenpseudoniem toegang tot het elektr. leermiddel. Terugleveren resultaten: Uitgever levert resulaten terug aan school obv ketenpseudoniem.	Opgaven waarbij de resultaten van de leerling aan de leraar/ school ter beschikking staan.	Distributeur - Ketenpseudoniem - School en klas - Leermiddel Uitgever - Ketenpseudoniem* - School - Leermiddel * NB: t.b.v. servicedoeleinden (helpdesk) is mogelijk ook naam leerling noodzakelijk.
		Geen gegevens van leerling nodig	Bestelling: school bestelt leermiddelen bij distributeur op basis van aantal licenties of school ontvangt via distributeur toegangscodes voor leerlingen Levering: uitgever autoristeert obv aantal gebruikte licenties of obv toegangscodes Gebruik: Leerling logt in met schoolaccount en krijgt via portaal automatisch toegang tot het elektr. leermiddel of leerling logt in met ontvangen toegangscode. Terugleveren resultaten: n.v.t.	Oefenpakket waarvoor de school een gelimiteerd aantal licenties heeft aangeschaft	Distributeur - School en klas - Leermiddel Uitgever - School en klas* - Leermiddel
	Folio leermiddel	Wel gegevens leerling nodig		Deze situatie is onwaarschijnlijk	
		Geen gegevens leerling nodig	School schaft leermiddel aan en deelt leermiddel fysiek uit aan leerling(en)	Werkboek dat door de school is betaald en aan leerlingen wordt uitgereikt.	Geen gegevens leerling nodig
Levering aan de leerling	Elektronisch leermiddel	Wel gegevens van leerling nodig	Bestelling: leerling logt in met schoolaccount en bestelt (en betaalt) leermiddel. Levering: uitgever autoriseert leerling op basis van ketenpseudoniem Gebruik: leerling logt in met schoolaccount en krijgt obv ketenpseudoniem toegang tot elektr. leermiddel. Terugleveren resultaten: Uitgever levert resulaten terug aan school obv ketenpseudoniem.	Opgaven waarbij de resultaten van de leerling aan de leraar/ school ter beschikking staan.	Distributeur - Ketenpseudoniem - School en klas - NAW- en betaalgegevens van besteller - Leermiddel Uitgever - Ketenpseudoniem* - School - Leermiddel
		Geen gegevens leerling nodig		Deze situatie komt niet voor	
	Combinatie van elektro-nische en folio leermiddelen	Wel gegevens van leerling nodig	Bestelling: leerling logt in met schoolaccount en bestelt (en betaalt) leermiddelen. Levering: Voor elektronische leermiddelen autoristeert uitgever obv ketenpseudoniem. Folio leermiddelen worden afgeleverd op adres dat leerling opgeeft. Gebruik: Voor het gebruik van elektronische leermiddelen logt leerling logt in met schoolaccount en krijgt obv ketenpseudoniem toegang tot elektr. leermiddel. Terugleveren resultaten: Uitgever levert resulaten met elektronische leermiddelen terug aan school obv ketenpseudoniem.	Bestelling van elektronische opgaven (waarbij de resultaten van de leerling aan de leraar/ school ter beschikking staan) in combinatie met schoolboeken	Distributeur - Ketenpseudoniem - School en klas - NAW- en betaalgegevens van besteller - NAW-gegevens van afleveradres - Leermiddel Uitgever (alleen elektronische leermiddelen) - Ketenpseudoniem* - School - Leermiddel
		Geen gegevens leerling nodig		Deze situatie komt niet voor	
	Folio leermiddel	Wel gegevens van leerling nodig	Bestelling: leerling logt in met schoolaccount en bestelt (en betaalt) leermiddel. Levering: Leermiddel wordt afgeleverd op adres dat leerling.opgeeft. Gebruik: geen elektronisch gebruik Terugleveren resultaten: n.v.t.	Schoolboeken	Distributeur - School en klas - NAW- en betaalgegevens van besteller - NAW-gegevens van afleveradres - Leermiddel
		Geen gegevens leerling nodig		Deze situatie komt niet voor	

Tabel 1: Mogelijke situaties voor verplichte leermiddelen en de daarbij benodigde gegevens

Uit bovenstaande tabel blijkt dat:

- alleen de distributeur zou hoeven te beschikken over de NAW-gegevens en betaalgegevens van de besteller en over de NAW-gegevens van het afleveradres (en de uitgever dus niet);
- de distributeur bij een gecombineerde levering van digitale en folio leermiddelen dient te beschikken over zowel het ketenpseudoniem als de NAW gegevens van de besteller en de NAW gegevens van het afleveradres. In bepaalde gevallen zal, afhankelijk van de inrichting van de bestelomgeving, ook daarbij het ketenpseudoniem gebruikt worden;
- alleen de uitgever zou hoeven te beschikken over de resultaten van leerlingen (en de distributeur dus niet).

Voor de niet verplichte leermiddelen is eenzelfde tabel op te stellen. Als aangenomen mag worden dat de levering van niet verplichte leermiddelen niet via de school verloopt, gaat het alleen om de leermiddelen die aan de leerling worden verstrekt. Het belangrijkste verschil met verplichte leermiddelen is dat een leerling een keuze zal hebben om resultaten die worden bereikt met niet verplichte leermiddelen wel of niet aan de school door te laten geven.

3.3 Juridische basis

3.3.1 Noodzakelijkheid van een identificator

In paragraaf 2.1 is reeds geconstateerd dat een identificator inderdaad noodzakelijk is, maar dat daarmee nog geenszins vaststaat welke identificator gebruikt kan worden en hoe het gebruik daarvan ingeregeld wordt.

Binnen de leermiddelenketen zijn in ieder geval vier mogelijke en (in beginsel) bruikbare identificatoren die gebruikt zouden kunnen worden. Dit zijn:

1. De NAW-gegevens;
2. Het BSN/ PGN;
3. Een ander door mensen te gebruiken nummer, zoals bijvoorbeeld een leerlingnummer of een personeelsnummer voor docenten;
4. Een ketenpseudoniem als een niet door mensen te gebruiken nummer.

Het is duidelijk dat voor een goede werking in de praktijk datasets bestaande uit NAW-gegevens niet te verkiezen zijn. De voorziene Nummervoorziening en het ketenpseudoniem zijn juist bedoeld om deze datasets met direct identificerende gegevens in de toekomst te vervangen. In die zin verdient het voorkeur om een nummer als identificator te gebruiken.

Het is eveneens duidelijk dat door mensen te gebruiken nummers die veelal ook als direct identificerende persoonsgegevens aangemerkt dienen te worden, een bredere verspreiding van herkenbare persoonsgegevens met zich meebrengt dan het voorziene ketenpseudoniem. Dit zelfs nog los van de vraag of het PGN van leerlingen of het BSN van docenten überhaupt wel als identificator gebruikt zouden mogen worden. Duidelijk is wel dat het BSN van docenten, gelet op de doelen waarvoor scholen hierover mogen beschikken, niet als identificator gebruikt kan worden zonder nadere regelgeving als bedoeld in artikel 24 van de Wbp (zie over art. 24 Wbp ook Bijlage B).

De conclusie in de PIA is dat een **ketenpseudoniem de voorkeur verdient als identificator binnen de leermiddelenketen** boven datasets met NAW-gegevens en boven direct identificerende nummers zoals het PGN of bijvoorbeeld het personeelsnummer voor docenten. Ook deze constatering geeft echter nog niet aan welk ketenpseudoniem (wat voor soort ketenpseudoniem) gebruikt dient te worden en wat (welke gegevens of welke dataset) voor dat ketenpseudoniem dan als basis gebruikt kan worden. Zoals in paragraaf 2.3 al is aangegeven, gaat de huidige opzet voor het pseudoniem uit van een combinatie van (gehasht) PGN, de sector en de keten als drievoudige basis voor het ketenpseudoniem.

3.3.2 Noodzakelijkheid van een nummer als identificator

Nummers die aan personen worden toegekend, worden voor één of meer verschillende functies gebruikt. Naast de administratieve functie zijn persoonsnummers ook een veelgebruikt hulpmiddel bij het vaststellen van de identiteit van een persoon. Om te kunnen bepalen of het gebruik van een bepaald nummer noodzakelijk is, hangt af van de functies die een nummer vervult. Een door een organisatie zelf toegekend leerling-, klant- of personeelsnummer voldoet veelal voor de administratieve functie, maar veelal juist niet voor de functie bij identiteitsvaststelling. Er zijn drie functies van nummers te onderscheiden:

1. De administratieve functie. Het nummer is een hulpmiddel bij:
   - het vastleggen en weer raadplegen/ophalen van gegevens over een bepaalde persoon;
   - het uitwisselen van gegevens over een bepaalde persoon;
   - de communicatie met een bepaalde persoon.
2. Nummers als representatie van een bepaalde bevoegdheid of hoedanigheid. Vergelijk:
   - pincode: representeert dat degene die de pincode invoert bevoegd is de bankpas te gebruiken,
   - Een personeelsnummer of leerlingnummer: representeert dat iemand een medewerker of leerling van een school is of in het verleden geweest is.
3. Nummer als uitvloeisel/resultaat van een eerder proces (bijv. identiteitsvaststelling). Het nummer wordt pas toegekend ná een bepaalde identiteitscontrole. Een typisch voorbeeld is het Strafrechtketennummer. Dat krijgt iemand pas na een zeer specifieke en uitgebreide vaststelling van de identiteit. Ook het BSN kent een voorafgaande identiteitsvaststelling, zeker als iemand uit het buitenland naar Nederland verhuist en zich in Nederland vestigt en daarbij een BSN krijgt.

Hierbij is van belang dat een nummer de mogelijkheid biedt dataminimalisatie toe te passen. Hierbij wordt ter aanduiding van de persoon enkel het nummer vastgelegd, in plaats van een gegevensset met de personalia en adresgegevens. Bij een dergelijke dataminimalisatie is tevens sprake van een bepaalde mate van versluiering van de identiteit omdat personalia dan niet meer vastgelegd worden. De mogelijkheid tot dataminimalisatie, waarbij het nummer een uitgebreidere dataset vervangt, kan bij nummers als representatie van een bepaalde bevoegdheid of hoedanigheid of nummers als uitvloeisel/resultaat van een eerder proces (bijv. identiteitsvaststelling) benut te worden. Of en in welke mate er daadwerkelijk sprake is van dataminimalisatie of versluiering van de identiteit hangt daarbij niet af van het nummer zelf, maar de gehele dataset waarover men beschikt. Een voorbeeld. Het is duidelijk dat het voorziene ketenpseudoniem in de leermiddelenketen op zich

de identiteit verluiert. Als het ketenpseudoniem daarbij echter vastgelegd wordt als onderdeel van een dataset waarin ook het BSN of de NAW-gegevens opgenomen zijn, is er echter geen verluierende of data minimaliserende werking meer.

In het kader van deze PIA komen we tot de conclusie dat **de identificator (het ketenpseudoniem) met name een administratie functie vervult en, bij het gebruik van bepaalde digitale leermiddelen, de bevoegdheid representeert om die leermiddelen te gebruiken**. Binnen de leermiddelenketen heeft de identificator geen functie als nummer dat het resultaat is van een voorafgaande identiteitsvaststelling. Dit sluit overigens aan bij het gebruik van het PGN. Ook het PGN heeft met name een administratieve functie en identiteitsvaststelling is binnen het onderwijs (bij inschrijven van leerlingen) expliciet niet verplicht gesteld.

3.3.3 Het te gebruiken type nummer

Naast verschillende functies van nummers, zijn er ook verschillende typen nummers. Relevant zijn dan: welke typen nummers kunnen onderscheiden worden, wat zijn de privacyrisico's van nummers en welke specifieke regels zijn er over het gebruik van nummers?

Er kunnen drie typen nummers onderscheiden worden:

a. algemene nummers (bijvoorbeeld het BSN),
b. sectorale nummers (bijvoorbeeld het voorgestane ketenpseudoniem),
c. lokale nummers (bijvoorbeeld het personeelsnummer)

Het type nummer speelt een rol bij de reikwijdte waarvoor het nummer gebruikt wordt. Zo hebben algemene nummers een algemeen bereik. Als uitgangspunt kan gehanteerd worden dat de beoogde reikwijdte van een nummer moet corresponderen met het te gebruiken type nummer: de reikwijdte moet passen bij het type nummer en het type nummer moet passen bij de reikwijdte. Privacywetgeving gaat er daarbij vanuit dat juist een "breed" of "breder" gebruik van een nummer een onderbouwing behoeft en heeft in die zin als stelregel dat de reikwijdte in beginsel beperkt dient te zijn tot lokale nummers en sectorale nummers.

Voor wat de reikwijdte van de voorgestelde ketenpseudoniemen betreft spelen verschillende aspecten voor de verschillende betrokken partijen een rol. Aspecten die met name een rol spelen zijn:

- Het pseudoniem vervangt het huidige gebruik van datasets die vanwege hun inhoud (NAW-gegevens) een zeer brede reikwijdte hebben. Dergelijke gegevens, met name personalia, blijven immers lange tijd zo niet gedurende het gehele leven hetzelfde. In die zin levert een sectoraal ketenpseudoniem zoals voorzien is, op voorhand al een beperking van de reikwijdte van de te gebruiken identificator.
- Bij verhuizing van een leerling worden op basis van hetzelfde pseudoniem administratieve lasten verlicht en fouten voorkomen door resultaten, dossiers en licenties te delen met de nieuwe school. In het MBO is de student zelf ook eigenaar van de licenties en moeten deze verbonden blijven aan de student en diens ketenpseudoniem.

- Als scholen overstappen van leverancier van een LAS, LVS of ELO verkleind een sectoraal ketenpseudoniem migratie-perikelen en eventuele fouten daarbij.[4]

Op basis van deze aspecten, komen we in deze PIA tot onderstaande observaties. We tekenen hierbij aan dat het om een afweging van factoren en aspecten gaat en in die zin niet om dwingende conclusies.

Voor wat de reikwijdte van het voorziene ketenpseudoniem betreft, komen we, strikt juridisch bezien, tot onderstaande bevindingen.

Vanuit het oogpunt van de scholen bezien is de conclusie dat een sectorale identificator zoals het voorziene ketenpseudoniem en de thans voorziene uitgifte per sector (PO, VO en MBO), als juridisch mogelijk aan te merken is voor zover dit enkel en alleen het ketenpseudoniem zelf betreft. Een aandachtspunt daarbij is dat met een gelijkblijvend ketenpseudoniem bij een overstap binnen een sector (bij voorbeeld van de ene basisschool naar de andere), de mogelijkheid ontstaat dat de nieuwe school kennisneemt van in leermiddelensystemen vastgelegde gegevens en resultaten die zijn gegenereerd tijdens het verblijf op de eerdere school. Ook is niet uitgesloten dat de eerdere school kennis zou kunnen krijgen van gegevens die gegenereerd worden bij de nieuwe school. Dit aspect is met name van belang omdat er reeds een specifieke regeling is ten aanzien van overdrachtsdossiers. Een gelijkblijvend pseudoniem mag er niet toe leiden dat er de facto meer gegevens voor de nieuwe school beschikbaar komen dan op grond van de huidige regelgeving bij overdracht (zoals onderwijskundig rapport, overstap service onderwijs) toelaatbaar is. We bevelen dan ook aan om nader aandacht te besteden aan dit onderwerp en de relatie met de reeds bestaande regeling over overdrachtsdossiers bij wijziging van school binnen een bepaalde sector. Daarbij kan ook aandacht besteed worden aan de overgang van Wbp-verantwoordelijkheid als een leerling naar een andere school gaat en gebruik blijft maken van dezelfde leermiddelen.

Vanuit de leerling bezien achten wij het kunnen volgen van leerlijnen en het kunnen blijven gebruiken van persoonlijk aangeschafte autorisaties voor digitale leermiddelen de inhoudelijke criteria voor de bepaling van de reikwijdte van het ketenpseudoniem. Dit betekent dat bij verhuizing naar een andere school binnen dezelfde sector (PO, VO of MBO) er voldoende redenen zijn om het pseudoniem te behouden. Dit is juridisch aanvaardbaar. Bij de overgang van PO naar VO en van VO naar bijvoorbeeld HBO of universiteit zijn er geen leerlijn-argumenten die ertoe noodzaken dat hetzelfde pseudoniem behouden blijft. Indien een overgang van VO (met name Vmbo) naar MBO ertoe noodzaakt dat eenzelfde pseudoniem behouden wordt in verband met het (wel) doorlopen van de specifieke leerlijn, verzet de Wbp zich daar niet tegen.

Bezien vanuit de leermiddelenproducenten is voorstelbaar dat er meerdere of verschillende identificatoren zouden (kunnen) zijn voor een bepaalde leerling. Omdat de distributeurs en uitgevers binnen de leermiddelketen als Wbp-bewerker voor de scholen optreden, is er echter geen strikt juridische noodzaak om meerdere pseudoniemen te hanteren.

[4] Bij de mogelijke maatregelen in paragraaf 4.2 bevelen wij aan om encryptie toe te passen op het ketenpseudoniem (en het PGN) in vooral de systemen van de scholen (LAS etc.). Met deze maatregel wordt het risico op misbruik van het ketenpseudoniem na een datalek in een LAS verkleind. Dit verminderde risico is voor ons tevens een aspect dat meeweegt bij de afweging van de reikwijdte.

Voorgaande vrij strikt juridische beoordeling van de reikwijdte van het ketenpseudoniem, laat de specifieke privacyrisico's van nummers in dit onderdeel buiten beschouwing. Deze privacyrisico's komen in hoofdstuk 4 aan de orde. In die zin gaat het in dit onderdeel om voorlopige conclusies over de reikwijdte van het ketenpseudoniem.

3.3.4 Passend gebruik

Bij het verwerken van persoonsgegevens en dus ook bij het gebruik van de Nummervoorziening en pseudoniemen, is naast aandacht voor de taken, doelen en de noodzakelijke gegevens, ook aandacht nodig voor de gegevensverwerking in de praktijk en voor de wijze waarop de gegevensverwerking dan plaatsvindt. Het onderdeel over passend gebruik gaat in het bijzonder over het "hoe' van de gegevensverwerking en het gebruik van ketenpseudoniemen. De verschillende elementen die bij passend gebruik aan de orde komen zijn:

A. Verschillende technieken voor het bewerken van gegevens;
B. De machtsverhouding tussen scholen en leermiddelendistributeurs en -uitgevers;
C. De basis voor het te gebruiken ketenpseudoniem;

A. Technieken voor het bewerken van gegevens

In de diverse documenten van het project voor de Nummervoorziening, het Privacy Convenant en in de discussie over de Nummervoorziening en het ketenpseudoniem keren de begrippen anonimiseren, encryptie, en pseudonimiseren herhaaldelijk terug. Verwarrend daarbij is dat deze begrippen soms gebruikt worden om een bepaalde techniek voor het bewerken van gegevens aan te duiden en soms gebruikt worden om een bepaald resultaat aan te duiden. Zo wordt het begrip 'anonimiseren' gebruikt voor de situatie waarin er geen sprake meer is van persoonsgegevens. Hierbij dient bedacht te worden dat het Cbp voorheen (bijvoorbeeld bij de risicoverevening in de gezondheidszorg) het begrip pseudonimiseren gebruikte om aan te geven dat het resultaat van het 'proces van pseudonimiseren' de situatie is dat er geen sprake meer is van persoonsgegevens. Bij dat proces werd een vijftal voorwaarden geformuleerd en was bepaald meer nodig dan enkel de inzet van pseudonimiseren als techniek. Tegenwoordig gebruikt het Cbp in navolging van de Europese art. 29-Groep) in dat verband de term anonimiseren om een resultaat aan te geven.

In de tabel hieronder wordt, op hoofdlijnen, een beeld geschetst van de technieken "als techniek" en van de verschillende resultaten en doelen waarvoor die technieken ingezet kunnen worden.

Voor de leermiddelenketen, zijn met name de doelen van dataminimalisatie en het vermijden van risico's bij het gebruik van bepaalde technieken van belang. Zoals al is aangegeven, dient het ketenpseudoniem binnen de leermiddelenketen met de scholen als Wbp-verantwoordelijken en de distributeurs en uitgevers van leermiddelen in de rol van Wbp-bewerker niet te leiden tot het eindresultaat dat er geen sprake meer is van persoonsgegevens. Wel kan door gebruik van het ketenpseudoniem bewerkstelligd worden dat de herleidbaarheid en de mogelijkheden voor distributeurs en uitgevers van leermiddelen om leerlingen en docenten te identificeren, (beduidend) verminderd worden. Bij eventuele meer zelfstandige doelen van uitgevers - waarbij gegevens van het gebruik van leermiddelen als basis gebruikt worden voor bijvoorbeeld verbetering van de leermiddelen - kan het te bereiken resultaat waarbij er geen sprake meer is van persoonsgegevens, weer wel een rol spelen. Hierbij wordt in het Privacy Convenant gesproken over

‘anonimiseren’ als begrip om het te bereiken resultaat aan te duiden.

Binnen de leermiddelenketen kan pseudonimiseren als techniek een bijdrage leveren aan dataminimalisatie en aan het vermijden van risico’s. Encryptie kan een bijdrage leveren aan informatiebeveiliging. Anonimiseren speelt als techniek wat meer indirect een rol omdat de thans gebruikte datasets met direct identificerende gegevens (zoals NAW-gegevens), vervangen worden door het ketenpseudoniem. Binnen de leermiddelenketen spelen deze technieken met name ten aanzien van de gegevensverwerkingen die door de diverse Wbp-bewerkers uitgevoerd worden voor de scholen als Wbp-verantwoordelijken.

		Technieken			
		anonimiseren	encryptie (versleutelen)	aggregeren	pseudonimiseren (hashen)
		Verminderen van de gedetailleerd-heid van de gegevens	Onleesbaar maken voor anderen dan de directe gebruikers	Samen-voegen van gegevens over meerdere personen	Vervangen van (direct identificerende) persoonsgegevens door een code / nummer (versluieren identiteit)
Resultaat	*Doel/ redenen gebruik technieken*				
Geen persoonsgegevens meer (niet meer herleidbaar)	Vermijden of ontlopen van de toepasselijkheid van privacywetgeving	X		X	X (2 maal)
	Geen noodzaak van persoonsgegevens voor het specifieke doel	X		X	X (2 maal)
(nog steeds) Persoonsgegevens	Dataminimalisatie	X			X (ten minste 1 maal)
	Vermijden van risico’s (informatiebeveiliging, aansprakelijkheid of sancties)	X	X		X (ten minste 1 maal)

Figuur 4: Binnen de leermiddelenketen te gebruiken technieken

B. Machtsverhouding tussen scholen en leermiddelendistributeurs en -uitgevers

Zoals in paragraaf 2.2 al is aangegeven, was er voorheen sprake van een scheve balans c.q. een scheve machtsverhouding tussen de scholen als Wbp-verantwoordelijken en de distributeurs en uitgevers van leermiddelen als Wbp-bewerkers. Het Privacy Convenant pakt deze onbalans aan en is daardoor essentieel om de Nummervoorziening en de voorziene pseudoniemen rechtmatig en in overeenstemming met de Wbp te kunnen gebruiken binnen de leermiddelenketen. Het gebruik van de ketenpseudoniemen kan een technische bijdrage leveren aan een juiste balans in de verhouding tussen scholen als Wbp-verantwoordelijken en uitgevers en distributeurs als bewerkers.

Omdat het Privacy Convenant en de bijbehorende bewerkersovereenkomst in deze PIA als essentiële voorwaarde gezien worden, achten wij het de moeite waard om, op termijn en indien het door het Convenant beoogde resultaat onvoldoende bereikt wordt, **in overweging te nemen om het Convenant en (in het bijzonder) de bewerkersovereenkomst van een nadere en aanvullende wettelijke basis te voorzien**. Hiermee kan bijvoorbeeld bereikt worden dat het in de praktijk niet (meer) nodig is dat alle scholen met alle distributeurs en uitgevers van leermiddelen afzonderlijke bewerkersovereenkomsten moeten sluiten. Een nadere wettelijke basis voor de bij het Convenant behorende bewerkersovereenkomst kan bewerkstelligen

dat er inderdaad sprake is van het volgens artikel 14 Wbp, lid 5, vereiste bewijs dat de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in artikel 13 schriftelijk of in een andere, gelijkwaardige vorm vastgelegd worden. Hiermee kan - naar aangenomen mag worden - een ondertekencircus van de bewerkersovereenkomsten vermeden worden.
Voor een dergelijke nadere wettelijke basis voor het Privacy Convenant en de bewerkersovereenkomst kan gedacht worden aan een drietal opties:

1. Het bij AmvB of ministeriële regeling vaststellen van bepalingen overeenkomstig het Privacy Convenant en de bewerkersovereenkomst. Dit lijkt niet de meest aantrekkelijke optie.
2. Het creëren van een wettelijke basis waarbij het Privacy Convenant en de bijbehorende bewerkersovereenkomst als gezamenlijk en wettelijk geregeld informatieprotocol vastgesteld kan worden. Een voorbeeld van een dergelijke optie is te vinden in artikel 7.5.4, lid 1 en lid 2, van het Besluit Jeugdwet waarin, kort gezegd, geregeld is dat bij ministeriële regeling nadere regels gesteld kunnen worden en dat die nadere regels kunnen bestaan uit het goedkeuren c.q. vaststellen van een door de veldpartijen opgesteld informatieprotocol. Zie in dit verband ook artikel 7 van de Regeling Jeugdwet waarin het in bijlage 2 opgenomen informatieprotocol als nadere regeling vastgesteld wordt.
3. Het creëren van een wettelijke basis waarbij het Privacy Convenant en de bijbehorende bewerkersovereenkomst op verzoek van partijen als gezamenlijk en wettelijk geregeld informatieprotocol vastgesteld kan worden. Een dergelijke optie is wel vergelijkbaar met de mogelijkheden die de Europese Privacyrichtlijn biedt voor de goedkeuring van modelcontracten voor de doorgifte van gegevens naar zogenaamde derde landen.

Zoals hiervoor in paragraaf 3.2 reeds is aangegeven, zijn **ook de beheerder van de Nummervoorziening en de beheerders van de inlogfaciliterende applicaties (SSO) aan te merken als Wbp-bewerkers voor de scholen**.
De verhouding tussen de scholen de beheerder van de Nummervoorziening en de beheerders van de SSO-applicaties vormen geen onderdeel van het Privacy Convenant voor de leermiddelenketen. Dat is ook verklaarbaar: die beheerders leveren of produceren geen leermiddelen, maar leveren en beheren meer generieke ICT-applicaties voor de scholen die de gegevensverwerking binnen verschillende ketens (kunnen) ondersteunen. Ook binnen het project voor de ontwikkeling van de Nummervoorziening is geen specifieke plaats ingeruimd om deze Wbp-verantwoordelijke – Wbp-bewerkers relaties te regelen. Het is duidelijk dat nadere aandacht wel noodzakelijk is.

In die zin wordt in deze PIA aanbevolen om nadere aandacht te besteden aan de relatie tussen de scholen als Wbp-verantwoordelijke en de beheerders van de generieke voorzieningen als Wbp-bewerkers. Voor een dergelijke regeling kan mogelijk aangesloten worden bij de reeds voorziene nadere regeling voor LAS/ LVS-leveranciers (het voorziene convenant voor schooladministratiesystemen) en bij afspraken in verband met beheer van de leerlingenadministratiesystemen en/ of de leerlingvolgsystemen.

C. De basis voor het te gebruiken ketenpseudoniem
Bj het ontwerp van de Nummervoorziening wordt voorgesteld om het PGN (in de praktijk veelal het BSN) van de leerlingen te gebruiken als het nummerelement uit de basis voor het ketenpseudoniem. Dit naast een aanduiding van de sector en de keten. Voor docenten wordt geen specifieke voorkeur voor een bepaald nummer als basis uitgesproken. Verder is het gebruik van de pseudoniemen voor wat docenten betreft maar beperkt uitgewerkt.

In het kader van deze PIA passeren drie mogelijke bases voor het nummerelement van het ketenpseudoniem de revue:

1. De al bij wet geregelde nummers ter identificatie van een natuurlijk persoon, zoals het BSN/ PGN;
2. Andere, reeds vastgelegde gegevens zoals een leerlingnummer of een personeelsnummer;
3. Een zelf samen te stellen basis, bijvoorbeeld een combinatie voornaam en andere kenmerken.

Leerlingen
Het ketenpseudoniem is bij leerlingen nadrukkelijk ook bedoeld om een overstap naar een andere school binnen dezelfde keten te faciliteren, zodat leerlingen als ze naar een andere school gaan gebruik kunnen blijven maken van hun leermiddelen. Ook bij MBO-scholieren speelt dit in verband met de door de leerlingen zelf aangeschafte leermiddelen en licenties. Hierdoor komt het leerlingnummer (wat bij wijziging van school ook wijzigt) in feite niet (in eerste instantie) in aanmerking om als basis voor het ketenpseudoniem te fungeren. Slechts indien het PGN als basis zou dienen te worden afgewezen, komt eventueel gebruik van het leerlingnummer aan de orde.

Omdat een zelf samen te stellen basis, bijvoorbeeld een combinatie voornaam, achternaam en andere kenmerken een geheel nieuwe functie voor de leerlingenadministratiesystemen zou zijn en de uniciteit van nummers daarbij vooralsnog onvoldoende duidelijk is, komt in deze PIA voornamelijk het gebruik van het PGN als basis aan de orde. Ook hier geldt dat slechts indien het PGN als basis zou moeten worden afgewezen, het eventueel gebruik van een zelf samen te stellen nummer aan de orde komt.

In het kader van deze PIA komen we tot de conclusies dat:

1. het PGN/BSN het als eerst voor de hand liggende nummer is om als basis voor het ketenpseudoniem van leerlingen te gebruiken;
2. niet met zekerheid gesteld kan worden dat het PGN (juridisch gezien) inderdaad als basis gebruikt mag worden;
3. tegelijkertijd eveneens niet gesteld kan worden dat het PGN niet als basis gebruikt zou mogen worden;
4. er, gelet op de bestaande situatie, desalniettemin aanknopingspunten zijn op basis waarvan gebruik van het PGN verdedigbaar is.

We baseren deze conclusies op de volgende (juridische) overwegingen.

Het PGN is in het onderwijs in het bijzonder geïntroduceerd met een administratieve functie. Het gaat om het vastleggen van gegevens in de leerlingenadministratiesystemen en om het uitwisselen van gegevens met de rijksoverheid, de gemeente in het kader van de leerplichtwet en bij de in- en uitschrijving als een leerling naar een andere school gaat.

Verder kan het BSN door de school ook gebruikt worden in het verkeer met de leerling op wie het nummer betrekking heeft. Het is dit “verkeer met de leerling” dat een basis kan geven voor gebruik van het PGN als basis voor het ketenpseudoniem voor de leermiddelenketen. Strikt genomen gebruikt de leerling het ketenpseudoniem daarbij voor gegevensverwerkingen waar de school de Wbp-verantwoordelijke voor is. In die zin gebruikt de leerling het ketenpseudoniem tijdens communicatie met de school, althans tijdens communicatie bij gegevensverwerkingen waarvoor de school de Wbp-verantwoordelijke is. Ook heeft het ketenpseudoniem een functie bij het in- en uitschrijven naar een andere school binnen dezelfde sector, zodat de leermiddelen ter beschikking kunnen blijven staan van de leerling. In die zin is dit gebruik van het ketenpseudoniem wel vergelijkbaar met het gebruik van het PGN bij de in- en uitschrijving zelf en bijvoorbeeld het overleggen van het onderwijskundig rapport.
Voor zover aangenomen wordt dat deze argumenten over het gebruik van het PGN niet als voldoende solide juridische basis aangemerkt kunnen worden voor gebruik, kan aanvullende regelgeving gemaakt worden om een dergelijk gebruik juridisch te faciliteren. Vanuit het oogpunt van privacywetgeving en de vormgeving van het ketenpseudoniem, zien we in het kader van de PIA geen zwaarwegende bezwaren die aan dergelijke aanvullende regelgeving in de weg zouden staan.

Docenten
Voor de docenten valt de afweging voor het als basis te gebruiken nummer anders uit dan bij leerlingen. Het BSN van docenten waar scholen over beschikken, mogen de scholen enkel gebruiken ter uitvoering van de belastingwetgeving. Deze wetgeving biedt in feite geen aanknopingspunten om het BSN van docenten ook als basis voor het ketenpseudoniem te gebruiken. Om het BSN te kunnen gebruiken zou, kort gezegd, wetgeving nodig zijn waarmee in feite ook aan docenten een soort van PGN toegekend zou dienen te worden. In het kader van deze PIA zien we daartoe onvoldoende redenen.

Hierbij speelt vooral dat wij op grond van de documenten en de interviews concluderen dat er geen noodzaak is om als een docent naar een andere school gaat, het ketenpseudoniem mee te nemen. Voor wat docenten betreft is het ketenpseudoniem immers direct gekoppeld aan de school als werkgever en kan bij wijziging van werkgever een nieuw ketenpseudoniem toegekend worden. Dit leidt ertoe dat het personeelsnummer de aangewezen basis lijkt voor het ketenpseudoniem. Het personeelsnummer behoort tot de relatie van werknemer (docent) en werkgever (school) en kan ook gebruikt worden voor het ter beschikking stellen van bedrijfsmiddelen, zoals leermiddelen die de docent als docent gebruikt.

We komen in het kader van de PIA tot de conclusie dat het personeelsnummer het (eerst) aangewezen nummer is om als basis voor het ketenpseudoniem van docenten te gebruiken. Een aandachtspunt is dan wel of het personeelsnummer voldoende uniek is om als basis bij het ketenpseudoniem te gebruiken. Het is niet onvoorstelbaar dat er meerdere docenten binnen een sector zijn die eenzelfde personeelsnummer hebben. Hierbij valt het te overwegen om naast het personeelsnummer tevens een toevoeging voor de desbetreffende school, bijvoorbeeld het BRIN, te gebruiken. De Nummervoorziening kan dan het personeelsnummer met de toevoeging per school, samen met de sectoraanduiding en een aanduiding voor de keten, gebruiken als basis voor het ketenpseudoniem.

4. Risicobeoordeling

4.1 Privacyrisico's

In onderstaande tabel wordt een overzicht gegeven van de privacyrisico's en de mate waarin de Nummervoorziening en het Privacy Convenant deze risico's adresseren. In de paragrafen 4.1.1 en in het bijzonder 4.2.2 wordt nader op de risico's ingegaan.

Risico	Mate waarin de Nummervoorziening het risico verkleint of wegneemt	Mate waarin het convenant het risico verkleint of wegneemt
1.Verspreiding van direct identificerende gegevens over/ binnen de leermiddelenketen, waardoor: - gegevensverwerking juridisch niet meer rechtmatig is (want bovenmatige verwerking); - gegevensverwerking als onnodig of onwenselijk wordt ervaren.	Door het ketenpseudoniem wordt dit risico (grotendeels) weggenomen. Dit door het vervangen van de huidige diverse datasets door het ketenpseudoniem.	Het Privacy Convenant leidt op zich niet tot minder verspreiding van gegevens, maar geeft wel een nader kader voor het rechtmatig gebruik van persoonsgegevens.
Conclusie m.b.t. risico 1: het risico wordt adequaat aangepakt		
2.Distributeurs en uitgevers verwerken gegevens (als bewerker) op een manier die zich aan het zicht van scholen onttrekt ofwel waar de scholen zich niet (volledig) bewust van zijn, waardoor: - scholen hun rol als Wbp-verantwoordelijke niet meer kunnen waarmaken; - de distributeur of uitgever in juridische zin Wbp-verantwoordelijke wordt; - gegevensverwerking juridisch niet meer toelaatbaar is.	Door het ketenpseudoniem wordt het verwerken van direct identificerende gegevens verminderd en wordt een duidelijkere identificator en gebruik van die identificator gerealiseerd.	Het Privacy Convenant met de bijbehorende bewerkersovereenkomst dekt dit risico af.
Conclusie m.b.t. risico 2: het risico wordt adequaat aangepakt		
3.Distributeurs en uitgevers gebruiken de gegevens - waarover zij in het kader van hun rol in de leermiddelenketen beschikken - voor	Het ketenpseudoniem dekt dit risico ten dele af omdat met de introductie van het ketenpseudoniem – in ieder geval	Het Convenant met de bijbehorende bewerkersovereenkomst adresseert dit risico ten dele

de eigen bedrijfsvoering en/ of voor commerciële benadering van leerlingen of ouders, waardoor: - de gegevensverwerking juridisch niet meer rechtmatig is; - de gegevensverwerking als onnodig of onwenselijk wordt ervaren.	in theorie - een distributeur niet beschikt over resultaten van leerlingen en een leverancier niet beschikt over NAW-gegevens van bestellers en afleveradressen.	door een bepaling over hergebruik te formuleren en daarbij anonimiseren (als resultaat) verplicht te stellen.
Conclusie m.b.t. risico 3: het risico wordt ten dele aangepakt en nadere maatregelen worden hieronder voorgesteld		
4.Rechtmatigheidsproblemen die ontstaan doordat het gebruik van nummers breder is dan met betrekking tot persoons-identificerende nummers binnen de wet is toegestaan.	Het ketenpseudoniem is zelf geen bij wet ingesteld identificerend nummer. Indien bij leerlingen het PGN als een van de elementen voor de basis van het ketenpseudoniem gebruikt wordt, is mogelijk aanvullende regelgeving nodig.	Het Convenant geeft een nader kader voor het rechtmatig gebruik van persoonsgegevens, waardoor breder gebruik als (duidelijk) onrechtmatig gezien (kunnen) worden.
Conclusie m.b.t. risico 4: het risico wordt deels aangepakt. In onderdeel C van paragraaf 3.3.4 is reeds ingegaan op eventuele aanvullende regelgeving voor gebruik van het PGN van leerlingen als basis voor het ketenpseudoniem		
5.Gegevenssets die op basis van verschillende doelen zijn verkregen worden op basis van het ketenpseudoniem aan elkaar gekoppeld waardoor een grotere gegevensset ontstaat (koppelingsrisico, ook bij eventuele datalekken). Dit risico kan optreden als: A. Partijen gegevenssets – waarover zij in het kader van hun rol in de leermiddelenketen beschikken – al beschikken. Bijvoorbeeld als een distributeur en een uitgever hun gegevenssets op basis van het ketenpseudoniem koppelen. B. Een partij gegevenssets illegaal bemachtigd door meerdere systemen te kraken (‘hacken’) en deze gegevenssets op basis van het ketenpseudoniem koppelt tot een grotere dataset.	**5A:** Het risico wordt met de introductie van het ketenpseudoniem niet groter of kleiner dan in de huidige situatie: distributeurs en uitgevers hebben een unieke identificator voor een leerling nodig om een door een leerling bij de distributeur besteld elektronisch leermiddel, door de uitgever aan diezelfde leerling beschikbaar te laten stellen. De enige manier waarop het risico eventueel technisch verkleind kan worden is om pseudoniemen die bestaan uit verschillende en afzonderlijke geencrypte delen, toe te passen. De bijdrage van dergelijke pseudoniemen als maatregel voor dit risico is echter gering omdat partijen dan op basis van het Convenant ook al onrechtmatig handelen. **5B:** het risico dat een hacker	**5A:** Het Convenant geeft een nader kader voor het rechtmatig gebruik van persoonsgegevens, waardoor dergelijke koppelingen als (duidelijk) onrechtmatig gezien (kunnen) worden. **5B:** het Convenant ziet niet op dit risico anders dan dat het adequate beveiliging voorschrijft.

	meerdere systemen kan kraken neemt met de introductie van het ketenpseudoniem niet toe of af. Als een hacker een of meerdere leerlingenadministratiesystemen kraakt speelt er een groter privacy-issue. Als een hacker het gemunt heeft op systemen van uitgevers of distributeurs is de gevoeligheid van te bemachtigen data met de introductie van het ketenpseudoniem wel afgenomen omdat - in ieder geval in theorie - een distributeur niet beschikt over resultaten van leerlingen en een uitgever niet beschikt over NAW-gegevens van bestellers en afleveradressen. Een hacker zal dus systemen van distributeurs èn van uitgevers moeten kraken om resultaten van leerlingen te koppelen aan NAW-gegevens (besteller en/ of afleveradres).	
Conclusie m.b.t. risico 5: het risico 5A wordt grotendeels aangepakt. Voor 5A en 5B hieronder worden enkele nadere maatregelen voorgesteld.		
6.Resultaten van leerlingen worden gebruikt als personeelsvolgsysteem van de docent.	De Nummervoorziening speelt hierbij geen rol. Het risico van een personeelsvolgsysteem is een risico van de elektronische leeromgeving zelf en niet van de Nummervoorziening	Het Convenant regelt niets over de verwerking van persoonsgegevens van docenten. Dit is mogelijk een lacune in het Convenant
Conclusie m.b.t. risico 6: het risico speelt niet bij de Nummervoorziening. Voor het overige valt het fungeren van leermiddelensystemen als personeelsvolgsystemen voor docenten buiten de scope van de PIA.		

4.1.1 Privacyrisico's voor leerlingen en docenten

Privacyrisico's die binnen de leermiddelenketen een rol spelen zijn, naast risico's in verband met de regelgeving over het verwerken van persoonsgegevens (onrechtmatigheid) vooral:

- de verspreiding van direct identificerende gegevens binnen c.q over de leermiddelenketen;
- de in de praktijk vrij zelfstandige positie van distributeurs en uitgevers en (mogelijke) gegevensverwerkingen door die partijen die zich aan het zicht van de scholen onttrekken dan wel

waar de scholen zich niet (volledig) bewust van zijn;
- de mogelijkheid dat distributeurs en uitgevers de gegevens waarover zij in het kader van hun rol in de leermiddelenketen beschikken, zouden (gaan) gebruiken voor de eigen bedrijfsvoering en zouden (gaan) gebruiken voor commerciële benadering van leerlingen of ouders.

In de Nummervoorziening en vooral in de leermiddelensystemen zelf (de school als Wbp-verantwoordelijke) worden ook gegevens over docenten verwerkt. Het personeelsnummer wordt omgezet in een pseudoniem bij de Nummervoorziening en in de leermiddelensystemen kunnen allerlei gegevens over docenten staan, bijvoorbeeld welke resultaten de leerlingen bij docenten behalen etc. Dit leidt ertoe dat voor wat docenten betreft leermiddelensystemen als personeelsvolgsysteem kunnen fungeren en dat de Wet op de Ondernemingsraden daarbij specifieke voorwaarden kent, waaronder de toestemming van de ondernemingsraad. Zie voor deze aspecten Bijlage D over de Wet op de Ondernemingsraden.
De Nummervoorziening zelf fungeert niet als een (eventueel) personeelsvolgsysteem, waardoor de Nummervoorziening zelf niet onder het instemmingsrecht valt. Dit aspect van leermiddelensystemen die t.a.v. docenten als personeelsvolgsysteem kunnen fungeren, valt verder buiten het bereik van deze PIA gericht op de Nummervoorziening.

4.1.2 Privacyrisico's van nummers

Hét privacyrisico van nummers is de mogelijkheid om eenvoudig gegevens over een persoon terug te kunnen vinden in verschillende bestanden en om eenvoudig gegevens uit verschillende bestanden te kunnen koppelen en te kunnen samenvoegen. Deze koppelings- en samenvoegpotentie is van oudsher het privacyrisico bij nummers. Uiteraard hangt dit risico af van de mate waarin een bepaald nummer bij verschillende organisaties en in verschillende bestanden gebruikt wordt. Een specifiek klantnummer van één enkel bedrijf heeft het risico niet of nauwelijks. Het is ook vanwege het ontbreken van het risico bij dergelijke specifieke nummers voor één enkel bestand of voor één enkele verantwoordelijke dat dergelijke nummers (mits ze informatieloos zijn) gebruikt kunnen worden bij gegevensverwerkingen die in het Vrijstellingsbesluit Wbp van melding vrijgesteld zijn.
Een algemeen nummer, zoals het BSN met het brede verplichte gebruik daarvan binnen de overheid, zorg en onderwijs leidt juist weer wel tot het koppelingsrisico. Het is dit koppelingsrisico van algemene nummers waarom de Wbp - in navolging van de Europese Privacyrichtlijn - in artikel 24 specifieke regels geeft over het gebruik van dergelijke algemene bij wet voorgeschreven persoonsnummers. Daarbij worden deze algemene persoonsnummers aangemerkt als bijzondere gegevens. Ook artikel 31 Wbp over het voorafgaand onderzoek is een bepaling in het licht van dit koppelingsrisico als eerder lokale nummers gebruikt worden voor andere doelen en om gegevens uit te wisselen met andere partijen.

Naast de algemene bij wet toegekende persoonsnummers, worden ook de 'gevoelige gegevens' data van artikel 16 Wbp aangemerkt als bijzondere persoonsgegevens. De redenen om van gevoelige gegevens te spreken zijn verbonden met de inhoud en de inhoudelijke betekenis van de gegevens zelf. Bij de gegevens die als gevoelige gegevens opgesomd worden in artikel 16 Wbp speelt het risico van stigmatisering of discriminatie juist een rol.

Bovenstaande geeft aan dat er zeer verschillende redenen zijn om aan de ene kant de gevoelige gegevens en aan de andere kant algemene persoonsnummers aan te merken als bijzondere gegevens.

In de discussie over het gebruik van nummers en ook in de regeling van het Vrijstellingsbesluit Wbp speelt de ‘informatieloosheid’ van een nummer een rol. De algemene norm is dat nummers geen inhoudelijke informatie zouden dienen te bevatten zoals bijvoorbeeld de geboortedatum (voorheen was de geboortedatum vaak onderdeel van bijvoorbeeld personeelsnummers). Het is duidelijk dat inhoudelijke informatie in een nummer zelf het koppelingsrisico vergroot. Gegevens over een bepaalde persoon kunnen dan niet enkel gekoppeld worden met gegevens in andere bestanden waar hetzelfde nummer gebruikt wordt, maar kunnen ook (nog eens) gekoppeld worden met gegevensbestanden die weliswaar niet hetzelfde nummer bevatten, maar wel dezelfde gegevens als de ‘inhoud’ van het nummer.
Het zou echter een groot misverstand zijn om vanwege het feit dat een nummer informatieloos is, te concluderen dat daardoor (die informatieloosheid) aan dat nummer geen (extra) privacyrisico’s meer verbonden zijn. Immers, het koppelingsrisico is bij informatieloze nummers nog steeds en volop aanwezig. Het koppelingsrisico houdt immers direct verband met het feit dat een nummer gebruikt wordt en is niet afhankelijk van hoe het nummer dan precies is opgebouwd c.q. de inhoud van het nummer. Wat sterk gezegd, zou men zelfs kunnen stellen dat het argument dat een nummer informatieloos is weliswaar een aspect van dataminimalisatie betreft, maar geen enkel (of nauwelijks) gewicht in de schaal legt ten aanzien van het aan nummers inherent verbonden koppelingsrisico. Anders gezegd: het argument over informatieloosheid van nummers ziet meer op de privacydiscussie over gevoelige gegevens van artikel 16 Wbp en hun stigmatiseringsrisico, dan dat het betrekking heeft op het koppelingsrisico van nummers. In die zin lijkt de informatieloosheid als argument dat er bij nummers geen privacyprobleem (meer) is, een argument ‘op de verkeerde plaats’.

Het bovenstaande geldt, mutatis mutandis, ook als in plaats van bijvoorbeeld een algemeen nummer zoals het BSN, pseudo-identiteiten toegekend worden om het BSN “onzichtbaar” te maken c.q. te versleutelen. Ook daarbij kan het gaan om pseudo-identiteiten met een algemeen gebruik (alhoewel dit niet direct voor de hand lijkt te liggen), pseudo-identiteiten voor een bepaalde sector of een lokale pseudo-identiteit voor een specifieke organisatie.

4.2 Risico’s en maatregelen afgezet tegen de Nummervoorziening

Uitgaande van de in paragraaf 4.1 opgesomde risico’s, wordt in onderstaande tabel voor de verschillende risico’s afzonderlijk aangegeven of en zo ja, welke maatregelen mogelijk zijn.

Risico	Mogelijke maatregelen
1.Verspreiding van direct identificerende gegevens over/ binnen de leermiddelenketen, waardoor: - gegevensverwerking juridisch niet meer rechtmatig is (want bovenmatige verwerking); - gegevensverwerking als onnodig of onwenselijk wordt ervaren.	Er worden (naast de voorziene Nummervoorziening en de pseudoniemen) geen nadere maatregelen voorgesteld.
2.Distributeurs en uitgevers verwerken gegevens (als bewerker) op een manier die zich aan het zicht van scholen onttrekt ofwel waar de scholen zich niet (volledig) bewust van zijn waardoor: - scholen hun rol als Wbp-verantwoordelijke niet	Er worden (naast de voorziene Nummervoorziening en de pseudoniemen) geen nadere maatregelen voorgesteld.

meer kunnen waarmaken; - de distributeur of uitgever in juridische zin Wbp-verantwoordelijke wordt; - gegevensverwerking juridisch niet meer toelaatbaar is.	
3.Distributeurs en uitgevers gebruiken de gegevens - waarover zij in het kader van hun rol in de leermiddelenketen beschikken - voor de eigen bedrijfsvoering en/ of voor commerciële benadering van leerlingen of ouders, waardoor: - de gegevensverwerking juridisch niet meer rechtmatig is; - de gegevensverwerking als onnodig of onwenselijk wordt ervaren.	Als eerste maatregel wordt een voorafgaand akkoord van de school bij hergebruik voorgesteld omdat het gaat om hergebruik van gegevens door een bewerker. Daarnaast zal er in de praktijk ook en vooral aandacht dienen te zijn voor de vraag of en welk hergebruik inderdaad rechtmatig en toelaatbaar is (zie ook de toelichting hieronder)
4.Rechtmatigheidsproblemen die ontstaan doordat het gebruik van nummers breder is dan met betrekking tot persoons-identificerende nummers binnen de wet is toegestaan.	Voorstelbaar is dat aanvullende regelgeving wordt gemaakt om duidelijk aan te geven dat het PGN als basis voor het ketenpseudoniem gebruikt mag worden. Zie hiervoor onderdeel C van paragraaf 3.3.4
5.Gegevenssets die op basis van verschillende doelen zijn verkregen worden op basis van het ketenpseudoniem aan elkaar gekoppeld waardoor een grotere gegevensset ontstaat (koppelingsrisico, ook bij eventuele datalekken).	Als maatregel wordt datascheiding tussen de gegevens van distributeurs en uitgevers voorgesteld. Verder wordt encryptie van het ketenpseudoniem (en het PGN) in vooral de systemen van de scholen (LAS etc.) voorgesteld (zie ook de toelichting hieronder)
6.Resultaten van leerlingen worden gebruikt als personeelsvolgsysteem van de docent.	Er worden in het kader van deze PIA geen nadere maatregelen voorgesteld

Toelichting maatregel bij risico 3
Deze maatregelen zien op het risico dat distributeurs en uitgevers gegevens - waarover zij in het kader van hun rol als Wbp-bewerker in de leermiddelenketen beschikken - gebruiken of hergebruiken voor de eigen bedrijfsvoering en / of voor commerciële benadering van leerlingen of ouders,

Het is voorstelbaar en op voorhand niet geheel af te wijzen of als onrechtmatig te bestempelen dat in het bijzonder uitgevers gegevens die ze als Wbp-bewerker beheren, willen en ook kunnen gebruiken voor mogelijke productverbetering of productontwikkeling. Gelet op de bestaande verhouding met de scholen als Wbp-verantwoordelijke en de uitgevers als bewerkers, zal daarvoor in alle gevallen - en als eerste per voorzien hergebruik - het akkoord van de school als Wbp-verantwoordelijke nodig zijn. Zo behouden de scholen de regie over het gewenste hergebruik. De achtergrond van deze accordering door de scholen is dat een bewerker gegevens zonder een dergelijk akkoord van de Wbp-verantwoordelijke eenvoudigweg niet voor eigen doeleinden mag aanwenden.
Een dergelijk akkoord van de school als Wbp-verantwoordelijke voor hergebruik door de bewerker voor eigen doeleinden, geeft echter nog geenszins aan of en onder welke voorwaarden een dergelijk hergebruik ook inderdaad rechtmatig en toelaatbaar is. Dat zal ook – en vooral - bezien dienen te worden. Uiteraard is duidelijk dat als blijkt dat het voorziene hergebruik niet rechtmatig is, de school in de rol van Wbp-verantwoordelijke ook geen akkoord zal geven voor hergebruik.

Voorstelbaar is dat bij de beoordeling van de rechtmatigheid van hergebruik een verdergaande bewerking van gegevens plaats zal dienen te vinden zoals bijvoorbeeld een nieuwe pseudonimisering, zo mogelijk door een derde partij (*Trusted Third Party*), van het ketenpseudoniem waardoor bereikt zou kunnen worden dat er sprake is van anonimiseren zoals in het Privacy Convenant is aangegeven. Zie hierbij ook onderdeel A van paragraaf 3.3.4 en onderdeel 4 van Bijlage C.

Toelichting maatregelen bij risico 5
Deze maatregelen zien op het risico dat gegevenssets die op basis van verschillende doelen door de distributeurs en uitgevers van leermiddelen zijn verkregen, op basis van het ketenpseudoniem aan elkaar gekoppeld waardoor een grotere gegevensset ontstaat.

Om het koppelingsrisico verder te vermijden, wordt aanbevolen dat als maatregel ingevoerd wordt dat er datascheiding aanwezig is tussen de gegevens van distributeurs en die van uitgevers. Dit met name om te voorkomen dat distributeurs de beschikking zouden (kunnen) krijgen over gegevens van leerlingen en hun resultaten bij het gebruik van leermiddelen. Een dergelijke scheiding vloeit overigens ook al voort uit het Privacy Convenant en de bijbehorende bewerkersovereenkomst.
Daarnaast wordt aanbevolen dat bij gegevensbestanden die distributeurs gebruiken een scheiding (een zogenaamde Chinese muur) aangebracht wordt tussen enerzijds het ketenpseudoniem en anderzijds NAW-gegevens betreffende de aflevering en betaling van leermiddelen. Deze scheiding kan doorgevoerd worden zodra de aflevering en de betaling van de leermiddelen hebben plaatsgevonden.

Voor wat informatiebeveiliging en eventuele datalekken betreft, wordt, weliswaar ter afsluiting van de PIA maar wel degelijk essentieel, aanbevolen om het ketenpseudoniem en het PGN op geëncrypte wijze vast te leggen in de systemen van de scholen en met name in de leerlingenadministratiesystemen en andere systemen waarin zowel het PGN, personalia en het ketenpseudoniem vastgelegd zijn. Een dergelijke beveiligingsmaatregel past bijvoorbeeld bij de inmiddels gebruikelijke handelwijze dat ook gebruikersnamen en wachtwoorden geëncrypt vastgelegd worden.

Bovenstaande risicoanalyse vormt geen basis om de voorlopige conclusie die ten aanzien van de reikwijdte van het ketenpseudoniem (paragraaf 3.3.3) werd getrokken, te herzien. Dit, gelet op de in die paragraaf gedane aanbeveling om aandacht te schenken aan de relatie met de reeds geregelde overdracht van gegevens zoals het onderwijskundig rapport en overstap service onderwijs.

In de risicoanalyse worden zes privacyrisico's geduid. Bij twee van deze risico's wordt het risico al (middels de Nummervoorziening, het ketenpseudoniemen en/ of het Privacy Convenant) adequaat aangepakt.
Van één risico (resultaten van leerlingen worden gebruikt als personeelsvolgsysteem van docent) wordt geconcludeerd dat het risico niet speelt bij de Nummervoorziening.
Voor de overige drie risico's worden aanvullende maatregelen voorgesteld.
Deze mogelijke maatregelen zijn:

- Voorafgaand akkoord van de school bij hergebruik van gegevens door distributeurs en uitgevers. Daarnaast zal er in de praktijk ook en vooral aandacht dienen te zijn voor de vraag of en welk hergebruik inderdaad rechtmatig en toelaatbaar is.
- 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

ketenpseudoniem aan elkaar worden gekoppeld waardoor een grotere gegevensset ontstaat (koppelingsrisico, ook bij eventuele datalekken).

- Datascheiding bij gegevensbestanden die distributeurs gebruiken tussen enerzijds het ketenpseudoniem en anderzijds NAW-gegevens betreffende de aflevering en betaling van leermiddelen. Deze scheiding kan doorgevoerd worden zodra de aflevering en de betaling van de leermiddelen hebben plaatsgevonden .
- Encryptie van het ketenpseudoniem (en het PGN) in vooral de systemen van de scholen (LAS etc.).

Verder achten wij het voorstelbaar dat aanvullende regelgeving wordt gemaakt om duidelijk aan te geven dat het PGN als basis voor het ketenpseudoniem gebruikt mag worden.

Bijlage A Beschrijving Privacy Impact Assessment

Een PIA kan worden omschreven als een hulpmiddel bij het inschatten van privacyrisico's bij wetgeving en bij ICT- projecten. Een PIA dient om tijdig inzicht te krijgen wat de gevolgen en risico's van wetgeving, een project of activiteit kunnen zijn, vooral voor wat betreft inbreuken op de persoonlijke levenssfeer. Daarbij worden ook aanbevelingen meegenomen voor het treffen van maatregelen om de geconstateerde risico's af te wenden. Met de aanbevelingen en maatregelen richt de PIA zich ook op privacybeleid. Uiteindelijk moet de PIA inzicht geven in hoeverre en onder welke voorwaarden het project, eventueel met aanvullende maatregelen, doorgang kan vinden. Een PIA draagt daarmee bij aan het vermijden of verminderen van privacyrisico's. Een impact assessment (effectbeoordeling) wordt door de International Association for Impact Assessment (IAIA) wat formeel omschreven als "de identificatie van toekomstige gevolgen van een huidige of voorgestelde actie". Naast de mogelijkheid om een PIA te voeren, zijn er diverse andere privacyhulpmiddelen beschikbaar om de privacyaspecten van gegevensverwerkingen te beoordelen. Veel van deze middelen zijn direct op de toetsing van de naleving van de wettelijke eisen gericht.
Een PIA verschilt van deze hulpmiddelen omdat het zich niet beperkt tot de vraag of de activiteiten en verwerkingen bij wet zijn toegestaan, maar ook hoe het vraagstuk bijvoorbeeld maatschappelijk wordt ervaren. Het beperkt zich daarbij niet alleen tot dataprotectie wet en regelgeving, maar richt zich ook breder op percepties van privacy, en de uitgangspunten van dataprotectie. Een PIA kan zich ook richten ook op de vraag of de organisatie in staat is om eventuele tekortkomingen te signaleren, en er bereidheid is om de maatregelen te treffen die het risico kunnen afwenden ('in control').

Een PIA toetst, kort gezegd, óf de voorziene gegevensverwerking inderdaad doorgang dient te vinden, welke gegevensverwerkingen dan noodzakelijk zijn en vervolgens hoe deze gegevensverwerkingen plaats mogen vinden.

Een PIA kan op verschillende momenten uitgevoerd worden. Bijvoorbeeld voorafgaande aan het treffen van regelgeving, voorafgaande aan de ontwikkeling van ICT-projecten of op het moment dat regelgeving of ICT-projecten een nieuwe fase in gaan. In bepaalde gevallen kan een PIA de nadruk hebben op privacy by design, in andere gevallen kan er meer nadruk zijn op compliance-achtige aspecten. Het onderscheid tussen een vroegtijdige risicogeoriënteerde PIA en compliance is echter vaak lastig aan te brengen. De verwevenheid van een risicobeoordeling, privacy by design en compliance-achtige aspecten kwam ook naar voor in het advies van het College bescherming persoonsgegevens van 5 maart 2013 over het Toetsmodel PIA Rijksdienst (z2012-00847).

De benodigde flexibiliteit bij de uitvoering van een PIA houdt in dat een PIA iedere keer maatwerk is. Een bijzonderheid bij de PIA Tijdschrijven is de rol van de Ondernemingsraad. Het gaat om regelingen van de werkgever over het verwerken van personeelsgegevens en om een personeelsvolgsysteem.

Het ontstaan en de ontwikkeling van de PIA

De PIA als instrument is oorspronkelijk tot ontwikkeling gekomen in landen met een Angelsaksisch georiënteerd rechtssysteem. Zo verschenen er rond 2005 modellen en beschrijvingen voor een PIA van de hand van de Canadese, de Britse en de Australische privacytoezichthouders. Ook de federale overheid van de

Verenigde Staten kwam in die periode met een model en procedure voor het uitvoeren van een PIA. De PIA was daarbij verbonden met het eerder door o.a. de Nederlandse privacytoezichthouder ontwikkelde uitgangspunt van “Privacy Enhancing Technologies” en met het in bijvoorbeeld artikel 13 van de Wet bescherming persoonsgegevens wat impliciet opgenomen uitgangspunt van privacy by design.

Belangrijke ontwikkelingen in Nederland bij de ontwikkeling van een PIA zijn de motie Franken van 17 mei 2011 over het uitvoeren van een PIA in het kader van wetgeving (EK, 31 051, nr. D) en bijvoorbeeld de motie Elissen en Gesthuizen van 13 oktober 2011 over privacy by design en safety by design bij de ontwikkeling van nieuwe ICT-projecten (TK, 26 643, nr. 203). De ontwikkeling en de uitvoering van een PIA kwam ook aan de orde in de Notitie Privacybeleid van het kabinet van 29 april 2011. Ook in het Regeerakkoord komt het uitvoeren van een PIA aan de orde.

In november 2011 was er in het kader van de I-strategie Rijk het besluit van het kabinet om de bestaande maatregelen ten aanzien van de beheersing van grote ICT-projecten van het Rijk uit te breiden met maatregelen ter bescherming van privacy. De reeds bestaande eisen ten aanzien van de inhoud van projectplannen voor grote ICT-projecten zijn daartoe aangevuld met de eis om in het projectplan informatie op te nemen of er bij het project sprake is van het opnemen van privacygevoelige gegevens en koppelingen of verrijking daarvan en om, zo nodig, een PIA uit te voeren.

Inmiddels is voor een PIA voor de Rijksdienst het Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst van 24 juni 2013 (Bijlage bij TK, 26 643, nr. 282) verschenen. Het Toetsmodel dient vanaf 1 september 2013 standaard te worden toegepast bij ontwikkeling van nieuwe wetgeving en beleid waarmee de bouw van nieuwe ICT-systemen of de aanleg van grote databestanden wordt voorzien.

Bijlage B Regeling gebruik Persoonsgebonden nummer (PGN)

Deze bijlage geeft het overzicht van de bepalingen die van toepassing zijn bij het gebruik van het Persoonsgebonden nummer (PGN).

Wet bescherming persoonsgegevens
De centrale bepaling over gebruik van bij wet toegekende nummers ter identificatie van een persoon is opgenomen in artikel 24 van de Wet bescherming persoonsgegevens.

1. 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.
2. Bij algemene maatregel van bestuur kunnen andere dan in het eerste lid bedoelde gevallen worden aangewezen waarin een daarbij aan te wijzen nummer als bedoeld in het eerste lid, kan worden gebruikt. Daarbij kunnen nadere regels worden gegeven over het gebruik van een zodanig nummer.

Onderwijswetgeving
De Wet op het primair onderwijs, de Wet op het voortgezet onderwijs, de Wet educatie en beroepsonderwijs en de Wet op de expertisecentra bevatten ieder een eigen regeling over het PGN en het gebruik van het PGN. De verschillende regelingen zijn, in ieder geval voor wat de leermiddelenketen betreft, inhoudelijk gelijk. Hieronder worden de specifieke bepalingen uit de Wet op het primair onderwijs (als voorbeeld) weer gegeven.

Artikel 1. Begripsbepalingen
persoonsgebonden nummer:
het burgerservicenummer, bedoeld in artikel 1, onder b, van de Wet algemene bepalingen burgerservicenummer, dan wel het door Onze minister uitgegeven onderwijsnummer, bedoeld in artikel 40b, vierde lid;

Artikel 40b. Te verstrekken gegevens bij toelating

1. Onverminderd bij algemene maatregel van bestuur gegeven voorschriften met betrekking tot de in- en uitschrijving van leerlingen, vindt toelating van een leerling als bedoeld in artikel 40 slechts plaats nadat de ouders de gegevens betreffende de geslachtsnaam, de voorletters, de geboortedatum, het geslacht en het persoonsgebonden nummer van de leerling hebben overgelegd. Indien de ouders aannemelijk maken dat zij geen persoonsgebonden nummer van de leerling kunnen overleggen, vindt de toelating plaats met inachtneming van het derde lid.

[…]

3. Indien de ouders aannemelijk maken dat zij geen persoonsgebonden nummer van de leerling kunnen overleggen, meldt het bevoegd gezag binnen twee weken na het besluit tot toelating aan Onze minister de beschikbare gegevens van de leerling, bedoeld in het eerste lid, alsmede zijn adres en woonplaats en, indien aanwezig, het leerlingenadministratienummer.
4. Onze minister verstrekt binnen acht weken na ontvangst van de melding, bedoeld in het derde lid, aan het bevoegd gezag het burgerservicenummer van de leerling, dan wel, indien is gebleken dat hem niet van overheidswege een burgerservicenummer is verstrekt, het onderwijsnummer van de leerling. Het

onderwijsnummer is een door Onze minister uitgegeven en aan de leerling toegekend persoonsgebonden nummer.

5. Het bevoegd gezag neemt de in het eerste en vierde lid bedoelde gegevens op in de leerlingenadministratie van de school. Bij ministeriële regeling kan worden bepaald welke andere gegevens in de leerlingenadministratie worden opgenomen.
6. Indien aan een leerling een onderwijsnummer is toegekend en het bevoegd gezag de beschikking krijgt over zijn burgerservicenummer, neemt het bevoegd gezag dit burgerservicenummer terstond als persoonsgebonden nummer op in de leerlingenadministratie van de school in de plaats van het onderwijsnummer. Het bevoegd gezag meldt deze wijziging binnen twee weken aan Onze minister onder opgave van het burgerservicenummer en het onderwijsnummer van de leerling.

Artikel 178a. Gebruik persoonsgebonden nummer door bevoegd gezag

1. Het bevoegd gezag kan het persoonsgebonden nummer van een leerling gebruiken in het verkeer met de leerling op wie het nummer betrekking heeft, of met de ouders van deze leerling.

In de andere onderwijswetgeving is, kort gezegd, geregeld dat het persoonsgebonden nummer alleen in verkeer met bijvoorbeeld ouders en voogden gebruikt wordt als de leerling minderjarig (of handelingsonbekwaam) is.

6. Het bevoegd gezag gebruikt het persoonsgebonden nummer van een leerling in het contact met een andere school of een school voor ander onderwijs ten behoeve van de in- en uitschrijving van die leerling en bij het overleggen van het onderwijskundig rapport, bedoeld in artikel 42.

Bijlage C Persoonsgegevens, datasets en soorten bestanden

1 Definitie Persoonsgegevens
Vaak wordt bedoeld of onbedoeld aangenomen dat vooral of enkel gegevens die een bepaalde persoon direct identificeren, persoonsgegevens zijn. De invulling van het begrip persoonsgegeven maakt echter dat vele gegevens al snel als persoonsgegevens moeten worden aangemerkt. Het is bij persoonsgegevens niet de vraag of een bepaald gegeven op zich een persoonsgegeven is, maar ook en meestal is het de vraag of een set van gegevens samen bezien persoonsgegevens kunnen opleveren. Kort gezegd is er vaak al sprake van persoonsgegevens volgens de privacywetgeving op een moment dat de persoon zelf nog niet bekend is, maar wel te achterhalen is wie de persoon zou zijn.
Zo zal er in het algemeen bij de omschrijving van “de bezitter van de rode sportauto” niet snel sprake zijn van persoonsgegevens. Maar als deze omschrijving bijvoorbeeld in een bericht zou staan over een voorval in een klein dorpje waar uitgerekend alleen de enige bakker een rode sportauto heeft, dan zal iedereen uit het dorp wel weten wie bedoeld wordt.

1.1 Definities in wet en regelgeving
Een ruime definitie van het begrip persoonsgegeven wordt op internationaal terrein gegeven in zowel artikel 2, onder a, van het Databeschermingsverdrag als in artikel 2, onder a, van de EU Privacyrichtlijn.

Databeschermingsverdrag
Het databeschermingsverdrag spreekt in artikel 2, onder a over: ‘personal data’ means any information relating to an identified or identifiable individual (‘data subject’).

EU Algemene Privacyrichtlijn
De Europese Algemene Privacyrichtlijn spreekt in artikel 2, onder a over: "persoonsgegevens", iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna "betrokkene" te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

De Wet bescherming persoonsgegevens
De Wet bescherming persoonsgegevens spreekt in artikel 1, onder a, over: 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.'

1.2 De elementen 'Relating to / betreffende' en 'identified or identifiable / geïdentificeerde of identificeerbare'
Bij persoonsgegevens gaat het volgens de genoemde definities om ‘iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’ De twee elementen 'iedere informatie betreffende' en 'geïdentificeerd of identificeerbare' staan hierbij centraal.

1.2.1 'Betreffende'
Bij de formulering 'iedere informatie betreffende' wordt bedoeld dat het om alle gegevens gaat die omtrent een bepaalde persoon informatie kunnen verschaffen. In veel gevallen, zoals bij gegevens over eigenschappen,

opvattingen of gedragingen, zal dit duidelijk zijn. In andere gevallen zal onder omstandigheden de context waarin het gegeven wordt vastgelegd en gebruikt bepalend zijn. Van belang is dan of het gegeven bepalend kan zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. Anders gezegd: het gaat over de wijze waarop de betrokkene aan het maatschappelijk leven deelneemt. Zo kunnen gegevens over een onderneming of over uitgaande telefoongesprekken persoonsgegeven zijn. Ook telefoonnummers en kentekens van auto's of soms zelfs perceelnummers kunnen persoonsgegeven zijn.

1.2.2 'Geïdentificeerde of identificeerbare'
Bij 'geïdentificeerde of identificeerbare' natuurlijke persoon speelt vooral de vraag of de identiteit van de persoon redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Twee factoren zijn hierbij vooral van belang:
1. de aard van de gegevens; en,
2. de mogelijkheden om de identificatie tot stand te brengen.

De aard van de gegevens
Een persoon is identificeerbaar indien sprake is van gegevens die alleen of in combinatie met andere gegevens, zo kenmerkend zijn voor een bepaalde persoon dat deze aan de hand daarvan kan worden geïdentificeerd. Niet ieder gegeven zal echter in dezelfde mate bijdragen tot de mogelijke identificering van een persoon. In dit kader kan een onderscheid worden gemaakt tussen direct en indirect identificerende gegevens.

Van direct identificerende gegevens is sprake wanneer gegevens betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig vast te stellen is. Voorbeelden zijn de gegevens-set van naam, adres en geboortedatum, die in combinatie met elkaar dermate uniek zijn voor een bepaalde persoon dat deze kan worden geïdentificeerd. Er zijn ook gegevens die zodanig uniek zijn dat ze direct identificerend zijn, zoals het BSN.

Bij indirect identificerende gegevens kunnen de gegevens (de set van gegevens) weliswaar niet rechtstreeks, maar wel via nadere stappen in verband gebracht worden met een bepaalde persoon. Zij kunnen, alhoewel er geen direct identificerende gegevens zijn, door combinatie met andere gegevens weer worden teruggebracht tot een bepaalde persoon. Bij indirect identificerende gegevens kan een onderscheid worden gemaakt tussen gegevens met een hoog onderscheidend karakter, zoals een datum, leeftijd, woonplaats en beroep en gegevens met een laag onderscheidend karakter, zoals leeftijdsklasse, woonregio en beroepsklasse. Het onderscheidend vermogen van dergelijke (combinaties van) gegevens is echter vooral afhankelijk van de context waarbinnen ze worden gebruikt. Ze zijn bijvoorbeeld afhankelijk van de omvang van de bevolkingsgroep waarop de gegevensverwerking betrekking heeft.

Vanwege de identificeerbaarheid van indirect identificerende gegevens, is het verwijderen van enkel de direct identificerende kenmerken op zichzelf geen voldoende garantie dat er geen sprake meer is van persoonsgegevens. Door middel van spontane herkenning, vergelijking van gegevens en/of koppeling aan gegevens uit andere bron, kan soms zonder bijzonder veel inspanning, identificatie tot stand worden gebracht.

De mogelijkheden om identificatie tot stand te brengen
Naast de aard van de gegevens moeten de mogelijkheden om identificatie tot stand te brengen worden meegewogen bij de vraag of sprake is van persoonsgegevens. Bij de afweging is een absolute maatstaf niet

aan de orde: gekeken moet worden naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om die persoon te identificeren.

2 Identificeerbaarheid
De Memorie van Toelichting bij de Wet bescherming persoonsgegevens (TK 25 892, nr. 3) bevat een aantal specifieke opmerkingen ten aanzien van het anonimiseren van gegevens (lees: de gegevensset ontdoen van direct identificerende gegevens en soms ook het weglaten van enkele indirect identificerende gegevens, in combinatie met aanvullende maatregelen zoals een geheimhoudingsplicht. De passage op p. 49-50 luidt:

> Een gegeven is geen persoonsgegeven indien doeltreffende maatregelen zijn getroffen waardoor een daadwerkelijke identificatie van individuele natuurlijke personen redelijkerwijs wordt uitgesloten. Deze maatregelen kunnen bijvoorbeeld zijn gegevenscodering in combinatie met nadere bewerkingen of bijzondere besluitvormingsprocedures. Een verantwoordelijke kan bij voorbeeld gegevens ontdoen van de direct identificerende gegevens en deze onderbrengen bij een derde dan wel een derde de sleutel geven die toegang geeft tot deze gegevens. De vraag of in een dergelijk geval al dan niet gesproken kan worden van persoonsgegevens is afhankelijk van de mate waarin medewerking van de betrokken derde verwacht mag worden. Indien bijvoorbeeld degene die de code heeft opgesteld is onderworpen aan een geheimhoudingsplicht die naar uit de praktijk is gebleken daadwerkelijk wordt gehandhaafd, kan in de regel ervan worden uitgegaan dat er onvoldoende feitelijke mogelijkheden zijn tot daadwerkelijke identificatie. Is de code echter zonder veel moeite of met eenvoudige omzeiling van waarborgen te verkrijgen door de verantwoordelijke, dan is er sprake van identificeerbaarheid en dus van persoonsgegevens in de zin van het wetsvoorstel. De feitelijke situatie, niet de juridische constructie, is bepalend voor de toepasselijkheid van het wetsvoorstel.

3 Drie typen datasets
Gebaseerd op de definitie van persoonsgegevens, kunnen drie categorieën van datasets onderscheiden worden.[5] Bij een dataset gaat het om verschillende gegevens over dezelfde persoon.

Categorie I datasets zijn de datasets waarin direct identificerende gegevens opgenomen zijn (bijv. het BSN of een combinatie van naam, geboortedatum en adres). De set zelf zijn (al) persoonsgegevens omdat de persoon in de dataset zelf ook geïdentificeerd is.

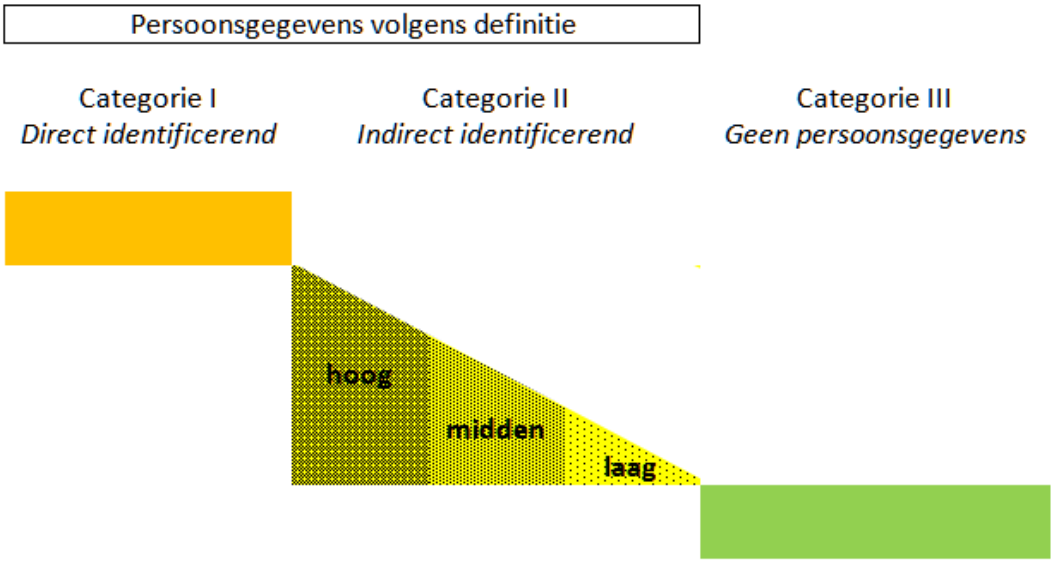
Categorie II datasets zijn de datasets waarin geen direct-identificerende gegevens zijn opgenomen of waaruit de direct identificerende gegevens verwijderd zijn. Soms zijn de direct identificerende gegevens vervangen door een "pseudo-identiteit". Door de combinatie van gegevens in de dataset is het echter vaak nog wel mogelijk om de identiteit, bijvoorbeeld door de combinatie met andere gegevens of het “kraken” van de pseudo-identiteit, te achterhalen. Er is nog steeds sprake van persoonsgegevens, waarbij de persoon

[5] De indeling is mede gebaseerd op het rapport "Privacywetgeving en het gebruik van persoonsgegevens voor wetenschappelijke doeleinden" van de Commissie Kordes uit 1997. In het rapport (bijlage 5) worden verschillende soorten bestanden onderscheiden (categorie I, II en III).

identificeerbaar is. Daarbij wordt dan gesproken over een dataset met indirect identificerende gegevens. De mate waarin de indirect identificerende gegevens de persoon identificeerbaar maken, kan daarbij sterk verschillen. Dit hangt geheel af van de gedetailleerdheid van de gegevens en ook over welke bestanden een organisatie beschikt om te gebruiken bij het alsnog identificeren van gegevens.

Categorie III datasets zijn de datasets die niet meer tot een persoon te herleiden zijn, ook niet met gebruik van andere bestanden of door het “kraken” van de pseudo-identiteit. Dit betekent dat bij dergelijke bestanden er twee keer en onafhankelijk van elkaar pseudo-identiteiten gemaakt worden en dat de gegevens die overblijven niet meer zo gedetailleerd mogen zijn dat identificeren toch nog mogelijk is. Bij deze sets is er geen sprake meer zijn van indirect identificerende gegevens en geen sprake van persoonsgegevens.

De drie categorieën van datasets zijn hieronder weergegeven. Bij de categorie II datasets met indirect identificerende gegevens is een verdeling gemaakt in ‘hoge’ identificeerbaarheid, ‘midden’ identificeerbaarheid en ‘lage’ identificeerbaarheid. In welke mate er sprake is van identificeerbaarheid hangt bij categorie II datasets altijd af van de omstandigheden (inhoud dataset en wie beschikt of kan beschikken over de dataset).



In de praktijk is het vaak vrij eenvoudig om van een categorie I dataset een categorie II dataset te maken. Het is echter beduidend lastiger om de dataset ‘eventjes’ om te zetten in een categorie III dataset waarbij er in het geheel geen sprake meer is van persoonsgegevens.

4 Drie soorten bestanden bij analyse en productontwikkeling of – productverbetering

Bij het gebruik van gegevens voor analysen en productontwikkeling of – productverbetering kunnen drie soorten bestanden onderscheiden te worden. Bestanden zijn de gegevensverzamelingen waarin de datasets over verschillende personen opgenomen zijn.

Als eerste zijn er de bestanden met de zogenaamde ruwe data. Dat zijn de bestanden die ten behoeve van

beleidsinformatie en statistiek ontvangen worden. In het algemeen zijn dit bestanden met categorie I datasets, soms ook met categorie II datasets. Vaak worden de bestanden met ruwe data niet (direct) voor de analyse of de statistische bewerkingen gebruikt.

Als tweede zijn er de zogenaamde onderzoeksbestanden. Dit zijn bestanden die daadwerkelijk voor de analyse of de productontwikkelen en –verbetering gebruikt worden. In het algemeen zijn onderzoeksbestanden het resultaat van enkele bewerkingen van de ruwe data om de ruwe data geschikt te maken voor analyse of statistische bewerkingen. De onderzoeksbestanden bestaan meestal uit categorie II datasets, waarbij er in plaats van de direct identificerende gegevens een “pseudo-identiteit” gebruikt wordt.

Als derde zijn er de resultaten. Vaak gaat het om cijfermatige overzichten en rapportages. Soms gaat het bij de resultaten om bestanden met categorie III datasets. Uitgangspunt (en ook juridisch vereiste) is dat de resultaten geen persoonsgegevens meer zijn.

Bijlage D Wet op de Ondernemingsraden

Binnen arbeidsverhoudingen is sprake van een zekere spanning tussen het recht van de werknemer op privacy en bescherming van de persoonlijke levenssfeer en het recht van de werkgever om gezag uit te oefenen door het werk te controleren, toezicht te houden en leiding te geven. Privacy op de werkplek kan in zeer uiteenlopende situaties aan de orde zijn. Binnen arbeidsverhoudingen kan men denken aan personeelsregistraties en de zogenaamde personeelsvolgsystemen.

De wet- en regelgeving waarin privacy van werknemers een onderwerp is, is zeer divers. Enkele voorbeelden zijn het Burgerlijk Wetboek, de Wet op de medische keuringen, de Arbeidsomstandighedenwet en de Wet op de ondernemingsraden (Wor).

Bij een organisatorische regeling en inbedding van de implementatie en naleving van de Wet bescherming persoonsgegevens is met name het instemmingsrecht van de Wet op de ondernemingsraden van belang. Hieronder komt dit instemmingsrecht kort aan de orde.

In 1998 is artikel 27 van de Wet op de ondernemingsraden aangevuld met de onderdelen k en l. Deze artikelonderdelen bepalen dat de instemming van de ondernemingsraad nodig is voor het vaststellen van regelingen omtrent:

k. de registratie van, de omgang met en de bescherming van persoonsgegevens van in de onderneming werkzame personen, en
l. een voorziening die gericht is op of geschikt is voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen (een personeelsvolgsysteem).

Personeelsregistraties:
Bij onderdeel k, bij personeelsregistraties, kan in eerste instantie gedacht worden aan het invoeren, wijzigen of afschaffen van een bepaalde personeelsadministratie, zoals het personeelsinformatiesysteem of een ziekteverzuimregistratie. De vaststelling van regelingen over dergelijke systemen en verwerkingen vallen onder deze bepaling. Daarvoor is dan ook instemming van de ondernemingsraad nodig.

Personeelsvolgsystemen:
Een personeelsvolgsysteem is zowel een systeem dat gericht is op het volgen van personeel (bijvoorbeeld een prikklok), als een systeem dat daarvoor geschikt is (bijvoorbeeld een videocamera of een systeem voor toegangspasjes). Het geschiktheidcriterium betekent dat ook voor een personeelsvolgsysteem dat (nog) niet als zodanig wordt gebruikt, maar daar (in de toekomst) wel de mogelijkheid toe zou kunnen bieden, de instemming nodig is van de ondernemingsraad. In het algemeen kan gesteld worden dat alle geautomatiseerde systemen op basis van dit geschiktheidscriterium zijn aan te merken als een personeelsvolgsysteem.
Het is een werkgever toegestaan zijn werknemers te controleren middels een personeelsvolgsysteem, mits dat zorgvuldig geschiedt. Zo dient een belangenafweging plaats te vinden tussen de bedrijfsbelangen van de werkgever en de privacybelangen van de werknemers, dient overleg plaats te vinden met de ondernemingsraad en dienen de werknemers goed geïnformeerd te worden over de doelstellingen en het gebruik van personeelsvolgsystemen.

Omvang instemmingsrecht
In de memorie van toelichting bij de introductie van de “privacyinstemming” in 1998 (TK, 1995/1996, 24 615, nr. 3) zijn er enkele opmerkingen over de omvang c.q. reikwijdte van het instemmingsrecht. Daaruit valt op te maken dat de instemming van de ondernemingsraad nodig is als de werkgever de “beleidsruimte” invult in o.a. meldingsformulieren. Op basis van deze toelichting kan aangenomen worden dat in de gevallen dat een werkgever geen enkele beleidsruimte heeft, de instemming van de ondernemingsraad niet vereist is. Dit valt ook te baseren op artikel 27, lid 3, waarin bepaald is dat instemming niet vereist is, voor zover de betrokken aangelegenheid voor de onderneming reeds inhoudelijk is geregeld in een collectieve arbeidsovereenkomst of een regeling van arbeidsvoorwaarden vastgesteld door een publiekrechtelijk orgaan, zoals de BBRA.

Bijlage E Geïnterviewde personen

#	Datum	Naam	Organisatie
	20 apr 2015	Job Vos en H-P Köhler	Kennisnet
	20 apr 2015	Marc Fleischeuers en H-P Köhler	Kennisnet
	23 apr 2015	Ronald Slomp M. Zwinkels	OCW

Bijlage F Bestudeerde documentatie

#	Documentnaam	Versie	Datum
1	Advies ontwerp Nummervoorziening	Versie 1.0	5 maart 2015
2	Ontwerp besluit Nummervoorziening (final draft) stuk voor DBP	Versie 8	6 maart 2015
3	Advies Juridische Aspecten Nummervoorziening		6 maart 2015
4	Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen – en de daarbij behorende Model Bewerkersovereenkomst	Definitieve versie	24 april 2015
5	Keycontrols = Rapport Stichting Kennisnet, Privacy Enhanced Keten (PEK) pseudoniemen in de onderwijsketen	Concept	23 april 2015
6	Eindrapport SION IAA 2013: Persoonsnummers en IAA voorzieningen in het onderwijs	Versie 1.0, Definitief	3 februari 2014
7	Het belang van een unieke ID voor de leermiddelenketen in het VO en het kwantitatief belang van een sector overstijgende unieke ID per leerling - St Beter Digitaal Leren		10 april 2015