

CENTRALE DPIA

Basis van ParnasSys

(Leverancier: Topicus Education B.V.)

Versie 1.0 (november 2025)

Colofon

DPIA uitgevoerd door	Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A. (SIVON) www.sivon.nl info@sivon.nl
Betrokkenen bij uitvoering DPIA	<i>Schrijvers van de DPIA:</i> Sander van de Molen (jurist en adviseur IBP) Susan Ashworth (adviseur IBP) Pascal Marcelis (jurist en adviseur IBP) <i>Betrokken bij de uitvoering van de DPIA:</i> Ashley Hoogendoorn (DPIA-projectmanager) Reza Razai (ISO en adviseur IBP) Job Vos (jurist en adviseur IBP SIVON)
Met dank aan	Team van Topicus Education B.V. / ParnasSys Pim Koteris (Privacy Officer) Bob Reijnders (Head Technology) Dion van den Berg (CISO) Ina Klaster (Aurora Onderwijsgroep) Paul Deguelle (namens Aurora Onderwijsgroep) Liesbeth Jansen (TWijs) Chantal van Rijn (SCO Delft e.o.) Ravindra Kewal (Herman Broerenstichting)
Auteurs model DPIA	Hans-Peter Ligthart (portfoliomanager IBP SIVON) Job Vos (jurist en adviseur IBP SIVON) Ferdij IJsselmuiden (DPIA-projectmanager)

Deze DPIA is gebaseerd op de *Model DPIA Rijksdienst versie 3.0, Handreiking DPIA in het mbo, Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (1.0)*. De gebruiker mag deze publicatie kopiëren, verspreiden, doorgeven, remixen en afgeleide werken maken onder de voorwaarde van het vermelden van de “Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A., [de naam van de betrokken schrijvers van de DPIA]” en link/bron/vindplaats van dit document (Creative Commons CC-BY 4.0).

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden SIVON en de auteur(s) geen aansprakelijkheid voor eventuele fouten, onvolkomenheden of schade als gevolg van het gebruik van dit document. Deze DPIA helpt schoolbesturen als verwerkingsverantwoordelijke om zelf een DPIA uit te voeren en een oordeel te vormen over risico's voor de rechten en vrijheden van betrokkenen. Consulteer bij twijfel een in

privacy gespecialiseerde specialist, jurist of advocaat voor advies over de toepassing van DPIA voor uw eigen organisatie.

Versiebeheer

Datum	Versie	Wijziging
April 2024	0.1	Start tekst DPIA ParnasSys
September 2024	0.2	Aanpassingen tekst DPIA ParnasSys
November 2024 – Augustus 2025	0.3 – 0.9	Aanpassingen tekst DPIA ParnasSys
Augustus 2025	0.91	Concept gedeeld met Topicus Education B.V.
November 2025	0.93	2 ^e concept gedeeld met Topicus Education B.V.
18 november 2025	1.0	Finale versie

Inhoudsopgave

1. Leeswijzer	6
2. Samenvatting	7
3. Uitleg en achtergrond DPIA	11
1. Informatiebeveiliging en privacy (IBP)	11
2. Privacyconvenant en toetsing verwerkersovereenkomsten	11
3. DPIA	12
4. Verplichte uitvoering DPIA	12
5. Centrale en lokale DPIA	13
6. Methodiek DPIA	13
7. Funderend onderwijs referentie architectuur (FORA)	14
4. Motivering DPIA ParnasSys	15
1. Verplichting uitvoeren DPIA	15
2. Scope van deze DPIA	16
3. Buiten scope	16
5. Deel A: Gegevensverwerkingsanalyse	17
1. Beschrijving van het gegevensverwerkende proces	17
2. Persoonsgegevens	18
3. Gegevensverwerkingen	20
4. Verwerkingsdoeleinden	30
5. Betrokken partijen	32
6. Belangen bij de gegevensverwerking	35
7. Verwerkingslocaties	36
8. Data Transfer Impact Assessment (DTIA)	37
9. Technieken en methoden van gegevensverwerking	37
10. Juridisch en beleidsmatig kader	42
11. Bewaartermijnen	42
6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen	46
12. Rechtsgrond	46
13. Bijzondere persoonsgegevens	51
14. Doelbinding	52
15. Kinderrechten-afweging (Best Interests Assessment Children)	52

16 a. Noodzakelijkheid	54
16. b. Proportionaliteit en subsidiariteit	55
17. Rechten van de betrokkenen	55
18. Beoordeling verwerkersovereenkomst	57
7. Deel C: Beschrijving en beoordeling risico's voor de betrokkenen	60
Beoordelingskader risico's	60
19. Risico's	61
8. Deel D: Beschrijving voorgenomen maatregelen	64
20. Maatregelen	65
9. Deel E: MODEL lokale DPIA	70
A. Uitvoering lokale DPIA	70
B. Overwegingen over centrale DPIA	70
C. Organisatiespecifieke- en algemene applicatierisico's	70
D. Overwegingen implementatie en lokale DPIA: aanvullende risico's en maatregelen	75
E. Verklaring en advies functionaris voor gegevensbescherming (FG)	76
F. Visie betrokkenen	76
G. Conclusie	77
H. Risico-mitigerende maatregelen schoolbestuur	77
I. Aanbevelingen	77
J. Verklaring schoolbestuur	78
Bijlage 1: Gebruikte termen en definities	79
Bijlage 2: Uitleg risico's	82
Bijlage 3: Document Topicus inzake versleuteling (encryptie)	83

1. Leeswijzer

Dit DPIA-rapport bestaat uit de volgende opbouw en hoofdstukken:

Hoofdstuk 1 betreft deze leeswijzer.

In hoofdstuk 2 staat de samenvatting van de uitkomsten van deze DPIA voor communicatiedoeleinden.

Hoofdstuk 3 geeft een algemene uitleg over wat een DPIA is, wanneer deze verplicht is, wat het gevolgde model is, en wat de door SIVON gevolgde methodiek is.

Hoofdstuk 4 beschrijft de applicatie waarop deze DPIA ziet, en wat er wel en niet meegenomen is in het onderzoek (binnen scope en buiten scope).

De uitvoering van de DPIA bestaat uit de volgende onderdelen:

- Hoofdstuk 5: deel A bevat de gegevensverwerkingsanalyse (beschrijving van de gegevensverwerkingen).
- Hoofdstuk 6: deel B bevat de beoordeling van de rechtmatigheid van de gegevensverwerkingen.
- Hoofdstuk 7: deel C bevat de beschrijving en beoordeling van de risico's.
- Hoofdstuk 8: deel D is de beschrijving voorgenomen maatregelen die de gevonden risico's beperken.
- Hoofdstuk 9: deel E is het model lokale DPIA die schoolbesturen gebruiken voor het zelf uitvoeren van deze DPIA binnen hun eigen organisatie.

Bijlage 1 bevat veelgebruikte termen en definities.

Bijlage 2 bevat een uitleg van de in deze DPIA genoemde risico's.

Bijlage 3 bevat een toelichting van Topicus op de huidige methode van versleuteling

2. Samenvatting

Deze DPIA heeft betrekking op het *leerlingadministratie-* en *leerlingvolgsysteem* ParnasSys. ParnasSys wordt geleverd door de Topicus Education B.V. (hierna Topicus). Voor deze DPIA staat Basis van ParnasSys centraal. Toepassingen zoals Parro, Ouderportaal, Schoolkassa, Kindbegrip en Leerlijnen vallen buiten de scope van deze DPIA. ParnasSys wordt gebruikt door ongeveer 80% van het Nederlandse primaire onderwijs.

In ParnasSys staan veel persoonsgegevens. De mogelijke risico's die het gebruik van Basis van ParnasSys met zich meebrengen worden in deze DPIA geïnventariseerd. Op basis van de risico's wordt nagegaan of de juiste maatregelen worden toegepast om deze risico's te minimaliseren, zodat een veilig gebruik van Basis van ParnasSys mogelijk is. De DPIA bevat alle wettelijk verplichte elementen van de AVG: een systematische beschrijving van de verwerkingen en de verwerkingsdoelen, de beoordeling van de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden, en een beoordeling van de risico's voor betrokkenen en de getroffen maatregelen. Met het uitvoeren van een DPIA kan de verwerkingsverantwoordelijke (de onderwijsinstelling) aantoonbaar maken dat aan de verplichtingen van de AVG is voldaan.

In april 2021 hebben SIVON en Kennisnet een eerdere generieke DPIA uitgevoerd op het systeem ParnasSys. Uit deze DPIA – versie 1.1. - kwam naar voren dat er een aantal hoge risico's voor de rechten en vrijheden van betrokkenen waren geconstateerd bij de verwerking van persoonsgegevens binnen ParnasSys.

De reactie van leverancier Topicus op die bevindingen zijn niet opgenomen in het DPIA-rapport van 2021. Daarom is in september 2022 een *Remediation Report* uitgebracht, waarin de door Topicus getroffen maatregelen ter mitigatie van de in het oorspronkelijke DPIA-rapport geïdentificeerde risico's, en die betrekking hadden op de verantwoordelijkheid van de leverancier, zijn uiteengezet.

De bevindingen uit de eerdere rapportage uit 2021 op ParnasSys zijn in deze vernieuwde versie meegenomen. Zo heeft Topicus inmiddels meerdere verbeteringen doorgevoerd, zoals standaardisering van koppelingen. Met de voorliggende nieuwe generieke DPIA geeft SIVON invulling aan het voornemen om de eerder uitgevoerde DPIA's op leerlingadministratiesystemen te actualiseren.

Samenwerking

De samenwerking tijdens het DPIA-proces met Topicus als leverancier van ParnasSys was positief en constructief. De open werkwijze, goede besprekingen over de inhoud en gemotiveerde houding om verbetervoorstellen te overwegen hebben bijgedragen aan het onderzoek en identificatie van de risico's. Diverse inhoudelijke besprekingen van met name technische aard in het kader van beveiligingsmaatregelen, zijn in goed overleg gevoerd. Dit heeft ertoe geleid dat Topicus gedurende het DPIA-traject al een aantal verbeterpunten heeft uitgevoerd. Dit betrof onder andere bewaartermijnen voor technische logs, het jaarlijkse testen (pentesting) en het hebben van een aantoonbaar gedocumenteerde

procedure voor opvolging van de bevindingen hieruit. Ook het aantoonbaar maken van beleid en procedures rondom monitoring en detectie van onrechtmatige toegang tot *steppingstones* van de database is opgehelderd. Bovendien is vastgesteld dat Topicus voor wat betreft ParnasSys niet aan ‘Big data verwerkingen’¹ doet.

Daarnaast hebben de deelnemende onderwijsinstellingen belangrijke praktijkinzichten gebracht, die wezenlijk waren voor het begrip van de werking van Basis van ParnasSys. Dit heeft met name geleid tot de voorgestelde maatregelen voor schoolbesturen op basis van de geconstateerde risico’s die in Hoofdstuk 9 zijn beschreven.

Conclusie

Topicus, als leverancier van Basis van ParnasSys, heeft de in deze DPIA geconstateerde risico’s ofwel gedurende de uitvoering van de DPIA opgelost, dan wel voor bepaalde risico’s een oplossing voorgesteld die binnen een afgesproken termijn wordt toegepast. Wanneer scholen en Topicus zich houden aan de voorgestelde maatregelen, kan het gebruik van Basis van ParnasSys op een veilige manier plaatsvinden. Het schoolbestuur zal zelf de centrale DPIA nog specifiek moeten maken en eventuele restrisico’s accepteren.

Indien een onderwijsinstelling gebruik wenst te maken van Basis van ParnasSys, dan is de conclusie dat:

1. De verwerking van persoonsgegevens rechtmatig kan plaatsvinden en ook noodzakelijk is om het doel te bereiken. Het is hierbij van belang te vermelden dat het gebruik van een *Leerlingadministratiesysteem* en *Leerlingvolgsysteem* voor een onderwijsinstelling in het primair onderwijs een wettelijke verplichting is, waarbij het gebruik van ParnasSys een middel is om dit doel te bereiken;
2. De inbreuk op de persoonlijke levenssfeer in verhouding staat tot het doel en er geen minder belastende manier is om hetzelfde doel te bereiken;
3. Er adequate maatregelen zijn en worden getroffen om de verwerking te beschermen.

Hieronder staat een samenvatting van de geconstateerde risico’s en maatregelen.

Risico's en maatregelen

Hieronder staat een samenvatting van de geconstateerde risico’s en maatregelen.

De volgorde waarin de risico’s worden gepresenteerd, is afgestemd op de volgorde van de onderzochte aspecten en impliceert geen prioritering naar belangrijkheid.

¹ De definitie van ‘Big data verwerking’ is: *een big data verwerking betreft het geautomatiseerd verwerken en analyseren van extreem grote, diverse en snel geproduceerde datasets, met als doel om waardevolle inzichten te verkrijgen die traditionele systemen niet kunnen opleveren.*

1. Risico:

Autorisaties worden niet *by default* beperkt op basis van ‘need to have’.
Applicatiebeheerder kan alle persoonsgegevens inzien.

Maatregel:

Onderwijsinstelling: Moet de toewijzing van admin-accounts beperken. Tevens de admin een geheimhoudingsverklaring laten ondertekenen.

2. Risico:

Onvoldoende transparantie over inzage in BSN.

Maatregel:

Topicus: Neemt in het rollen en rechten-overzicht op schoolniveau op tot welke gegevens (en dus rechten en rollen) BSN behoort.

3. Risico

Onvoldoende encryptie op de database ‘*at rest*’, er ontbreekt een tweede encryptielaag.

Maatregel:

Topicus: Gaat dubbele encryptie implementeren.

4. Risico:

Exportfunctionaliteit is standaard beschikbaar zonder beperkingen (exporteren/downloaden staat *by default* aan).

Maatregel:

Topicus: Gaat exporteren/downloaden zichtbaar maken in logging (zie ook bij 6).
Onderwijsinstelling: moet afspraken maken over het genereren en gebruiken van exports/downloads en hier controle op uitoefenen.

5. Risico

Met betrekking tot exports wordt niet op alle functies een “voorvertoning”-mogelijkheid (tijdelijk browsertabblad) getoond. De huidige kleurstellingen bij exports werken bovendien zogenaamde *nudging* in de hand.

Maatregel:

Topicus: Past de voorvertoningen aan, voor zover technisch mogelijk, evenals de kleurstellingen bij de exportfuncties.

6. Risico:

Er worden onvoldoende beveiligingsmaatregelen toegepast (loggingfunctionaliteit exports en cijferwijzigingen niet standaard voor onderwijsinstellingen zelf beschikbaar).

Maatregel:

Topicus: Breidt de loggingfunctionaliteit uit die onderwijsinstellingen zelf beschikbaar hebben met informatie over welke gebruikers exports/downloads hebben uitgevoerd, alsmede wie mutaties in cijfers heeft doorgevoerd.

Onderwijsinstelling: Moet afspraken maken over monitoring en controle op deze logging.

7. Risico:

Gebruik 2FA staat niet *by default* aan.

Maatregel:

Onderwijsinstelling: Moet 2FA instellen en afdwingen.

8. Risico:

Ontoereikende afspraken in de verwerkersovereenkomst (inzake bewaartermijnen loggings, verwijdering na einde contract en cookiegebruik).

Maatregel:

Topicus: Past de informatie in de verwerkersovereenkomst aan.

3. Uitleg en achtergrond DPIA

1. Informatiebeveiliging en privacy (IBP)

In het onderwijs maken we steeds meer gebruik van persoonsgegevens en ict. We slaan steeds meer informatie op en wisselen digitaal steeds meer informatie uit. Dit doen niet alleen scholen, maar ook de leveranciers van digitale leermiddelen. Leerlingen, ouders en medewerkers willen erop kunnen vertrouwen dat scholen én leveranciers correct met hun gegevens omgaan en de privacy waarborgen.

Privacy is enerzijds het recht om met rust te worden gelaten. Anderzijds gaat het over het recht om gegevens over jezelf te kunnen controleren. Als je bij alles wat je doet, gevolgd wordt én je denkt of weet dat dit gevolgen voor jou kan hebben, dan pas je jouw gedrag daarop aan. Zonder het recht op privacy kan een mens niet vrij zijn. Privacy is een randvoorwaarde in een democratische samenleving. Daarom blijft het belangrijk dat scholen privacy goed organiseren. Het beschermen van privacy gaat niet zonder het beschermen van persoonsgegevens; gegevens van betrokkenen mogen immers niet in verkeerde handen vallen. Daarom spreken we vaak over IBP: Informatiebeveiliging en Privacy.

2. Privacyconvenant en toetsing verwerkersovereenkomsten

Volgens de Europese privacywet 'Algemene Verordening Gegevensbescherming' (AVG) is een schoolbestuur eindverantwoordelijk voor de bescherming van de privacy en persoonsgegevens van leerlingen, hun ouders, en medewerkers. Het schoolbestuur wordt **verwerkingsverantwoordelijke** genoemd. Het schoolbestuur moet de controle houden over het gebruik van deze persoonsgegevens en zij bepaalt dus voor welke doelen deze gegevens mogen worden gebruikt. Een leverancier van software waarin al deze persoonsgegevens zijn opgenomen, wordt in de AVG **verwerker** genoemd. Deze mag die persoonsgegevens niet zomaar voor eigen doeleinden gebruiken. In een **verwerkersovereenkomst** legt het schoolbestuur afspraken vast met deze leverancier. In het onderwijs wordt hiervoor gebruik gemaakt van de model-verwerkersovereenkomst van het Privacyconvenant onderwijs².

Scholen kunnen gemakkelijk verwerkersovereenkomsten goedkeuren en digitaal ondertekenen met behulp van de Dienst Verwerkersovereenkomsten van Kennisnet³. SIVON toetst voor het primair en voortgezet onderwijs vooraf of de verwerkersovereenkomsten van leveranciers van de meest gebruikte applicaties voldoen aan de eisen van het privacyconvenant⁴. Deze rapportages zijn onder andere beschikbaar in de Dienst Verwerkersovereenkomsten.

² <https://www.privacyconvenant.nl/>.

³ <https://www.kennisnet.nl/dienst-verwerkersovereenkomsten/>.

⁴ <https://sivon.nl/toetsen-verwerkersovereenkomsten/>.

3. DPIA

Om vast te stellen of de gegevens van leerlingen en medewerkers (persoonsgegevens) in een proces, applicatie, software of ict-middel veilig en verantwoord gebruikt worden, is het volgens de AVG verplicht om een Data Protection Impact Assessment (DPIA) uit te voeren. In de AVG wordt dit een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Een DPIA wordt uitgevoerd op een proces, applicatie of verwerking van persoonsgegevens. Meestal gaat het om een applicatie van een leverancier (verwerker). De DPIA wordt uitgevoerd volgens de eisen van artikel 35 van de AVG.

Met een DPIA wordt beoordeeld wat de risico's en (mogelijke) gevolgen zijn van het gebruik van de applicatie voor de bescherming van de persoonsgegevens van de leerlingen, hun ouders en medewerkers. Er wordt vastgesteld of het gebruik van persoonsgegevens (de verwerking) een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen. Als de privacyrisico's (te) hoog zijn, moet er worden gezocht naar maatregelen om deze risico's te beperken. Dit worden mitigerende maatregelen genoemd. Als de hoge risico's niet weggenomen kunnen worden, dan mag volgens de AVG deze verwerking (gebruik applicatie) niet worden uitgevoerd of voortgezet.

De uitkomst van de DPIA is o.a. deze rapportage met daarin een overzicht van geclassificeerde risico's voor de rechten en vrijheden van betrokkenen. In het rapport staan ook de nodige mitigerende maatregelen benoemd. De verwerkingsverantwoordelijke stelt uiteindelijk de DPIA vast. Hiermee wordt vastgesteld welke maatregelen nog moeten worden uitgevoerd en dat het schoolbestuur de resterende vastgestelde risico's accepteert.

4. Verplichte uitvoering DPIA

Deze privacytoets is verplicht als de verwerking van persoonsgegevens - gelet op de aard, de omvang, de context en de doeleinden van die verwerking - waarschijnlijk een hoog risico inhoudt voor de 'rechten en vrijheden' (privacy) van leerlingen en medewerkers. Ook is het mogelijk dat het uitvoeren van een DPIA verplicht is volgens de regels van de privacy toezichthouder Autoriteit Persoonsgegevens (AP), die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van een DPIA verplicht is⁵. Voor het onderwijs betekent dit dat een DPIA altijd verplicht is op tenminste het leerlingvolg- en/of -administratiesysteem (LVS/LAS) zoals ParnasSys, het personeelsadministratiesysteem en breed ingezette applicaties met digitaal leermateriaal. Ook de EDPB⁶ benadrukt dit: *'Een gegevensbeschermingseffectbeoordeling kan ook nuttig zijn om het gegevensbeschermingseffect van een technologisch product te beoordelen, bijvoorbeeld hardware of software, indien dit waarschijnlijk door verschillende verwerkingsverantwoordelijken zal worden gebruikt om verschillende verwerkingen uit te voeren. Natuurlijk blijft de verwerkingsverantwoordelijke die het product lanceert verplicht om zijn eigen gegevensbeschermingseffectbeoordeling uit te voeren met betrekking tot de*

⁵ <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf>.

⁶ EDPB: European Data Protection Board (de Europese privacy toezichthouder): https://www.edpb.europa.eu/edpb_en.

specifieke implementatie, al kan hij zich hiervoor baseren op een door de productaanbieder uitgevoerde gegevensbeschermingseffectbeoordeling, in voorkomend geval.'

5. Centrale en lokale DPIA

Bij applicaties die door veel verwerkingsverantwoordelijken – op dezelfde wijze – worden gebruikt, is het zinvol om deze DPIA samen uit te voeren. Denk bijvoorbeeld aan een leerlingadministratiesysteem, zoals ParnasSys. Hierdoor hoeft niet elk schoolbestuur zelf het spreekwoordelijke wiel uit te vinden. SIVON voert daarom in opdracht van OCW namens het primair en voortgezet onderwijs **centrale DPIA's** uit. Deze DPIA's worden door SIVON uitgevoerd namens een aantal schoolbesturen (leden) als verwerkingsverantwoordelijke(n). Door hierbij samen op te trekken met verschillende schoolbesturen die hun ervaring uit de onderwijspraktijk meebrengen, wordt expertise en ervaring samengebracht. Ook is het makkelijker om afspraken te maken met de leverancier als er aanvullende mitigerende maatregelen moeten worden getroffen, omdat SIVON namens de leden spreekt. Door deze centrale DPIA's uit te voeren op veelgebruikte systemen, helpt SIVON leerlingen en medewerkers aan een digitale veilige leeromgeving. Bovendien leidt deze centrale aanpak tot een kostenbesparing voor de onderwijsinstellingen.

Schoolbesturen moeten volgens de AVG zelf als verwerkingsverantwoordelijke een DPIA uitvoeren en zelf de risico's afwegen. Dat kan SIVON niet doen. Na de uitvoering van de centrale DPIA moet daarom ieder schoolbestuur de uitkomsten uit de centrale DPIA op hun eigen organisatie toepassen. We noemen dit een **lokale DPIA**. In deze lokale DPIA weegt het schoolbestuur de door SIVON gevonden risico's, identificeert eventuele aanvullende risico's en bepaalt zij zelf of er binnen het schoolbestuur nog mitigerende maatregelen moeten worden genomen.

SIVON helpt besturen hiermee doordat in de centrale DPIA de meest voorkomende risico's voor schoolbesturen worden bepaald. Het uitvoeren van een lokale DPIA is wel altijd nog noodzakelijk: SIVON heeft een algemene, centrale DPIA uitgevoerd en kan geen rekening houden met mogelijke lokale risico's van gebruik van het systeem op scholen.

6. Methodiek DPIA

SIVON volgt bij de uitvoering van de centrale DPIA het model van de Rijksoverheid⁷, aangevuld met onderwijs specifieke informatie uit de *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*⁸. Het model is daarnaast aangepast aan specifieke informatie over de applicatie en aangevuld met een model lokale DPIA voor schoolbesturen. Er wordt rekening gehouden met Europese richtlijnen van de gezamenlijke Europese toezichthouders (EDPB) waaronder de "Richtsnoeren voor gegevensbeschermingseffectbeoordelingen (2016/679, 4 april 2017)".

⁷ [Model DPIA Rijksdienst v3.0.pdf \(kcbr.nl\)](https://model.dpia.rijksoverheid.nl/).

⁸ <https://aanpakibp.kennisnet.nl/app/uploads/Handleiding-DPIA-v1.0-1.pdf>.

SIVON voert bij de uitvoering van de centrale DPIA de volgende activiteiten uit:

- Beschrijving van de (methoden van) gegevensverwerkingen (gegevensverwerkingsanalyse) en toegepaste (beveiligings)technieken;
- Beoordeling van de rechtmatigheid van de gegevensverwerkingen, inclusief afweging van kinderrechten;
- Beschrijving en beoordeling risico's voor de betrokkenen;
- Beschrijving en beoordeling van (eventuele) (voorgenomen) maatregelen die de gevonden (privacy)risico's beperken;
- Toetsen van de verwerkersovereenkomst;
- Beoordeling beveiligingsmaatregelen aan de hand van de BIV-classificatie en het ROSA certificeringsschema;
- Beoordeling van de mogelijkheden om te voldoen aan rechten van betrokkenen;
- Beoordeling van de default settings (privacy by design);
- Technologie-scan naar gebruikte webtechnologieën;
- Analyse van de wijze waarop het systeem voorziet in logging en de wijze waarop dit door de onderwijsinstelling gemonitord en gecontroleerd kan worden;
- Overleg met betrokken schoolbesturen en leverancier over (aanvullende) mitigerende maatregelen;
- Opstellen en bespreken DPIA-rapportage.

7. Funderend onderwijs referentie architectuur (FORA)

Bij de uitvoering van de DPIA wordt gebruik gemaakt van FORA: Funderend Onderwijs Referentie Architectuur.

Applicatielandschap

Het hebben van een architectuur helpt bij het tijdig en goed reageren op zakelijke of juridische (AVG) eisen en/of (externe) dreigingen die een (mogelijke) aanpassing in de informatiehuishouding vragen. (Norm 1.4 architectuur van het Normenkader IBP <https://aanpakibp.kennisnet.nl/normenkader/>)

In deze DPIA gebruiken we FORA om de applicatie te kunnen plaatsen in het applicatielandschap: welke plaats neemt de applicatie in het totaal aan applicaties die een school gebruikt in.

Voor het funderend onderwijs is de FORA (Funderend Onderwijs Referentie Architectuur) ontwikkeld (<https://fora.wikixl.nl/index.php/Hoofdpagina>).

FORA is een gestandaardiseerde methodiek die inzicht geeft in verplichte processen en onderwijsactiviteiten in het primair (po) en voortgezet onderwijs (vo).

De FORA biedt inzicht in wat de bedrijfsfuncties zijn van een po en vo school. Het hoofdbedrijfsfunctiemodel beschrijft op hoofdlijnen wat een onderwijsorganisatie doet. Verdieping daarvan vindt plaats in het bedrijfsfunctiemodel dat in meer detail weergeeft op welke manier invulling gegeven wordt aan het 'wat'. Hiermee is het mogelijk om

‘referentiecomponenten’ toe te voegen. Referentiecomponenten zijn typen systemen - zoals een LAS, een Toetssysteem, of een ELO - met bijbehorende functionaliteiten ('applicatiefuncties').

SIVON voert centrale DPIA's uit op een applicatie. Een applicatie kan in de FORA vertaald worden naar een of meerdere referentiecomponenten, zie <https://fora.wikixl.nl/index.php/Referentiecomponentenmodel>.

Een referentiecomponent is een functionele afbakening van een modulair, zelfstandig inzetbaar en vervangbaar (deel van een) systeem.

4. Motivering DPIA ParnasSys

1. Verplichting uitvoeren DPIA

Een DPIA is verplicht als de verwerking van persoonsgegevens - gelet op de aard, de omvang, de context en de doeleinden van die verwerking - waarschijnlijk een hoog risico inhoudt voor de privacy van onderwijsdeelnemers en medewerkers. Ook is het mogelijk dat het uitvoeren van een DPIA verplicht is volgens de regels van de privacytoezichthouder Autoriteit Persoonsgegevens die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van een DPIA verplicht is⁹. Het schoolbestuur voert door middel van een DPIA *voorafgaand* aan de verwerking van persoonsgegevens een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

Bij het onderzoek naar het LAS/LVS Basis van ParnasSys (van leverancier Topicus Education B.V., hierna Topicus) is gebleken dat het uitvoeren van een DPIA verplicht is.

De verplichting volgt onder meer uit artikel 35 AVG, aangezien de verwerking van persoonsgegevens binnen het LAS/LVS aan meerdere criteria voldoet. Er is sprake van op grote schaal verwerking van bijzondere categorieën van persoonsgegevens. Hierdoor is er sprake van een ‘*hoog risicoverwerking*’.

Volgens het overzicht van de European Data Protection Board¹⁰, de opvolger van de WP29, wordt aan vier criteria voldaan. Ook hierdoor spreken we van een ‘*hoog risicoverwerking*’.

Er is namelijk sprake van een verwerking van ‘*gevoelige gegevens*’ (1) die kunnen leiden tot ‘*evaluatie of scoretoekenning*’ (2), omdat er binnen Basis van ParnasSys leer- en testresultaten worden verwerkt over een langere periode en deze resultaten zichtbaar zijn voor gebruikers (*leerkrachten en leerlingen*). Daarnaast heeft deze verwerking van persoonsgegevens betrekking op kinderen onder de 16 jaar. Deze vorm van gegevensverwerking vereist een extra bescherming omdat het hier ‘*kwetsbare personen*’ (3) betreft. Tot slot is er sprake van ‘*op grote schaal verwerkte gegevens*’ (4) omdat binnen Basis van ParnasSys de gegevens van alle leerlingen (en in mindere mate van leerkrachten)

⁹ <https://autoriteitpersoonsgegevens.nl/uploads/imported/stcrt-2019-64418.pdf>.

¹⁰ De ‘WP29 werkgroep’ (vanaf mei 2018: European Data Protection Board – EDPB): zie de WP29-richtlijn voor DPIA's (WP 248 rev.01 zoals vastgesteld op 4 april 2017, en laatstelijk gewijzigd op 4 oktober 2017).

worden vastgelegd. Dit resulteert in een groot aantal betrokkenen en een groot volume aan verwerkte gegevens.

Bovendien is er volgens de lijst van de Autoriteit Persoonsgegevens¹¹ ook sprake van ‘15. *Profileren*’. Dit gaat om een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op automatische verwerking, zoals bijvoorbeeld *prestaties van leerlingen*. Daarnaast is er sprake van ‘7. *Gezondheidsgegevens*’. Dit gaat over grootschalige verwerkingen van gegevens over gezondheid door o.a. (speciaal)onderwijsinstellingen. Ook het voldoen aan deze criteria stelt het uitvoeren van een DPIA verplicht.

Aangezien meerdere hoogrisico-criteria uit zowel de Europese als nationale richtlijnen van toepassing zijn, is het uitvoeren van een DPIA voor deze applicatie dus een wettelijke verplichting voor verwerkingsverantwoordelijken die gebruikmaken van Basis van ParnasSys.

2. Scope van deze DPIA

Deze DPIA heeft betrekking op het digitale leerling administratie (LAS) en leerlingvolgsysteem (LVS) (hierna: leerling- en onderwijsvolgsysteem, of LAS/LVS) Basis van ParnasSys, dat door Topicus als leverancier wordt geleverd aan scholen voor primair en speciaal (basis)onderwijs. Basis van ParnasSys is een digitale oplossing om onderwijsinstellingen te ondersteunen bij hun administratieve taken rondom aanmeldingen, inschrijvingen, studievoortgang, leerlingbegeleiding en kwaliteitszorg.

Topicus biedt middels Basis van ParnasSys de mogelijkheid om de basisfunctionaliteit uit te breiden met diverse modules op onderwijsgerelateerde vlakken en om bijvoorbeeld koppelingen te maken met systemen van andere (externe) partijen. In deze DPIA richten we ons echter alleen op de basisfunctionaliteit (‘Basis van ParnasSys’) en de mogelijke risico's die het gebruik van dit digitale leerling- en onderwijsvolgsysteem met zich meebrengt.

Op basis van eventueel geconstateerde risico's wordt nagegaan of de juiste maatregelen worden toegepast om deze risico's te minimaliseren, zodat een veilig gebruik van Basis van ParnasSys mogelijk is.

3. Buiten scope

Er wordt uitsluitend gekeken naar de basisfunctionaliteit van ParnasSys (‘Basis van ParnasSys’) en niet naar de optionele modules en andere aanleverende en afnemende koppelingen¹².

¹¹ Zie Staatscourant 2019, nummer 64418 van 27 november 2019.

¹² zie <https://www.parnassys.nl/juridisch/privacybijsluiters> waar deze extra modules en koppelingen zijn opgesomd).

Er is dus expliciet niet gekeken naar modules zoals Kindbegrip, Ultimview, Parro, Privacybasis etc. Deze zijn geen onderdeel van Basis van ParnasSys.

Dat is ook niet gedaan voor specifieke koppelingen tussen Basis van ParnasSys en andere systemen, zoals DULT, Google, Microsoft, HR-koppeling, OSO, ROD, RIO en UWLR of andere (externe) partners.

5. Deel A: Gegevensverwerkingsanalyse

In dit hoofdstuk wordt een gegevensverwerkingsanalyse uitgevoerd: een uitgebreide beschrijving van de gegevensverwerking. Op gestructureerde wijze worden de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen beschreven.

1. Beschrijving van het gegevensverwerkende proces

In deze paragraaf wordt op hoofdlijnen beschreven waar de DPIA op ziet. Wat is het systeem, uit welke modules en/of processen bestaat het en wat is het voorziene gebruik en toepassing in de onderwijspraktijk?

Basis van ParnasSys wordt aangeboden als een zogenaamde Software-as-a-Service (SaaS) voor scholen in het primair en speciaal (basis)onderwijs. Het is dus een webbased applicatie die via de browser wordt gebruikt.

Basis van ParnasSys is een digitaal leerlingadministratiesysteem waarin alle gegevens van de leerlingen worden ingevoerd die van belang zijn om een goede administratie te kunnen voeren. Hiervoor worden ook persoonsgegevens van ouders/verzorgers en medewerkers verwerkt binnen Basis van ParnasSys.

Daarnaast bevat Basis van ParnasSys een digitaal leerlingvolgsysteem waarin scholen informatie invoeren die inzicht in de ontwikkeling van de leerlingen geeft, zodat zij het onderwijs kunnen analyseren en concrete (verbeter)plannen kunnen opstellen.

Alle gegevens van de leerlingen worden op individueel niveau vastgelegd en kunnen ook op groepsniveau worden getoond. Er kunnen digitale rapporten worden opgesteld waarmee de school inzicht krijgt in groepsontwikkeling en resultaten. Scholen kunnen eigen voorkeuren instellen voor het gebruik van Basis van ParnasSys. Daarnaast is het mogelijk om handmatige exports te maken.

De verschillende optionele modules en koppelingen tussen Basis van ParnasSys en andere aanleverende en afnemende systemen vallen niet binnen de scope van de verwerking waarvoor de DPIA is uitgevoerd (zie 4.2 en 4.3).

2. Persoonsgegevens

In dit onderdeel wordt beschreven welke categorieën persoonsgegevens van welke betrokkenen worden verwerkt binnen het systeem. Zie ook de definitiebepalingen in bijlage 1.

Betrokkenen

In Basis van ParnasSys worden persoonsgegevens verwerkt van leerlingen van de scholen, ouders/verzorgers van de leerlingen en van medewerkers (docenten en begeleiders) van de school.

Persoonsgegevens

Binnen Basis van ParnasSys worden de persoonsgegevens en typen persoonsgegevens zoals aangegeven in onderstaande tabel van betrokkenen verwerkt.

De persoonsgegevens worden rechtstreeks verkregen van betrokkenen (leerlingen, ouders/verzorgers en medewerkers) tijdens de inschrijving op de school als het een leerling betreft of bij indiensttreding als het gaat om medewerkers, evenals door het invoeren van eigen gegevens. Bovendien kunnen gedurende de schoolperiode gegevens nog worden gewijzigd of aangevuld, zoals bijvoorbeeld gegevens met betrekking tot gezondheid.

Tabel 3.1 - Persoonsgegevens

Categorie persoonsgegevens	Leerling	Medewerker	Ouder/voogd/ verzorger	Bron verkrijging B= betrokkene S = School
Algemene contact-gegevens	Voorna(a)me(en), Voorletter(s), Achternaam Geslacht Woonadres Postcode Woonplaats Telefoonnummer E-mailadres (privé)	Voorna(a)men, Achternaam Telefoonnummer E-mailadres (school)	Voorna(a)me(en), Voorletter(s), Achternaam Geslacht Woonadres Postcode Woonplaats Telefoonnummer E-mailadres (privé)	B/S
Onderwijsdeelnemer-nummer	Een administratienummer dat onderwijsdeelnemers identificeert			S
ECK-ID	X			S
Nationaliteit	X			B
Geboortedatum	X		X	B
Geboorteplaats	X		X	B
Financiële gegevens met het oog op het berekenen, vastleggen en innen van gelden en bijdragen.			Bankrekeningnr. Factureadministratie	B
Gegevens over gezondheid Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling of op verzoek van leerling/ouders/verzorgers worden	X			B/S

verwerkt, een en ander zover noodzakelijk voor het onderwijs				
Feiten en waarderingen over iemand zijn gedragingen, eigenschappen of opmerkingen (Begeleiding Onderwijsdeelnemers, inclusief handelingsplan)	X			S
Studievoortgang	Klas, leerjaar, ILT-code Examinering Studievoortgang en/of studietraject Begeleiding Onderwijsdeelnemers, inclusief handelingsplan Aan- en afwezigheidsregistraties	Klas, leerjaar, ILT-code		S
Personeelsnummer				
Gebruikersgegevens		Diagnostische gegevens, loggegevens, metadata en IP-adres	Diagnostische gegevens, loggegevens, metadata en IP-adres	S
Beeldmateriaal	Foto's en videobeelden (beeldmateriaal) van betrokkene met of zonder geluid, van activiteiten van de onderwijsinstelling	Foto's en videobeelden (beeldmateriaal) van betrokkene met of zonder geluid, van activiteiten van de onderwijsinstelling		B
Burgerservicenummer (BSN) of PGN ¹³ (Persoonsgebonden nummer)	X			B
Verzuimregistratie	X			S
Overige gegevens	IQ en andere leerpotentieel-gerelateerde gegevens	Gegevens met het oog op de organisatie van het onderwijs (zoals een rooster) en het verstrekken of ter beschikking stellen van leermiddelen.		

Rubrieken met extra invulvelden

In Basis van ParnasSys is het mogelijk om met behulp van rubrieken specifieke waarden, oftewel extra invulvelden voor situaties waarin er geen standaardveld beschikbaar is, toe te voegen aan de personalia van een leerling. Onderwijsinstellingen zijn hier zelf verantwoordelijk voor, Topicus doet hier geen suggesties voor. Deze functionaliteit is alleen toegankelijk voor een beperkt aantal rollen. De ingevulde waarden van deze rubrieken zijn zichtbaar voor alle gebruikers met toegang tot de personalia van de betreffende leerling.

¹³ [https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn/bsn-in-het-onderwijs#:~:text=Iedereen%20die%20onderwijs%20volgt%20dat,aan%20het%20Burgerservicenummer%20\(BSN\).](https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn/bsn-in-het-onderwijs#:~:text=Iedereen%20die%20onderwijs%20volgt%20dat,aan%20het%20Burgerservicenummer%20(BSN).)

Op de "Leerlingstamkaart" bestaat bijvoorbeeld de mogelijkheid voor onderwijsinstellingen om, naast de eerder genoemde lijst van verwerkte persoonsgegevens, ook aanvullende gegevens te verwerken. Dat kan gaan om, zoals in de praktijk voorkomt:

- Beroep ouders
- Genoten opleiding
- Burgerlijke staat etc.

SIVON adviseert onderwijsinstellingen hier zeer terughoudend mee om te gaan in verband met dataminimalisatie. Bovendien moet er sprake zijn van doelbinding en een rechtsgrond om deze gegevens te verwerken.

3. Gegevensverwerkingen

Voor het schetsen van de reikwijdte van de gegevensverwerkingsanalyse wordt gebruik gemaakt van de referentiearchitectuur (de FORA¹⁴ voor het primair en voortgezet onderwijs).

Basis van ParnasSys is zowel een Leerlingadministratiesysteem (LAS) als een Leerlingvolgsysteem (LVS). De verwerkingen binnen Basis van ParnasSys vinden primair plaats om onderwijsinstellingen te ondersteunen bij hun administratieve taken rondom aanmeldingen, inschrijvingen, studievoortgang, leerlingenbegeleiding en kwaliteitszorg.

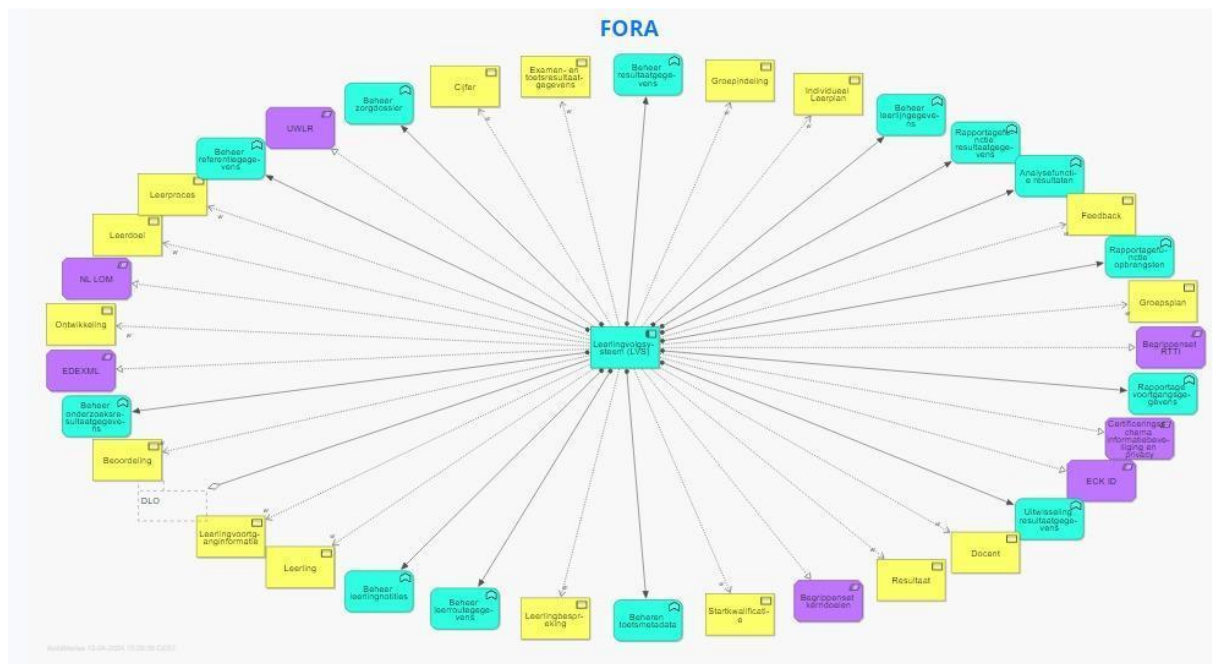
Basis van ParnasSys kan in termen van FORA worden geduid als:

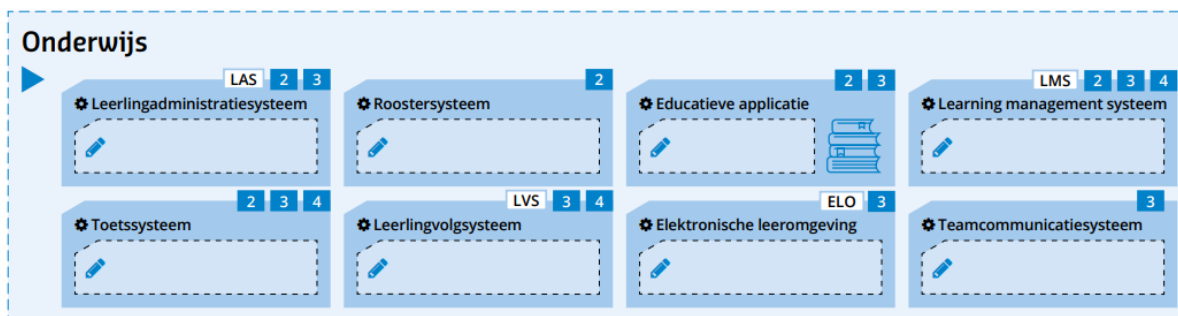
1. Leerlingadministratiesysteem (LAS)

Zie [Leerlingadministratiesysteem \(LAS\) - Funderend Onderwijs Referentie Architectuur \(wikixl.nl\)](https://www.wikixl.nl/wiki/fora/index.php/DPIA) voor vergroting van de afbeelding hieronder.

¹⁴ <https://www.wikixl.nl/wiki/fora/index.php/DPIA>.

Zie [Leerlingvolgsysteem \(LVS\) - Funderend Onderwijs Referentie Architectuur \(wikixl.nl\)](http://wikixl.nl) voor vergroting van de afbeelding hieronder.





Bij het gebruik van Basis van ParnasSys voor het primair onderwijs worden gegevens verwerkt voor een of meerdere van de volgende doeleinden, conform artikel 5 van het Convenant Digitale Onderwijsmiddelen en Privacy¹⁵:

- de opslag van leer- en toetsresultaten;
- het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten;
- de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer;
- analyse en interpretatie van leer- en toetsresultaten;
- het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen;
- de indeling en aanpassing van roosters;
- het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;
- het begeleiden en ondersteunen van leerkrachten/docenten en andere medewerkers van de Onderwijsinstelling *(niet van toepassing op Basis van ParnasSys)*;
- de communicatie met Onderwijsdeelnemers en ouders en met medewerkers van de Onderwijsinstelling;
- monitoring en verantwoording, met name ten behoeve van: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vormen) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;
- het voor zover noodzakelijk en wettelijk toegestaan uitwisselen van Persoonsgegevens met Derden, waaronder:
 - Toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;
 - Samenwerkingsverbanden in het kader van passend onderwijs en regionale samenwerkingen;
 - Partijen betrokken bij de invulling van stage- of leer- werkplekken;
 - Het leveren van Persoonsgegevens aan Onderwijsinstellingen in geval van overstappen tussen Onderwijsinstellingen en bij vervolgonderwijs;
 - Het in opdracht van Onderwijsinstelling leveren van Persoonsgegevens aan een andere partij.
- het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
- het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;

¹⁵ Zie ook 4.0 Gegevensverwerkingsdoeleinden, p. 30.

Bron: [Doeleinden voor verwerking d.d. 20240712.xlsx \(sharepoint.com\)](#)

- de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens;
- de continuïteit, verbetering en goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning;
- het door de Onderwijsinstelling beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek;
- het door de Onderwijsinstelling voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren;
- het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen;
- het behandelen van geschillen (*niet van toepassing op Basis van ParnasSys*);
- financieel beheer (*niet van toepassing op Basis van ParnasSys*);
- de uitvoering of toepassing van een Unierechtelijke of lidstaatrechtelijke wettelijk bepaling of regeling;
 - andere doeleinden ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces) en het begeleiden en volgen van Onderwijsdeelnemers (in hun leerproces), namelijk het kunnen inschrijven en plaatsen van leerlingen.

Adaptiviteit

Binnen ParnasSys wordt er niet gewerkt met adaptiviteit. Tevens vindt er geen verwerking plaats met het oog op de beoordeling van de leer- en testresultaten van één leerling ten opzichte van de resultaten van een normgroep, om inzicht te krijgen hoe een leerling presteert ten opzichte van deze groep.

Optionele verwerkingen

Bij het gebruik van de digitale leermiddelen voor het primair onderwijs kunnen met specifieke toestemming van de onderwijsinstelling ook andere verwerkingen plaatsvinden.

Onderwijsinstellingen hebben voor deze verwerkingen een actieve keuzeoptie en gaan in de digitale leermiddelen voor het primair onderwijs of anderszins expliciet akkoord met de verwerkingen voordat deze plaatsvinden.

Zoals in 2.4 is aangegeven, zijn deze producten/koppelingen aanvullend en optioneel en vallen buiten scope van deze DPIA. Zie ook verwijzing naar

<https://www.parnassys.nl/juridisch/privacybijsluiter>.

Applicatielandschap

[Instructie aan onderwijsinstelling] Neem hierbij een korte beschrijving op van het applicatielandschap van het schoolbestuur waarbinnen het systeem wordt gebruikt. DOEL: hulpmiddel om te komen tot oplossing.

Schets van de applicatie in de context van het applicatielandschap, zie hieronder en op https://fora.wikixl.nl/images/fora/d/d9/FORA_invulposter_mbt_systemen_die_persoonsgegevens_verwerken.pdf en Fora voor vergroting van deze afbeelding.

FORA: Systemen verwerken persoonsgegevens

FORA Kennisnet

Een slecht beveiligde ikt-omgeving of ondoordacht privacybeleid kan leiden tot vervelende situaties met grote gevolgen voor een school. Leertijd, factoren die niet doorgaan, verloren documenten, te laat betaalde facturen of aanslagen – het zijn maar enkele voorbeelden. Welke systemen zijn relevant voor een risico- en impactanalyse? Welke processen in de school raken deze systemen?

Deze poster maakt gebruik van de Fundamenteel Onderwijs Reformatie Architectuur (FORA) om een overzicht te bieden van de domeinen, processen en type systemen waar er sprake is van een hoge mate van verwerking van persoonsgegevens. Bij dit type systemen zou u extra bedacht moeten zijn op privacy en beveiliging.

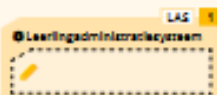
Wilt u aan de slag met ikt-beveiliging op school? Kijk dan verder op www.kennisnet.nl/ict-beveiliging



Bevoegd gezag



Schoolleiding



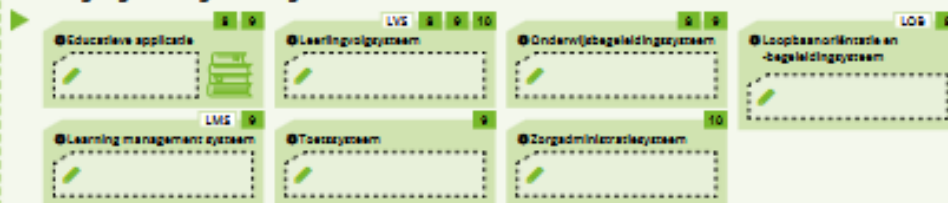
Onderwijs



Onderwijsondersteuning



Leerlingbegeleiding en -zorg



Bedrijfsvoering

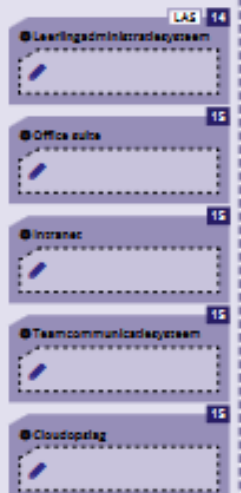


Legenda hoofdbedrijfsfuncties

- 1. Verantwoording
- 2. Onderwijsvoorbereiding
- 3. Onderwijsuitvoering
- 4. Onderwijsbeoordeling
- 5. Inroom, doorstrom, uitroom
- 6. Samenwerken en communiceren leerlingen
- 7. Samenwerken en communiceren ouders
- 8. Leerlingbegeleiding
- 9. Passend onderwijs
- 10. Zorgbegeleiding en -coördinatie
- 11. Personeel en organisatie
- 12. Risico beheer en beveiliging
- 13. Ict-ondersteuning
- 14. Ouderbetrokkenheid ouderschool
- 15. Samenwerken en communiceren medewerkers en samen

Versie 1.0

Algemeen

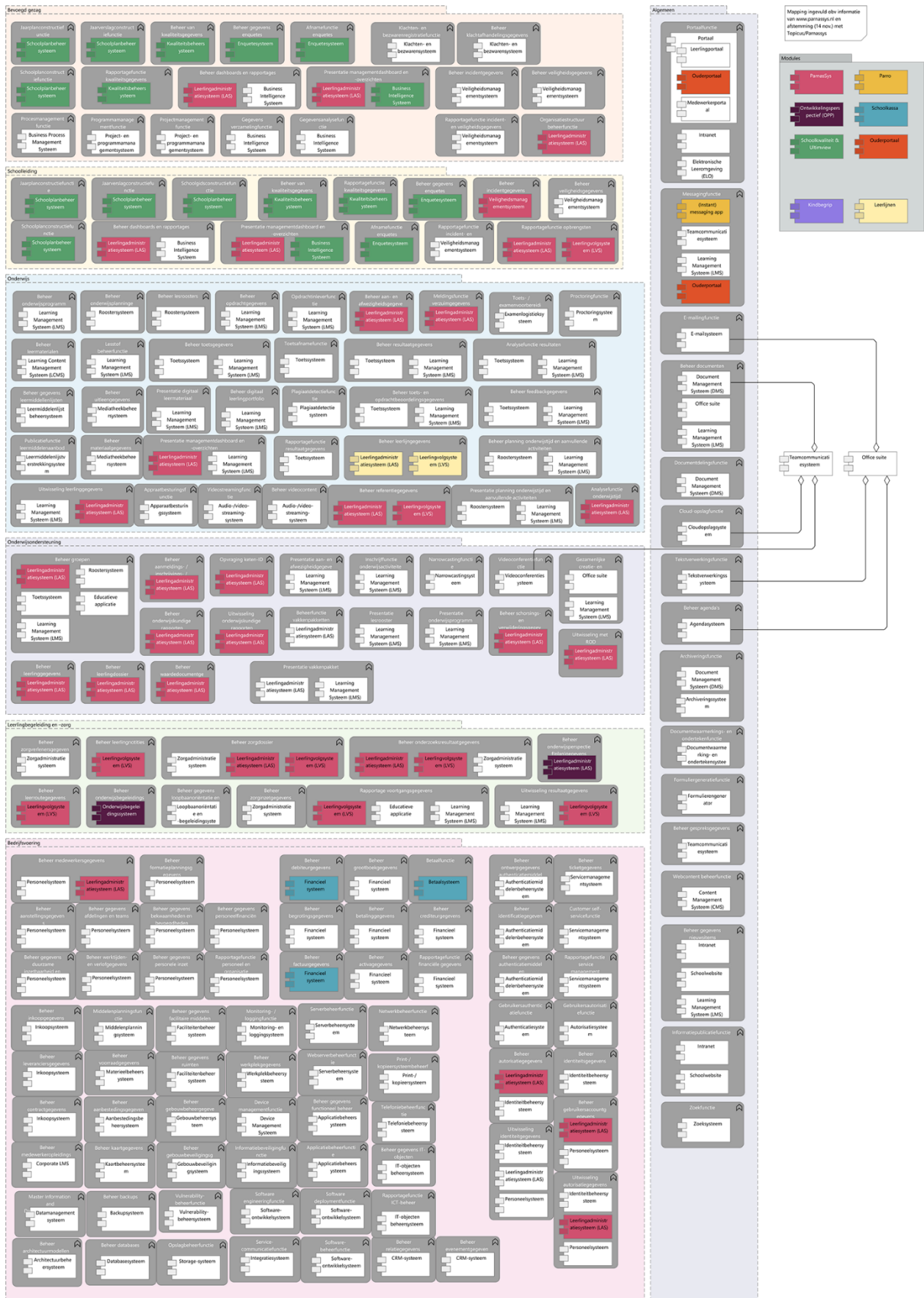


Gegevensstromen/stroomschema

Omdat de gegevensverwerkingen gecompliceerd kunnen zijn en het niet altijd gemakkelijk is om het geheel van gegevensverwerkingen in woorden uit te drukken, is het van belang om de gegevensverwerkingen te visualiseren, bijvoorbeeld aan de hand van een input-proces-output model, stroomschema of workflow.

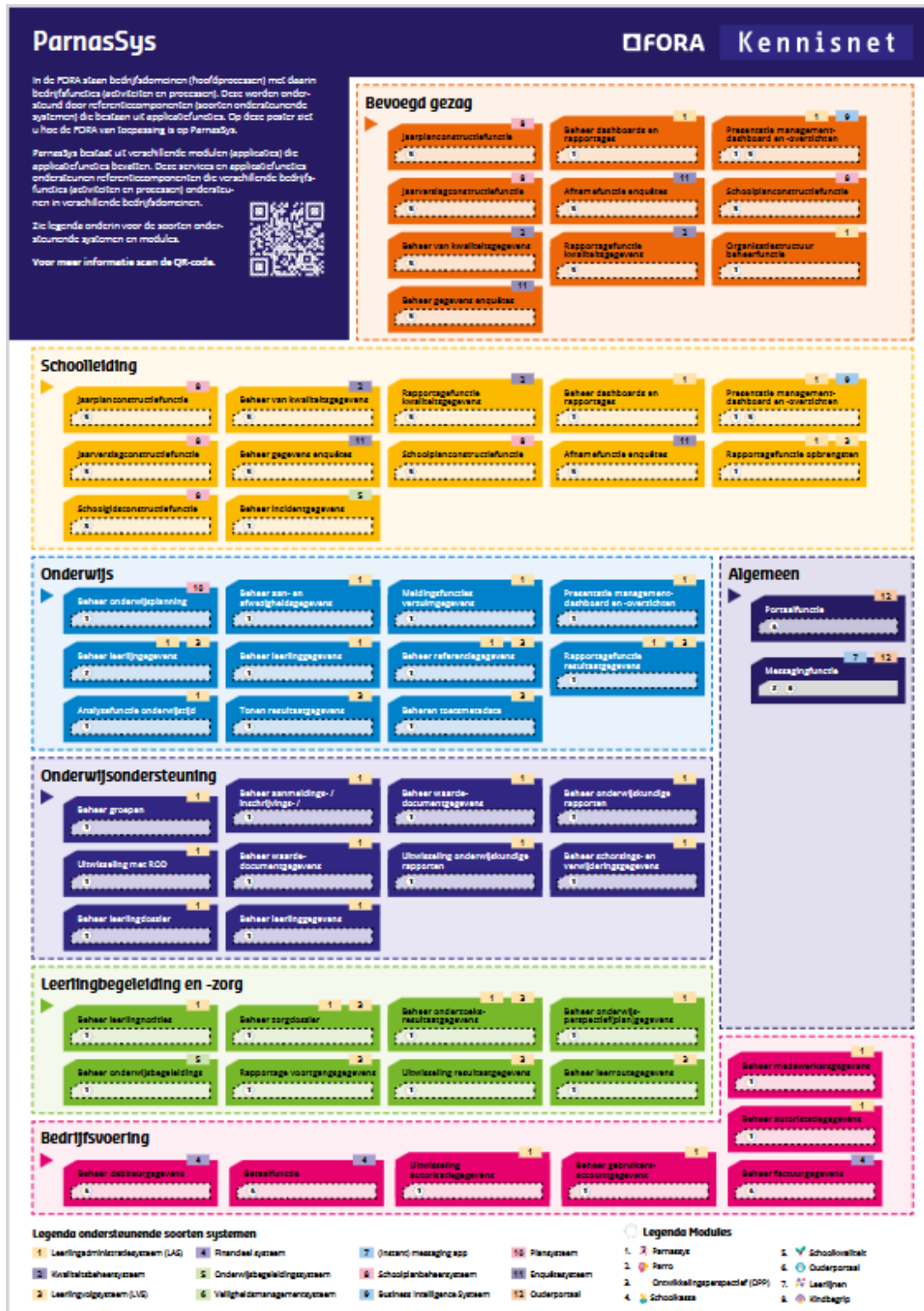
Voor wat betreft Basis van ParnasSys, is door FORA in afstemming met Topicus onderstaande visualisatie gemaakt.

Zie https://fora.wikixl.nl/images/fora/2/29/20221114_ParnasSys_mapping_op_FORA_-_Applicatiefuncties_en_referentiecomponenten_%282022%29.png voor een vergroting van de afbeelding hieronder.



Tevens is door FORA een overzicht gemaakt van alle modules en applicatiefuncties van ParnasSys. Deze services en applicatiefuncties ondersteunen referentiecomponenten die verschillende bedrijfsfuncties (activiteiten en processen) ondersteunen in verschillende bedrijfsdomeinen.

Zie onderstaande afbeelding. Deze DPIA richt zich alleen op: [1] Leerlingadministratiesysteem (LAS), en [3] het Leerlingvolgsysteem (LVS).



Koppelingen

De uitwisseling van persoonsgegevens met externe systemen en processen vindt plaats via (externe) koppelingen, waarvan de beoordeling buiten de scope van deze DPIA valt.

Wél binnen de scope zijn de koppelingsmogelijkheden zelf die vanuit Basis van ParnasSys worden gefaciliteerd.

In Basis van ParnasSys zijn al deze koppelingen inzichtelijk voor applicatiebeheerders, via het beheergedeelte. Hier is te zien welke koppelingen aangeboden worden, kunnen scholen zelf kiezen welke koppelingen men activeert en er is inzichtelijk welke gegevenssets via de koppelingen uitgewisseld worden.

Tevens is er een koppeling mogelijk met Basispoort. Basispoort is de toegangspoort om de toegang tot online lesmateriaal zo eenvoudig mogelijk te maken. Indien hier gebruik van wordt gemaakt (na toestemming van de onderwijsinstelling), verstuurt ParnasSys leerlinggegevens naar Basispoort en Basispoort geeft deze vervolgens door aan alle aangesloten (toetsuitgever)systemen. Voor Basispoort is het gebruik van een autorisatiesleutel sterk aan te raden. Een autorisatiesleutel zorgt ervoor dat de koppeling met Basispoort veiliger is. De koppeling met Basispoort valt verder buiten de scope van deze DPIA.

De toegang tot ParnasSys kan beveiligd worden via het instellen van 2FA. Dit kan door de onderwijsinstelling als 'default' setting worden ingesteld. ParnasSys biedt dit niet zelf als 'default setting' aan. Daarnaast kan een beveiligde inlog via 'Single Sign On' (SSO) worden ingericht via een inlogkoppeling met Microsoft/SSO of Google/SSO, en de HR koppeling. Zie: <https://www.parnassys.nl/oplossingen/hr-koppeling>.

Veel schoolbesturen maken gebruik van een Microsoft- of Google omgeving. Medewerkers moeten hier ook op inloggen. De HR-koppeling maakt het mogelijk om met behulp van de Microsoft- of Google accounts geautomatiseerd ParnasSys accounts aan te maken, dan wel – bij uitdiensttreding - de toegang van een medewerker tot Basis van ParnasSys geautomatiseerd te sluiten. Hierdoor is het eveneens mogelijk dat medewerkers met het Microsoft- of Google account in Basis van ParnasSys kunnen inloggen. Op deze wijze is het ook mogelijk om via de SSO (Single Sign On) 2FA/MFA toe te passen en af te dwingen bij gebruikers. Dit verhoogt het niveau van beveiligde en gecontroleerde toegang.

4. Verwerkingsdoeleinden

De AVG heeft het uitgangspunt dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijke voorwaarde om te kunnen beoordelen of de gegevensverwerkingen rechtmatig zijn en om vast te stellen welke maatregelen getroffen dienen te worden om de risico's te voorkomen of te verkleinen.

De FORA¹⁷ is gebruikt om de verwerkingsdoeleinden te bepalen.

De verwerkingsdoeleinden sluiten aan bij de in het Privacyconvenant¹⁸ opgenomen verwerkingsdoeleinden.

Hieronder zijn de verwerkingsdoeleinden schematisch weergegeven en gekoppeld aan de verwerking.

Doeleinde	Code ¹⁹	FORA – hoofdproces (3. Gegevensverwerkingen)	FORA – subproces Toelichting
de opslag van leer- en toetsresultaten;	D1	Onderwijsevaluatie	Resultatenregistratie Beoordeling
het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten;	D2	Onderwijsevaluatie	Resultatenregistratie Beoordeling
de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer;	D3	Leerlingbegeleiding	Monitoring en begeleiding voortgang leerroute en leerproces Onderwijsbegeleiding Voortgang- en resultatenweergave Leerroudebijstelling
analyse en interpretatie van leer- en toetsresultaten;	D4	Leerlingbegeleiding	Monitoring en begeleiding voortgang leerroute en leerproces
het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen;	D5	Onderwijsevaluatie. Leerlingbegeleiding	Resultatenregistratie. Monitoring en begeleiding voortgang leerroute en leerproces
de indeling en aanpassing van roosters	D6	Onderwijsvoorbereiding	Planning en roostering
het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;	D7	Zorgbegeleiding en -coördinatie. Leerlingbegeleiding	Vorming zorgdossier Onderwijsbegeleiding
het begeleiden en ondersteunen van leerkrachten/docenten en andere medewerkers binnen de Onderwijsinstelling;	D8	Personeel en organisatie (niet van toepassing op Basis van ParnasSys)	
de communicatie met Onderwijsdeelnemers en ouders en met medewerkers van de Onderwijsinstelling;	D9	Facilitering leerlingcommunicatie. Facilitering oudercommunicatie. Samenwerken en communiceren medewerkers en extern	

¹⁷ <https://fora.wikixl.nl/index.php/Hoofdpagina> en <https://fora.wikixl.nl/index.php/DPIA>.

¹⁸ <https://www.privacyconvenant.nl/downloads>.

¹⁹ [Variant-modelbijlage-1-bij-model-verwerkersovereenkomst-4_0.docx](#).

monitoring en verantwoording, met name ten behoeve van: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vormen) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;	D10	Verantwoording	
het voor zover noodzakelijk en wettelijk toegestaan uitwisselen van Persoonsgegevens met Derden, waaronder:	D11		
o toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;	D11	Leerlingbegeleiding en -zorg. Instroom, doorstroom, uitstroom	Organisatie passend onderwijs. Zorgbegeleiding en -coördinatie. Inschrijving en leerlinggegevensbeheer
o samenwerkingsverbanden in het kader van passend onderwijs en regionale samenwerkingen;	D11	Leerlingbegeleiding en -zorg. Onderwijsondersteuning	Organisatie passend onderwijs. Zorgbegeleiding en -coördinatie
o partijen betrokken bij de invulling van stage- of leer-werkplekken;	D11	Leerlingbegeleiding	
o het leveren van Persoonsgegevens aan Onderwijsinstellingen in geval van overstappen tussen Onderwijsinstellingen en bij vervolgonderwijs;	D11	Instroom, doorstroom, uitstroom	Overstap
o het in opdracht van de Onderwijsinstelling leveren van Persoonsgegevens aan een andere partij;	D11	Onderwijsondersteuning. Instroom, doorstroom, uitstroom	Inschrijving en leerlinggegevensbeheer
het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;	D12	Inkoop en contractbeheer. Ict-ondersteuning. Onderwijsuitvoering.	Inkoop. Beheer ict-middelen. (Toegang tot) aanbod leermateriaal
het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;	D13	Onderwijsuitvoering. Ict-ondersteuning	(Toegang tot) aanbod leermateriaal. Beheer identiteiten. Authenticatie en autorisatie
de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens;	D14	Informatiebeveiliging en privacy	
de continuïteit, verbetering en goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning;	D15	Ict-ondersteuning (Inkoop en contractbeheer)	Beheer ict-middelen (Contractbeheer)

het door de Onderwijsinstelling beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek;	D16	Onderwijsevaluatie. Onderwijsvoorbereiding. Beleid en planning	Opleidingontwikkeling. Materiaalontwikkeling
het door de Onderwijsinstelling voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren;	D17	Beleid en planning	Kwaliteitszorg
het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen;	D18	Instroom, doorstroom, uitstroom	Inschrijving en leerlinggegevensbeheer
het behandelen van geschillen;	D18	Klachten en bezwaren (niet van toepassing op Basis van ParnasSys)	Registratie klachten en bezwaren. Klachtbehandeling
financieel beheer;	D20	Financieel beheer en bekostiging (niet van toepassing op Basis van ParnasSys)	
de uitvoering of toepassing van een Unierechtelijke of lidstaatrechtelijke wettelijke bepaling of regeling;	D21		
andere doeleinden ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces) en het begeleiden en volgen van Onderwijsdeelnemers (in hun leerproces), namelijk het kunnen inschrijven en plaatsen van leerlingen.	D22	Zelf invullen door de onderwijsinstelling aan de hand van FORA-bedrijfsfuncties	

5. Betrokken partijen

De hieronder genoemde partijen zijn betrokken bij de gegevensverwerkingen.

Dit overzicht is gebaseerd op de informatie van de privacybijsluiter van ParnasSys, www.parnassys.nl/juridisch/privacybijsluiter.

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens	Verstrekker of ontvanger	De volgende personen hebben toegang tot deze pgg
Onderwijsinstelling	Verwerkings-verantwoordelijke	Beheer en toepassing van het digitaal onderwijsmiddel	Alle genoemde persoonsgegevens	Verstrekker	Directie, schoolleiders, leerkrachten, administratief medewerkers, ICT-en applicatiebeheerders, Intern

					begeleiders, zorgcoördinatoren en externe specialisten.
DUO/ROD	Andere Verantwoordelijke (derde)	DUO Register Onderwijsdeelnemers (ROD). Het Register Onderwijsdeelnemers (ROD) bevat leerlinggegevens van het basisonderwijs, voortgezet onderwijs, middelbaar beroepsonderwijs (mbo) en hoger onderwijs. De Dienst Uitvoering Onderwijs (Rijksoverheid) registreert beleids- en bekostigingsgegevens. ParnasSys is gekoppeld met o.a. de ROD.	Leerling-gegevens	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Onderwijsinspectie	Andere Verantwoordelijke (derde)	De Onderwijsinspectie (Rijksoverheid) heeft geen directe koppeling, maar krijgt wel gegevens aangeleverd en zo nodig toegang tot ParnasSys ten behoeve van onderwijs toezicht.	Mogelijk: alle gegevens in de database	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Samenwerkingsverband Passend Onderwijs	Andere Verantwoordelijke (derde)	Samenwerkingsverbanden Passend Onderwijs ontvangen gegevens uit ParnasSys, vaak via een gezamenlijke informatievoorziening, zoals Kindkans of OnderwijsTransparant.	Relevante gegevens in het kader van de begeleiding en zorg van leerlingen en nadere ondersteuning	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Gemeente	Andere Verantwoordelijke (derde)	Gezondheidsdiensten (GGD/JGZ) van de gemeente en leerplichtambtenaren ontvangen gegevens over de plaatsing en aan- of afwezigheid van leerlingen.	Plaatsing en aan/afwezigheid van leerlingen	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Hulp- of zorgverleners	Andere Verantwoordelijke (derde)	Het kan hierbij gaan om bijvoorbeeld orthopedagogen, schoolmaatschappelijk werkers of logopedisten die al dan niet in dienst van de school gegevens verwerken.	Noodzakelijke gegevens (inzake de gezondheid en / of begeleiding)	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Kennisnet	Andere Verantwoordelijke	Kennisnet levert de Overstap Service Onderwijs (OSO) waarmee het leerlingdossier uitgewisseld kan worden met een andere LAS (in het PO en VO). Ook levert Kennisnet het ECK iD (pseudo-ID) aan bij het LAS via de Nummervoorziening	Onderwijskundig rapport en eventuele noodzakelijke persoonsgegevens voor de goede begeleiding en zorg omtrent leerlingen	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Uitgeverijen en Leveranciers van digitaal leermateriaal, LVS-systemen of leerplatformen (optioneel)	Andere Verantwoordelijke (derde)	Uitgeverijen ontvangen via Basispoort, een centrale voorziening voor toegang tot leermiddelen, gegevens. Daarnaast zijn er rechtstreekse koppelingen met leveranciers van	Noodzakelijke gegevens voor de toegang verlening en het functioneren	Ontvanger	Geen toegang tot de persoonsgegevens in de database.

		leerlingvolgsystemen en leerplatformen.	van leermiddelen		
Topicus Education B.V. / ParnasSys	Verwerker	Aanbieder digitaal onderwijsmiddel	Alle genoemde persoonsgegevens	Ontvanger	Binnen Topicus is een autorisatiematrix vastgesteld waarbij toegang op basis van 'need to know' toegang wordt verkregen. De systeembeheerder heeft geen toegang tot de persoonsgegevens in de database, tenzij dit gebeurt op verzoek van de onderwijsinstelling. Dan wordt volgens geldende support/beveiligingsprocessen gewerkt.
Previder	Subverwerker Land van opslag/verwerking: Nederland Vestigingsland: Nederland	Verzorgt de opslag van de applicatie en de data die met behulp van ParnasSys en bijbehorende modules wordt verwerkt.	Alle genoemde persoonsgegevens	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
ActiveCampaign (Postmark, voorheen Wildbit)	Subverwerker Land van opslag/verwerking: Verenigde Staten Vestigingsland: Verenigde Staten	Verzorgt de verzending van e-mails vanuit Basis van ParnasSys.	Contactgegevens	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Hubspot	Subverwerker Land van opslag/verwerking: Duitsland Vestigingsland: Ierland	Verzorgt de verzending van serviceberichten.	Contactgegevens van medewerkers	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Zendesk	Subverwerker Land van opslag/verwerking: Duitsland en Ierland Vestigingsland: Verenigde Staten	Systeem dat de servicedesk gebruikt voor het registreren van vragen van gebruikers.	Contactgegevens van medewerkers	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Carry Technologies (Hightouch)	Subverwerker Land van opslag/verwerking: Ierland Vestigingsland: Verenigde Staten	Ondersteunt bij het bundelen van gegevens voor het versturen van serviceberichten.	Contactgegevens van organisatiebeheerder en contactpersonen ParnasSys	ontvanger	Geen toegang tot de persoonsgegevens in de database.

Cloudflare	Subverwerker Land van opslag/verwerking: Nederland, Duitsland Vestigingsland: Verenigde Staten	Verzorgt de Web Application Firewall om veelvoorkomende webapplicatie aanvallen op ParnasSys te detecteren en voorkomen.	IP-adressen en diagnostische gegevens	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Medewerkers	Betrokkene / geautoriseerde	Medewerkers, over het algemeen betreft dit de schoolleiding, IB-er en de leerkrachten incl. de invallers voor langere duur.	Noodzakelijke persoonsgegevens op basis van 'need to know' en 'least privilege'.	Betrokkene / geautoriseerde	Binnen de onderwijsinstelling is een autorisatiematrix vastgesteld waarbij toegang op basis van 'need to know' toegang wordt verkregen.
Ouders/verzorgers	Betrokkene	Ouders/verzorgers van de ingeschreven leerlingen. Het kan soms ook gaan om een voogd. Of om de contactgegevens van familie, kennissen van het kind in geval van nood.	Noodzakelijke persoonsgegevens	Betrokkene	Ouders/verzorgers
Leerlingen (incl aspiranten en oud-leerlingen)	Betrokkene	Onderwijsdeelnemers die zijn ingeschreven. Het kan ook gaan om de gegevens van oud-leerlingen in het kader van bewaarplicht of alumni-activiteiten.	Alle gegevens	Betrokkene	Betrokkene
Stagiaires	Betrokkene / geautoriseerde	Bijvoorbeeld studenten die voor langere tijd aan de school zijn verbonden.	Noodzakelijke persoonsgegevens op basis van 'need to know' en 'least privilege'.	Betrokkene / geautoriseerde	Binnen de onderwijsinstelling is een autorisatiematrix vastgesteld waarbij toegang op basis van 'need to know' toegang wordt verkregen.

6. Belangen bij de gegevensverwerking

De onderwijsinstelling (verwerkingsverantwoordelijke) heeft belang bij een goed werkend en betrouwbaar digitaal LAS/LVS, waardoor zij de leerlingadministratie optimaal kan inrichten en, doordat het inzicht geeft in de ontwikkeling van leerlingen, het onderwijs kan analyseren en concrete (verbeter)plannen kan opstellen.

De belangen die Topicus (verwerker) en haar subverwerkers hebben, zijn het leveren aan onderwijsinstellingen van een goed werkend digitaal LAS/LVS. Daarnaast hebben zij ook een commercieel belang; een goed werkend product levert financieel voordeel op en het ondersteunt een goede reputatie en marktpositie.

Naam partij	Belangen
Onderwijsinstelling	Het hebben van een goed werkend en betrouwbaar digitaal leerlingvolg- en administratie systeem.
DUO/ROD	Het via ROD uitwisselen door onderwijsinstellingen van gegevens van leerlingen en studenten uit met DUO, zoals inschrijvingen en diplomagegevens.

Onderwijsinspectie	Toezicht kunnen houden op de kwaliteit van het onderwijs.
Samenwerkingsverband Passend Onderwijs	Wettelijke taak uit kunnen voeren inzake passend onderwijs en juiste ondersteuning van de leerling.
Gemeente	Het kunnen uitvoeren van de wettelijke taak van gezondheidsdiensten (GGD/JGZ) van de gemeente en leerplichtambtenaren door gegevens te ontvangen over de plaatsing en aan- of afwezigheid van leerlingen.
Hulp- of zorgverleners	Zorgplicht en ondersteuning uit kunnen voeren, evenals juiste begeleiding van de leerling.
Kennisnet	Leveren van de Overstap Service Onderwijs (OSO) waarmee het leerlingdossier uitgewisseld kan worden met een andere LAS (in het PO en VO). Ook levert Kennisnet het ECK iD (pseudo-ID) aan bij het LAS via de Nummervoorziening
Uitgeverijen en Leveranciers van digitaal leermateriaal, LVS-systemen of leerplatformen (optioneel)	Leveren van gegevens aan uitgeverijen via Basispoort, een centrale voorziening voor toegang tot leermiddelen. Idem in geval van rechtstreekse koppelingen met leveranciers van leerlingvolgsystemen en leerplatformen.
Topicus Education B.V. / ParnasSys	Het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Previder	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
ActiveCampaign (Postmark, voorheen Wildbit)	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Hubspot	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Zendesk	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Carry Technologies (Hightouch)	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Cloudfare	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Medewerkers	Toegang kunnen hebben tot relevante gegevens voor het uitvoeren van hun onderwijstaken en begeleiding van leerlingen.
Ouders/verzorgers	Inzicht kunnen hebben in de voortgang en ontwikkeling van hun kind, communicatie met school en toegang tot relevante gegevens.
Leerlingen (incl aspirant- en oud-leerlingen)	Het ontvangen van gepersonaliseerd onderwijs, inzicht in eigen leerresultaten en begeleiding tijdens de schoolloopbaan.
Stagiaires	Praktijkervaring kunnen opdoen binnen een onderwijsomgeving door toegang tot relevante gegevens onder toezicht van bevoegde medewerkers.

7. Verwerkingslocaties

De gegevensverwerkingen vinden plaats op de volgende locaties.

Naam partij	Statutaire vestigings-plaats (sub-) verwerker	Beknpte omschrijving taak/dienst waaruit blijkt welke informatie wordt verwerkt door deze subverwerker	Plaats/land van opslag en verwerking persoonsgegevens en doorgifte mechanisme indien buiten de EER
Topicus Education B.V. / ParnasSys	Deventer (NL)	Leverancier/verwerker	Nederland
Previder	Hengelo (NL)	Subverwerker	Nederland
ActiveCampaign	Chicago (VS) Global headquarter	Subverwerker	Verenigde staten. Aangesloten bij het EU-US Data Privacy Framework
Hubspot	Cambridge (VS) Global headquarter	Subverwerker	Duitsland. Aangesloten bij het EU-US Data Privacy Framework en borging middels SCC en Data Processing Agreements
Zendesk	San Francisco (VS) Global headquarter	Subverwerker	Duitsland en Ierland. Aangesloten bij het EU-US Data Privacy Framework en borging middels SCC en Data Processing Agreements

Carry Technologies (Hightouch)	San Francisco (VS) Global headquarter	Subverwerker	Ierland. Aangesloten bij het EU-US Data Privacy Framework en borging middels SCC en Data Processing Agreements
Cloudflare	San Francisco (VS) Global headquarter	Subverwerker	Nederland, Duitsland. Aangesloten bij het EU-US Data Privacy Framework en borging middels SCC en Data Processing Agreements

8. Data Transfer Impact Assessment (DTIA)

De AVG bevat specifieke regels voor de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER). In beginsel mogen persoonsgegevens alleen worden overgedragen aan landen buiten de EER als het land een ‘passend beschermingsniveau’ heeft. Dat niveau kan op verschillende manieren worden bepaald: een multinational kan bindende bedrijfsvoorschriften vaststellen (BCR’s), de EU-standaardcontractbepalingen (SCC) toepassen of alleen overdragen aan landen waarvoor de Europese Commissie een zogeheten adequaatheidsbesluit²⁰ heeft genomen.

Topicus maakt voor Basis van ParnasSys gebruik van subverwerkers, zowel gevestigd binnen als buiten de EER. De subverwerkers die buiten de EER zijn gevestigd, vallen allemaal onder het adequaatheidsbesluit dat is uitgevaardigd door de Europese Commissie, zoals het EU-US Data Privacy Framework (EU-US DPF) (situatie juni 2025). Hierdoor is Topicus niet verplicht om een DTIA uit te voeren op haar subverwerkers.

Hoewel het EU-US DPF als ‘adequaats’ is aangemerkt door de Europese Commissie, is dit politiek en juridisch omstreden. Daarom adviseert SIVON om, daar waar nog niet gerealiseerd, met (sub)verwerkers SCC's overeen te komen.

9. Technieken en methoden van gegevensverwerking

Artikel 32 van de AVG schrijft voor dat er passende technische en organisatorische maatregelen genomen moeten worden om een op het risico afgestemd beveiligingsniveau te waarborgen. Om inzicht te krijgen in welke mate er vorm wordt gegeven aan deze abstracte formulering wordt gebruik gemaakt van de voor de verwerkers opgestelde standaard DPIA-vragenlijst. Deze vragenlijst is door de verwerker (Topicus) ingevuld en geeft voor een belangrijk deel inzicht in o.a. de genomen technische beheersmaatregelen en informatiebeveiliging. Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende risico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, AI/algorithmes, cloud, nieuwe technologie, profilering en big dataverwerkingen. Topicus voert voor wat betreft ParnasSys geen (semi-)geautomatiseerde besluitvorming toe, maakt binnen ParnasSys geen gebruik van AI/algorithmes of nieuwe technologieën, noch big dataverwerkingen. Voor wat betreft ‘profilering’ en het verwerken van bijzondere persoonsgegevens (gegevens betreffende de

²⁰ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

gezondheid) zijn voor deze DPIA de beveiligingsmaatregelen in beeld gebracht, waaronder bijvoorbeeld de encryptie op twee lagen.

Informatiebeveiliging

- Topicus beschikt voor de gegevensverwerking via het systeem ParnasSys over een ISO 27001-2023/A1:2024 certificaat dat geldig is tot 13 maart 2028. SIVON heeft het certificaat en de verklaring van toepasselijkheid beoordeeld en akkoord bevonden.
- Volgend uit deze ISO 27001 certificering, beschikt Topicus voor wat betreft ParnasSys ook over een werkend ISMS (Information Security Management Systeem). Documentatie m.b.t. het uitvoeren van risicoanalyses en behandelingen/beoordelingen staat beschreven in het ISMS en wordt dit jaar (2025) uitgebreid door het toevoegen van specifieke risicoanalyses.
- Binnen het onderwijsveld wordt daarnaast gebruikt gemaakt van het ROSA²¹ certificeringsschema. Door het bepalen van de BIV-classificatie (laag/midden/hoog) voor de onderdelen ‘Beschikbaarheid’, ‘Integriteit’ en ‘Vertrouwelijkheid’ worden de daarop van toepassing zijnde beheersmaatregelen inzichtelijk. De ROSA-rapportage is een onderdeel van de beveiligingsbijlage van de verwerkersovereenkomst.

Ook voor Basis van ParnasSys is het ROSA-certificeringsschema gebruikt. In wederzijds overleg is het BIV-niveau bepaald (Hoog-Hoog-Hoog), wat betekent dat voor alle onderdelen het hoogste niveau van beveiligingsmaatregelen van toepassing is. Over het algemeen geeft Topicus aan dat is ‘voldaan’ aan de bijbehorende maatregel. In enkele gevallen is er een alternatieve maatregel in het ROSA schema opgenomen.

Vervolgens heeft SIVON de BIV-classificatie beoordeeld en gecontroleerd of de daadwerkelijk genomen beheersmaatregelen in overeenstemming zijn met deze classificatie.

Uit deze beoordeling zijn de volgende punten naar voren gekomen:

Voor wat betreft de categorie **‘Beschikbaarheid’** geeft Topicus aan dat volledig wordt voldaan aan de eisen van het ROSA-certificeringsschema.

Voor wat betreft de categorie **‘Integriteit’** wordt ook voldaan aan de vereisten. In het ROSA schema d.d. 7 april 2025 was nog aangegeven dat voor de onderwerpen Onweerlegbaarheid en Onweerlegbaarheid (toepassing) alternatieve maatregelen van kracht waren, maar gedurende het DPIA-traject heeft Topicus bevestigd dat zij aan de vereiste maatregelen voldoet.

²¹ Zie: https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-v3-0/.

Voor wat betreft de categorie ‘**Vertrouwelijkheid**’ wordt op de meeste onderdelen aangegeven dat Topicus voldoet aan de beheersmaatregel. Voor het onderdeel ‘Transport en fysieke opslag’ en ‘Logging’ wordt aangegeven dat er sprake is van een alternatieve maatregel.

ROSA vereisten	Alternatieve maatregel opgenomen door Topicus Education B.V.
Transport en fysieke opslag	
Encryptie van transport (zowel voor intern als extern verkeer) is conform de Uniforme Beveiligingsvoorschriften (UBV) TLS van Edustandaard. Encryptie van opslag, moet minimaal op twee niveaus, zoals op (virtuele)disk en bestands- of recordniveau. Hiervoor wordt gebruik gemaakt van richtlijnen/best practices/standaarden, zoals van NCSC, ENISA, NIST.	<i>Zie bijgeleverd document: Versleuteling Data ParnasSys 03-2025</i> <i>(opgenomen als <u>bijlage 3</u> bij deze DPIA)</i>
ROSA vereisten	Alternatieve maatregel opgenomen door Topicus Education B.V.
Logging	
Toegang tot de applicatie (zowel gelukt als mislukt) en lezen van (persoons)gegevens wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen (op basis van autorisatie) en toegang ertoe wordt apart gelogd. Beide logging wordt regelmatig gecontroleerd op uitzonderingen op toegang en uitzonderlijke patronen in gebruik. Bijvoorbeeld door automatische loganalysetooling.	• <i>Het inloggen en het benaderen van persoonsgegevens in de applicatie wordt gelogd.</i> • <i>Het inzien van dit log is apart te autoriseren.</i> • <i>Er vindt geen automatische loganalyse plaats op de logging van de klant.</i> • <i>Het inloggen, activeren en geven van toegang via een IAM wordt gelogd.</i>

Met betrekking tot ‘Transport en fysieke opslag’ wordt op dit moment niet voldaan aan de beveiligingsmaatregel van encryptie op twee niveaus (zowel op de virtuele schijf als op recordniveau). Het risico hierbij is dat data, wanneer deze (on)bedoeld door bevoegden en onbevoegden benaderd worden, leesbaar is. Topicus heeft gedurende het DPIA-traject toegezegd om de encryptie op twee lagen te gaan toepassen. Dit maakt extra beveiliging en het beschermen op basis van de classificatie van gegevens mogelijk.

Met betrekking tot ‘Logging’: zie hieronder bij toelichting op exportfunctionaliteit.

- Naast het onderzoeken van de ROSA-vereisten, is beoordeeld hoe **Privacy by Default** wordt nageleefd. Met betrekking tot meerfactor-authenticatie (MFA of 2FA): ParnasSys beschikt over deze optie, echter deze wordt niet *by default* afgedwongen bij gebruikers. Het standpunt van Topicus:

“ParnasSys wijst nieuwe klanten reeds hierop en de impact van invoering zal zeer gering zijn. In praktijk stellen we voor om bestaande scholen beter te informeren en motiveren deze middelen in te schakelen. Dit kan landelijk een groter positief resultaat opleveren.”

Ondanks dat ParnasSys 2FA *by default* niet aanbiedt, kan de onderwijsinstelling dit zelf instellen en afdwingen. Hierop moet door de onderwijsinstelling beleid worden gemaakt, waarbij ook SSO met bijvoorbeeld Office 365 of Google kan worden meegenomen. Er resteert hierdoor geen ‘hoog risico’.

- De exportfunctionaliteit binnen ParnasSys is standaard voor gebruikers beschikbaar, daar zitten geen beperkingen op. Topicus verklaart hierover:

“Wat een gebruiker mag downloaden of exporteren op een pagina is gelijk aan wat deze daar reeds kan inzien of kan overnemen vanuit het beeldscherm zelf. Exporteren is in ParnasSys convenience, geen gatekeeping.”

De applicatiebeheerder van de onderwijsinstelling beschikt op dit moment al over functionaliteit om zelf de logging te monitoren inzake welke gebruiker welke gegevens heeft ingezien (ook waar het bijvoorbeeld gezondheidsgegevens betreft). De onderwijsinstelling heeft echter zelf geen loginformatie over het gebruik van de exportfunctionaliteit en wijziging van cijfers beschikbaar. Hierdoor ontbreekt inzicht in welke gebruiker, welke exports heeft uitgevoerd en is er geen monitoring op afwijkend gedrag met betrekking tot deze functionaliteit en cijferwijzigingen. Topicus biedt op dit moment wel maximale ondersteuning om op verzoek deze logfiles beschikbaar te stellen aan de onderwijsinstelling.

Het Normenkader IBP schrijft echter voor dat de onderwijsinstelling de logging zelfstandig moet kunnen monitoren. Daarnaast gaat ook de ISO 27001-norm ervan uit dat de verwerkingsverantwoordelijke zélf verantwoordelijk is voor de monitoring van loggegevens. Topicus onderkent het nut en de noodzaak hiertoe, en heeft aangegeven de huidige loggegevens die onderwijsinstellingen zelf ter beschikking hebben, uit te gaan breiden.

- Ook is onderzocht in hoeverre admins/beheerders toegang hebben tot de persoonsgegevens, inclusief bijzondere persoonsgegevens. Dit is niet beperkt, zij kunnen in eerste aanleg overal bij. De toelichting van Topicus hierop is:

“In vrijwel alle softwareapplicaties waar een bedrijf of instelling zelf beheer over de applicatie moet kunnen voeren is een admin of beheer account aanwezig voor de klant. De admin/beheerder is de eerste gebruiker in het systeem en heeft het vermogen om alle

andere gebruikers en rollen aan te maken/configureren. Met dit vermogen kan deze zichzelf altijd toegang verschaffen. De rol applicatiebeheerder dient daarom beperkt en weloverwogen toegekend te worden.

Voor veel voorkomende ondersteuningsvragen aan de beheerder is inzicht in het systeem ook gewenst. Het verwijderen van handelingsvermogen uit het admin/beheer account, veroorzaakt dat klanten workarounds gaan toepassen: zoals het aanmaken van accounts met veel te veel rechten. Dit wil ParnasSys niet promoten.

ParnasSys biedt ruim grip en inzicht op het beheeraccount. Tevens, indien een school een bestuur heeft kan het bestuur het instellen en uitdelen van deze rol inperken. Een school moet er altijd naar streven om medewerkers gepaste rollen te geven en gebruik te controleren. Het handelen van de beheerder is te controleren via de aanwezige logs en niet door een beheerder aan te passen of te verwijderen. In ParnasSys de Basis zit alles om dit te doen. Om het monitoren op grote schaal extra te vergemakkelijken bieden we ook speciale tools aan. Dit zal niet voor iedere school relevant zijn.”

Het is daarom van belang dat de onderwijsinstelling hiervoor zelf maatregelen implementeert en monitort, zodat de gebruiksgegevens van admins/beheerders (die brede toegang tot de persoonsgegevens hebben) gecontroleerd worden.

- Op het punt betreffende de jaarlijkse (pen)testen en het hebben van een aantoonbaar gedocumenteerde procedure voor opvolging van de bevindingen hieruit, was in eerste instantie onduidelijkheid. Dit heeft Topicus gedurende het DPIA-traject naar tevredenheid opgelost.
- Datzelfde hebben zij gedaan inzake het aantoonbaar maken van beleid en procedures rondom monitoring en detectie van onrechtmatige toegang tot steppingstones van de database.

In hoofdstuk 19 en 20 worden de risico's en mitigerende maatregelen nader toegelicht.

IAMA: mensenrechten in beeld bij algoritmes

Indien uit voornoemde vragenlijst blijkt dat er gebruik wordt gemaakt van AI technologie zal beoordeeld worden of er sprake is van een hoog risico.

Indien er sprake is van een hoog risico algoritme kan aan de hand van de uitvoering van een Impact Assessment Mensenrechten en Algoritmes ([IAMA](#)) inzichtelijk worden gemaakt of deze voldoet aan de wettelijke verplichtingen en of er sprake is van een verantwoorde inzet van AI en algoritmen.

Binnen de basisfunctionaliteit van ParnasSys wordt geen gebruik gemaakt van AI-technologie. Hierdoor is er geen sprake van een hoog risico algoritme en is het niet vereist om een Impact Assessment Mensenrechten en Algoritmes (IAMA) uit te voeren op ParnasSys.

10. Juridisch en beleidsmatig kader

Hieronder wordt alle wet- en regelgeving benoemd met mogelijke gevolgen voor de gegevensverwerkingen.

De artikelen art. 11 jo. 45b lid 1 van de Wet op het primair onderwijs (WPO), alsmede artikel 8 WPO bieden een solide wettelijke basis voor het verwerken van leerlinggegevens in het primair onderwijs.

Onderwijsinstellingen kunnen zich voor wat betreft het leerlingadministratie en -volgsysteem hierbij primair beroepen op de grondslag *wettelijke verplichting* (artikel 6 lid 1 onder (c) AVG), omdat zij op grond van de WPO (artikel 11 jo.45b lid 1) verplicht zijn de ontwikkeling van leerlingen te monitoren en dit vast te leggen in een leerling- en onderwijsvolgsysteem. Uit artikel 8 lid 1 en 2 WPO volgt dat dit geldt voor zowel de cognitieve als de sociaal-emotionele en creatieve ontwikkeling van leerlingen.

Aanvullend geldt, voor zover bepaalde gegevens niet direct zijn voorgeschreven door een wettelijke verplichting, de grondslag *vervulling van een taak van algemeen belang* (artikel 6 lid 1 onder (e) AVG op basis van onderwijswet- en regelgeving), omdat scholen van overheidswege een publieke taak uitvoeren.

In alle gevallen dient bij de verwerking van persoonsgegevens te worden voldaan aan de kernbeginselen van de AVG, zoals doelbinding, dataminimalisatie en transparantie, om te waarborgen dat de verwerking rechtmatig en behoorlijk plaatsvindt.

De specifieke wettelijke grondslagen zijn verder uitgewerkt in hoofdstuk 12.

11. Bewaartermijnen

Het uitgangspunt is dat de onderwijsinstelling zelf als verwerkingsverantwoordelijke doel en middelen van de verwerking van persoonsgegevens bepaalt, en derhalve tevens verantwoordelijk is voor het vaststellen en nakomen van de bewaartermijnen. Dit uitgangspunt betekent dat een onderwijsinstelling zelf de bewaartermijnen moet kunnen vaststellen en dus ook binnen ParnasSys moet kunnen bepalen en vervolgens ‘*schonen*’ (verwijderen van de persoonsgegevens).

In ParnasSys van toepassing zijnde bewaartermijnen:

Een bewaartermijn van twee (2) jaar (na uitschrijven leerling of beëindiging van de relatie met de medewerker) voor persoonsgegevens die niet onder de uitzonderingscategorie van vijf (5) jaar vallen, in overeenstemming met de huidige wet- en regelgeving en de handleiding bewaartermijnenoverzicht van Kennisnet (*versie januari 2025*)²², alsmede het vernieuwde bewaartermijnenoverzicht (versie 1.1. mei 2024)²³.

²² Zie Kennisnet: [Bewaren en vernietigen van gegevens - Normenkader informatiebeveiliging en privacy voor het onderwijs](#).

²³ Zie Kennisnet: [Bewaren en vernietigen van gegevens - Normenkader informatiebeveiliging en privacy voor het onderwijs](#).

De vijf (5) jaarstermijn is vervolgens van toepassing op:

- Besluit bekostiging WPO 2022²⁴:

Art. 11 Inhoud leerlingenadministratie

1. De directeur van een school draagt er zorg voor dat een overzichtelijke leerlingenadministratie beschikbaar is van:
 - a. de inschrijving, de uitschrijving en het verzuim van de leerlingen op de school;
 - b. de gegevens van de leerlingen en hun ouders die noodzakelijk zijn voor de berekening van de bekostiging; en
 - c. indien het een speciale school voor basisonderwijs betreft, de verklaring bedoeld in artikel 40, achtste lid, van de wet.

Art. 12 Bewaren gegevens

1. De gegevens, bedoeld in artikel 11, worden in ieder geval gedurende vijf jaar nadat de desbetreffende leerling van de school is uitgeschreven in de leerlingenadministratie bewaard.

- Besluit uitwisseling leer- en begeleidingsgegevens²⁵:

Art. 7a. Bewaartermijn

Het onderwijskundig rapport (OKR) wordt bewaard tot vijf jaar na uitschrijving van de leerling. Ook het ontwikkelingsperspectief (OPP – indien van toepassing), eindtoets en schooladvies maken onderdeel uit van OKR.

Een eventueel zorgdossier (meestal niet in ParnasSys, maar er zijn scholen die het zorgdossier wel in ParnasSys zetten) mag volgens art. 30 Uitvoeringswet AVG verwerkt worden, maar moet ook na 2 jaar na verlaten school verwijderd worden.

N.B.: totdat de sectorale selectielijsten voor po en vo zijn vastgesteld, is het advies aan de scholen gegeven om géén informatie en documentatie te vernietigen rondom

- vrijstellingen van de Leerplichtwet, en
- diploma's en (eindexamen)cijferlijsten.

Bovenstaande analyse is in lijn met de bekende wet- en regelgeving en richtlijnen vanuit het onderwijs. Hierbij moet wel rekening worden gehouden met mogelijke, door ons niet voorziene aanpassingen.

²⁴ [wetten.nl - Regeling - Besluit bekostiging WPO 2022 - BWBR0046159](#).

²⁵ [wetten.nl - Regeling - Besluit uitwisseling leer- en begeleidingsgegevens - BWBR0031619](#)

De specifieke bewaartermijnen worden bepaald door de onderwijsinstelling als de verwerkingsverantwoordelijke, in overeenstemming met de bewaartermijnen in het onderwijs, zoals hierboven weergegeven.

ParnasSys biedt een functionaliteit aan om **leerlinggegevens** te verwijderen. Het is echter de verantwoordelijkheid van de school om zowel de bewaartermijnen te bewaken als daadwerkelijk de gegevens te verwijderen. Het systeem is niet geautomatiseerd voor deze taken.

In het scherm 'leerlinggegevens verwijderen' kan men filters kiezen voor twee 'wettelijke bewaartermijnen'. Na uitschrijving van een leerling moeten gegevens in twee fases worden verwijderd, namelijk twee jaar na de uitschrijving van de leerling en vijf jaar na de uitschrijving. Dit ziet er als volgt uit:

- Tot 2 jaar nadat een leerling de school heeft verlaten mogen gegevens bewaard blijven. Na deze periode wordt door middel van een specifieke verwijderactie binnen ParnasSys alle toetsresultaten, vragenlijsten en documenten verwijderd. Enkel de volgende gegevens worden hierna in het leerlingdossier bewaard:
 - de gegevens onder *Personalia* > *Personalia*
 - de gegevens onder *Personalia* > *Gezin*
 - de gegevens onder *Onderwijs* > *Voorgeschiedenis* (behalve *Vroegschoolse programma's*)
 - de gegevens onder *Onderwijs* > *Deze school*
 - de gegevens onder *Onderwijs* > *Vervolgonderwijs*
 - de gegevens onder *Onderwijs* > *Absentie*
 - de gegevens onder *Onderwijs* > *Overstapdossier klaarzetten* (ook beschikbaar onder *School* > *OSO* > *Overstapdossiers klaarzetten*)
 - de gegevens onder *Onderwijs* > *Passend onderwijs*
 - de gegevens onder *Toetsen* > *Doorstroomtoetsen*
 - de PDF van het OSO-dossier is *Map* > *Documenten*
- Tot 5 jaar nadat een leerling de school heeft verlaten moeten gegevens over verzuim en in- en uitschrijving bewaard blijven. Na deze periode wordt door middel van een specifieke verwijderactie het gehele leerlingdossier verwijderd en deze handeling kan niet meer worden teruggedraaid, zelfs niet via een restore van een back-up.
- Tot 5 jaar nadat een leerling de school heeft verlaten moet OKR bewaard blijven. Na deze periode wordt door middel van een specifieke verwijderactie het gehele leerlingdossier verwijderd en deze handeling kan niet meer worden teruggedraaid, zelfs niet via een restore van een back-up.

Opmerking

Wanneer een leerlingdossier wordt verwijderd, blijven de groepsgegevens (zoals groepsplannen, bestanden, notities en sociogrammen) van de groepen waarin deze

leerling onderwijs heeft gevolgd behouden in ParnasSys. Deze groepsgegevens kunnen echter handmatig worden verwijderd.

Naar analogie van art. 7 lid 5 Vrijstellingsbesluit Wbp (vervallen) zijn op de persoonsgegevens van **leerkrachten** die binnen ParnasSys worden verwerkt de volgende bewaartermijnen van toepassing:

‘De persoonsgegevens worden verwijderd uiterlijk twee jaren nadat het dienstverband of de werkzaamheden van de betrokkene ten behoeve van de verantwoordelijke zijn beëindigd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.’

Bij vertrek van medewerkers worden hun gegevens meestal gedeactiveerd maar niet verwijderd. Dit is omdat het belangrijk is om te kunnen traceren wie verantwoordelijk was voor bepaalde groepen, wie notities heeft gemaakt bij een leerling, of wie bepaalde documenten heeft aangemaakt. Om deze reden worden de gegevens van medewerkers bewaard voor de gehele schoolperiode van een leerling.

Daarnaast worden binnen ParnasSys persoonsgegevens van **ouders/verzorgers** verwerkt. Deze gegevens worden na 5 jaar definitief verwijderd, tegelijk met het verwijderen van het leerlingdossier.

Beëindiging contract ParnasSys

Na afloop van het contract zullen de gegevens volgens de bepalingen van de verwerkersovereenkomst worden verwijderd en op verzoek overgedragen aan de onderwijsinstelling. Deze regeling voor verwijdering is ook van toepassing op de gegevens die zijn verkregen door subverwerkers.

Back-up

De back-ups van gegevens worden dagelijks volledig overschreven waardoor de wettelijke bewaartermijnen worden toegepast.

6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen

In dit hoofdstuk wordt de rechtmatigheid van de gegevensverwerkingen beoordeeld. Het gaat om de rechtsgrond, noodzakelijkheid (proportionaliteit en subsidiariteit) en doelbinding, transparantie van de leverancier over de voorgenomen gegevensverwerkingen en de rechten van de betrokkene.

12. Rechtsgrond

Als onderdeel van de verantwoordingsplicht dient te worden aangetoond dat de verwerking van persoonsgegevens op een rechtmatige grondslag berust. Deze grondslag moet worden bepaald voordat de onderwijsinstelling begint met het verwerken van persoonsgegevens.

Artikel 6 AVG kent 6 grondslagen:

- a) Toestemming van de betrokkene (art.6, eerste lid, sub a, AVG)
- b) Uitvoering van een overeenkomst (art.6, eerste lid, sub b, AVG)
- c) Wettelijke verplichting²⁶(art.6, eerste lid, sub c, AVG)
- d) Vitaal belang van de betrokkene (art.6, eerste lid, sub d, AVG)
- e) Taak van algemeen belang²⁷ (of openbaar gezag) (art.6, eerste lid, sub e, AVG)
- f) Gerechtvaardigd belang (art. 6, eerste lid, sub f, AVG)

Zie voor een overzicht van de grondslagen tevens Hoofdstuk 10, het Juridisch en Beleidsmatig kader. In die *'Juridische paragraaf'* wordt uiteengezet wat de wettelijke grondslag is voor de verwerking van persoonsgegevens in het LAS/LVS ParnasSys.

ParnasSys is een gecombineerd leerlingadministratie én -volgsysteem (LAS en LVS) dat fungeert als centrale administratiesysteem voor onderwijsinstellingen in het primair onderwijs. Met ParnasSys is het mogelijk voor een onderwijsinstelling om gemakkelijk de leerlingadministratie te beheren én inzicht te krijgen in leerlingprestaties, met als doel de onderwijskwaliteit te verbeteren. Basis van ParnasSys kan worden uitgebreid met aanvullende modules op gebieden zoals oudercommunicatie, beleidsvorming, en ontwikkeling.²⁸ De scope van deze DPIA op ParnasSys richt zich enkel op de basisversie van ParnasSys, daarbij wordt alleen de functionaliteit voor een LAS en LVS onderzocht.

Het verwerken van persoonsgegevens via Basis van ParnasSys is geen doel op zich. Het doel is het administreren en volgen van onderwijsdeelnemers. Er is dus geen grondslag vereist

²⁶ De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn.

²⁷ Met betrekking tot rechtsgrond taak van algemeen belang geldt dat deze taak moet blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak persoonsgegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak ook worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

²⁸ <https://www.parnassys.nl/oplossingen/de-basis>.

voor het gebruik van Basis van ParnasSys als applicatie²⁹, er dient wel een grondslag te zijn voor het verwerken van de persoonsgegevens zelf. Daarnaast zullen we in deze paragraaf zien dat er een wettelijke plicht is voor een onderwijsinstelling om een *leerling- en onderwijsvolgsysteem* te gebruiken.

In de volgende paragrafen worden de verwerkingsgrondslagen van enkele onderdelen toegelicht, opgesplitst per categorie van betrokkenen.

1. Leerlingen

Leerlingvolgsysteem (LVS)

De rechtsgrond voor de verwerking van persoonsgegevens die inzicht geeft in de voortgang van kennis en vaardigheden op het niveau van de leerling, de groep en de school binnen een leerling- en onderwijsvolgsysteem, is een wettelijke plicht (artikel 6 lid 1 sub c AVG). Op grond van art. 11 jo. 45b lid 1 van de Wet op het Primair Onderwijs (WPO) zijn basisscholen namelijk verplicht om de ontwikkeling van hun leerlingen te monitoren en vast te leggen in een *leerling- en onderwijsvolgsysteem*. Uit art. 8 lid 1 en 2 WPO volgt dat het onderwijs zich richt op zowel de cognitieve als de sociaal-emotionele en creatieve ontwikkeling van leerlingen. Deze wettelijke verplichting vormt een solide basis voor de verwerking van leerlinggegevens en valt hierdoor rechtstreeks onder artikel 6 lid 1 sub c AVG, omdat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de onderwijsinstelling rust.

Dit vindt bevestiging in jurisprudentie³⁰ waarin wordt gesteld dat artikel 8 lid 1 en 2 WPO een voldoende rechtsgrondslag biedt zoals bedoeld in artikel 6 lid 1 sub c AVG voor het verwerken van persoonsgegevens in een leerlingvolgsysteem, ook als dat betrekking heeft op de sociaal-emotionele ontwikkeling van leerlingen. Ook wordt er benadrukt in dit verband dat de AVG niet vereist dat voor elke afzonderlijke verwerking specifieke wetgeving aanwezig is, zoals blijkt uit overweging 45 in de considerans bij de AVG. Het is voldoende dat er algemene wetgeving bestaat die als basis kan dienen voor diverse verwerkingen op grond van een wettelijke verplichting. Op basis hiervan kan ook de grondslag van wettelijke verplichting (art. 6 lid 1 sub c) voldoen als wettelijke grondslag.

Leerlingadministratiesysteem (LAS)

Het onderdeel leerlingadministratiesysteem wordt ingezet voor administratieve taken, zoals het registreren van persoonsgegevens van leerlingen, de in- en uitschrijving, het faciliteren van communicatie met ouders en het beheren van de schoolorganisatie. De noodzaak hiervoor is gelegen in het feit dat men moet voldoen aan wettelijke verplichtingen, zoals de leerplichtwet, WPO en de Wet register onderwijsdeelnemers, maar ook op de uitvoering van een taak van algemeen belang, zoals het organiseren van goed onderwijs. Hierdoor kan deze verwerking gebaseerd worden op artikel 6, lid 1, sub e van de AVG (taak van algemeen belang op grond van onderwijswetgeving). Hierbij geeft artikel 40b WPO en de Wet register onderwijsdeelnemers duidelijk aan welke persoonsgegevens moeten worden

²⁹ Naast ParnasSys zijn er ook andere leveranciers van een *leerling- en onderwijsvolgsysteem*.

³⁰ *Rechtspraak.nl* <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBOBR:2021:5776>.

geadministreerd. In zoverre kan er ook sprake zijn van een rechtsgrond ‘wettelijke verplichting’ (sub c). Zie voor een uitwerking de tabel in hoofdstuk 10.

De WPO biedt een duidelijke wettelijke basis voor het verwerken van persoonsgegevens in zowel een leerlingadministratie- als een leerlingvolgsysteem. Dit komt omdat het verwerken van persoonsgegevens via een platform zoals ParnasSys geen doel op zich is, maar een hulpmiddel om andere doelen te bereiken. Denk hierbij aan het inschrijven en administreren van leerlingen, het volgen van hun ontwikkeling en het organiseren van onderwijs.

2. Medewerkers

In het leerlingadministratiesysteem (LAS) worden ook medewerkersgegevens verwerkt. De verwerking hiervan heeft de volgende doeleinden:

- Het beheren van contact- en identificatiegegevens.
- Het organiseren van klassen en het opstellen van lesroosters.
- Het ondersteunen van de schooladministratie en, indien van toepassing, de salarisadministratie (niet van toepassing in Basis van ParnasSys).

De rechtsgrond voor het verwerken van medewerkersgegevens verschilt van die van leerlingen. Deze verwerking is doorgaans gebaseerd op de arbeidsovereenkomst, die als juridische grondslag dient. Dit maakt het mogelijk om medewerkers bijvoorbeeld te koppelen aan schoolroosters, administratieve processen en interne communicatie.

Conclusie

De artikelen 11 jo. 45b lid 1 van de WPO, alsmede artikel 8 WPO bieden een solide wettelijke basis voor het verwerken van leerlinggegevens in het primair onderwijs. Onderwijsinstellingen kunnen zich voor wat betreft het leerlingadministratie en -volgsysteem hierbij primair beroepen op de grondslag *wettelijke verplichting* (artikel 6 lid 1 sub c AVG), omdat zij op grond van de WPO verplicht zijn de voortgang (ook sociaal-emotioneel) van leerlingen te monitoren. Aanvullend kan ook de grondslag *vervulling van een taak van algemeen belang* (artikel 6 lid 1 sub e AVG) een rol spelen, omdat scholen van overheidswege een publieke taak uitvoeren. Deze rechtsgrond kan dienen daar waar er mogelijk geen expliciete wettelijke grondslag is voor het verwerken van persoonsgegevens, zoals bepaald in de WPO en de Wet register onderwijsdeelnemers.

Een belangrijk aanvullend punt is dat, hoewel er duidelijke grondslagen zijn om persoonsgegevens van leerlingen en medewerkers te verwerken, scholen bij elke verwerking ook de AVG-beginselen (*zoals doelbinding, dataminimalisatie en transparantie*) in acht moeten nemen. Scholen moeten dus niet alleen kunnen terugvallen op een ‘rechtsgrondslag’ zoals bepaald in de AVG om te onderbouwen welke gegevens ze verwerken, maar ook kunnen aantonen dat de verwerking niet verder gaat dan noodzakelijk voor het onderwijsdoel, dat ze de gegevens niet langer bewaren dan strikt nodig, en dat ouders (en leerlingen zelf, voor zover van toepassing) en medewerkers duidelijk worden geïnformeerd over het hoe en waarom van de gegevensverwerkingen. Deze invulling van

deze AVG- beginselen³¹ is essentieel om de verwerking van persoonsgegevens ook in de praktijk rechtmatig, behoorlijk en transparant te laten plaatsvinden.

Tabel 12.1 Rechtsgrond

Verwerkingsdoeleinden (zie hiervoor 4. Verwerkingsdoeleinden)	Grondslag AVG	Relevante wet- en regelgeving (wettelijke verplichting/taak van algemeen belang)
De opslag van leer- en toetsresultaten.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 11 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag)).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (<i>wettelijke grondslag</i>) en / of e AVG (<i>algemeen belang, o.b.v. onderwijswetgeving</i>).
Het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 11 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag)).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (<i>wettelijke grondslag</i>) en / of e AVG (<i>algemeen belang, o.b.v. onderwijswetgeving</i>).
De beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 11 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag)).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (<i>wettelijke grondslag</i>) en / of e AVG (<i>algemeen belang, o.b.v. onderwijswetgeving</i>).
Analyse en interpretatie van leer- en toetsresultaten.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 11 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag)).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (<i>wettelijke grondslag</i>) en / of e AVG (<i>algemeen belang, o.b.v. onderwijswetgeving</i>).
Het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 11 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag)).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (<i>wettelijke grondslag</i>) en / of e AVG (<i>algemeen belang, o.b.v. onderwijswetgeving</i>).
De indeling en aanpassing van roosters.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag)).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (<i>wettelijke grondslag</i>) en / of e AVG (<i>algemeen belang, o.b.v. onderwijswetgeving</i>).

³¹ Zie artikel 5 AVG.

Het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgend van onderwijs.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Tevens artikel 9 lid 2 sub g jo. artikel 30 lid 2 sub a UAVG. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
De communicatie met Onderwijsdeelnemers en ouders en met medewerkers van de Onderwijsinstelling.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 11 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
Monitoring en verantwoording, met name ten behoeve van: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vormen) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
Het voor zover noodzakelijk en wettelijk toegestaan uitwisselen van Persoonsgegevens met Derden, waaronder: - Toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak; - Samenwerkingsverbanden in het kader van passend onderwijs en regionale samenwerkingen; - Partijen betrokken bij de invulling van stage- of leerwerkplekken; - Het leveren van Persoonsgegevens aan Onderwijsinstellingen in geval van overstappen tussen Onderwijsinstellingen en bij vervolgonderwijs; - Het in opdracht van Onderwijsinstelling leveren van Persoonsgegevens aan een andere partij.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag). Artikel 1 en 4c WPO (inspectie). Artikel 18a WPO (samenwerkingsverband) . Artikel 42 WPO (onderwijskundig rapport).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
Het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag). Artikel 28 AVG.	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
De continuïteit, verbetering en goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).

		e AVG (algemeen belang, o.b.v. onderwijswetgeving).
Het door de Onderwijsinstelling beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
Het door de Onderwijsinstelling voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
Het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
De uitvoering of toepassing van een Unierechtelijke of lidstaatrechtelijke wettelijk bepaling of regeling.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).
Andere doeleinden ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces) en het begeleiden en volgen van Onderwijsdeelnemers (in hun leerproces), namelijk het kunnen inschrijven en plaatsen van leerlingen.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 11 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ParnasSys is toegestaan op grond van artikel 6 lid 1 sub c (wettelijke grondslag) en / of e AVG (algemeen belang, o.b.v. onderwijswetgeving).

13. Bijzondere persoonsgegevens

In het kader van de verwerkingen via het leerling- en onderwijsvolgsysteem ParnasSys worden er geen gevoelige en bijzondere persoonsgegevens van medewerkers verwerkt. Dit geldt wel voor de gegevens van leerlingen, zoals hieronder is uitgewerkt.

Bijzondere persoonsgegevens:

Gezondheidsgegevens

Verwerking van persoonsgegevens die betrekking hebben op de gezondheid, verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de betrokkene. Gezondheidsgegevens betreffen alle persoonsgegevens over de fysieke en mentale gezondheid van een persoon. Voor deze bijzondere persoonsgegevens geldt een strenger regime: verwerking is verboden tenzij de AVG een uitzondering maakt, en dan alleen binnen de grenzen van die uitzondering. De AVG

laat ruimte voor nationale regelingen omtrent de verwerking van onder andere gegevens over de gezondheid.

Artikel 30 van de Uitvoeringswet AVG (UAVG) beschrijft enkele uitzonderingen inzake gegevens over gezondheid. Volgens art. 30 lid 2 sub a UAVG is het verbod om gegevens over gezondheid te verwerken niet van toepassing op onderwijsinstellingen, voor zover de verwerking met het oog op de speciale behandeling van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is. In de Wet op het primair onderwijs (WPO) wordt dit eveneens behandeld in artikel 8 lid 4 WPO³².

Wettelijk gezien mag een onderwijsinstelling dus gezondheidsgegevens verwerken van leerlingen, maar hierop gelden de beginselen van de AVG, waaronder dataminimalisatie en ‘need to know’. Bij scholen is dat dus beperkt tot begeleiding of speciale voorzieningen die nodig zijn voor de leerlingen om deel te nemen aan het onderwijs. In de praktijk vertaalt zich dit door deze informatie door een beperkt aantal medewerkers te laten verwerken in ParnasSys.

Gevoelige Persoonsgegevens:

BSN

Artikel 46 van de Uitvoeringswet AVG (UAVG) regelt dat verwerking van het BSN-nummer bij wet moet zijn voorgeschreven, dan wel voor doelen bij de wet bepaald. Deze wettelijke bepaling is voor een school vastgelegd in de WPO. Op grond van artikel 40b WPO is het verstrekken en daarmee ook het verwerken van het BSN-nummer noodzakelijk voor de inschrijving van de leerling. Het BSN-nummer is nodig ter identificatie van de leerling. Artikel 40b WPO rechtvaardigt dan ook de verwerking van het BSN-nummer van de leerling in de inschrijffase door de school in ParnasSys.

Open tekstvelden

In het kader van deze DPIA wordt gewezen op het risico dat de leerkracht in ParnasSys in een open tekstveld ‘aantekeningen’ kan maken. Het vraagt om een gedragsregel vanuit de scholen om de medewerker van de scholen erop te wijzen dat in het kader van de leermiddelen en aantekeningen er geen gevoelige en/of bijzondere persoonsgegevens mogen worden verwerkt.

14. Doelbinding

In het kader van de verwerking van persoonsgegevens via het LAS/LVS van ParnasSys worden er geen persoonsgegevens verwerkt voor een ander doel dan oorspronkelijk verzameld.

³² Zie ook: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/onderwijs/leerlingdossiers>.

15. Kinderrechten-afweging (Best Interests Assessment Children)

Artikel 3 van het Verdrag inzake de rechten van het kind, schrijft voor dat bij alle maatregelen betreffende kinderen - ongeacht of deze worden genomen door openbare of particuliere instellingen, rechterlijke instanties, bestuurlijke autoriteiten of wetgevende lichamen - de belangen van het kind de eerste overweging (moeten) vormen. Deze belangenafweging gaat verder dan een veilige gegevensverwerking maar ziet ook op de mogelijke gevolgen van de verwerking. Met schoolbesturen als leden van SIVON in het primair en voortgezet onderwijs, betekent dit dat SIVON in haar DPIA's rekening houdt met o.a. gebruikers (betrokkenen) in de leeftijd van 4 tot 18 jaar (of ouder). Kinderen hebben recht op specifieke bescherming van hun persoonsgegevens. Dit volgt uit het feit dat zij zich minder bewust zijn van de risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van hun persoonsgegevens. SIVON geeft hier in deze DPIA invulling aan door af te wegen of het gebruik van het ParnasSys en/of de gegevensverwerking(en) die daarmee samenhangen, in het belang zijn van de betrokkenen (kind/leerling als betrokkene). SIVON maakt hierbij gebruik van de systematiek van de best interests assessment children van de Britse ICO³³. De afweging bestaat uit 4 stappen:

1. Wat zijn de (relevante) rechten van kinderen in het kader van deze DPIA?

Hieronder wordt beschreven welke rechten³⁴ van en voor kinderen relevant zijn in het kader van deze DPIA. Van belang is de leeftijd van de kinderen (leeftijdsadequaat). Hierbij wordt nagegaan of de gegevensverwerking (negatieve) gevolgen heeft voor de ondersteuning en van de behoeften van het kind op het gebied van veiligheid, gezondheid, welzijn, familierelaties, fysieke, psychologische en emotionele ontwikkeling, identiteit, vrijwaring van economische commerciële en/of fysieke uitbuiting, vrijheid van meningsuiting, privacy en de mogelijkheid om een eigen mening te vormen en deze te laten horen, het belang van toegang tot informatie, omgang met anderen en spel (buiten spelen) om de ontwikkeling van het kind te ondersteunen. Het gaat erom dat het kind in overeenstemming met zijn of haar ontwikkelende capaciteiten, een stem heeft (kan hebben) in zaken die hem of haar aangaan.

De basisfunctionaliteit van het leerling- en onderwijsvolgsysteem ParnasSys wordt niet gebruikt door kinderen. Hierdoor is het niet nodig om te beoordelen of het gebruik van de applicatie leeftijdsadequaat is en past bij de leeftijd van de leerlingen.

2. Identificeer het effect van de gegevensverwerking en gebruik van ParnasSys op deze rechten.

De onderstaande rechten komen terug in regelgeving en in het Verdrag inzake de Rechten van het Kind (IVRK) en zijn van toepassing op ParnasSys:

- Het recht op privacy wordt geëerbiedigd;

³³ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/best-interests-self-assessment/>

³⁴ https://wetten.overheid.nl/BWBV0002508/2002-11-18#Verdrag_2

- Persoonlijke gegevens worden beschermd;
- Kinderen worden niet onderworpen aan willekeurige of onrechtmatige inmenging in hun privéleven;
- Kinderen worden beschermd tegen beslissingen op basis van automatische verwerking van gegevens, als die hun kansen of vrijheden significant kunnen beïnvloeden;
- Er moet een mogelijkheid zijn voor menselijk ingrijpen, waarbij kinderen of hun voogden de kans krijgen om hun standpunt te uiten en de beslissing aan te vechten.

Het gebruik van Basis van ParnasSys heeft in beginsel geen negatieve invloed op de ondersteuning van de behoeften van het kind op gebieden zoals veiligheid, gezondheid, welzijn, familierelaties, fysieke, psychologische en emotionele ontwikkeling, identiteit, bescherming tegen economische en commerciële uitbuiting, vrijheid van meningsuiting, privacy, het vormen en uiten van een eigen mening, toegang tot informatie, sociale interactie en spel (zoals buitenspelen) ter bevordering van hun ontwikkeling³⁵.

Het is echter belangrijk te benadrukken dat Basis van ParnasSys veel persoonlijke en gevoelige gegevens van leerlingen verzamelt en beheert, waaronder informatie over hun sociaal-emotionele ontwikkeling en leerprestaties. Omdat er binnen Basis van ParnasSys over een langere periode persoonsgegevens in de vorm van prestaties worden bewaard en deze resultaten zichtbaar zijn voor gebruikers (leerkrachten) kan dit leiden tot evaluatie of scoretoekenning. Daarom is het cruciaal dat deze gegevens nauwkeurig en correct worden geregistreerd en regelmatig worden gecontroleerd.

3. Beoordeel of dit effect wenselijk is

Zoals onder punt 2 aangegeven, zijn er op dit moment geen aanwijzingen dat het gebruik van Basis van ParnasSys negatieve gevolgen heeft. Basis van ParnasSys wordt altijd ingezet ten behoeve van het onderwijskundige proces van de onderwijsinstelling, waarbij de onderwijsinstelling bepaalt wie verantwoordelijk is en er dus geen sprake is van willekeurigheid of onrechtmatigheid.

4. Bepaal of aanvullende maatregelen noodzakelijk zijn om effecten te beperken

Er is geen noodzaak om aanvullende maatregelen te nemen om de rechten van het kind te beschermen. De effecten die de gegevensverwerkingen binnen Basis van ParnasSys hebben op de kinderrechten, zijn over een brede linie tegen het licht gehouden zonder dat daarbij is gebleken dat er sprake is van een niet te rechtvaardigen inbreuk.

16 a. Noodzakelijkheid

Verwerking van persoonsgegevens met behulp van digitale onderwijsmiddelen door onderwijsinstellingen vindt plaats ten behoeve van het verzorgen van onderwijs, waaronder

³⁵ NB: Dit is wel het geval bij inzet van het dashboard Prognose referentieniveaus in Ultimview, welke scholen en besturen inzicht biedt in de behaalde resultaten van de doorstroomtoets en een prognoses geeft voor de huidige leerjaren 6 en 7. Dit is buiten scope van deze DPIA.

het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces) en het begeleiden en volgen van onderwijsdeelnemers (in hun leerproces).

Uit de analyse van de gegevensverwerking (zie deel A: de gegevensverwerkingsanalyse) blijkt dat de door Basis van ParnasSys te verwerken persoonsgegevens noodzakelijk zijn in relatie tot het doel van de gegevensverwerking.

De verwerkingen door de onderwijsinstelling via Basis van ParnasSys vinden plaats om door middel van een digitaal systeem de gegevens van leerlingen te administreren en ontwikkelingen/vorderingen bij te houden. Tevens is de gegevensverwerking noodzakelijk in het kader van de wettelijke verplichtingen om onderwijs te verzorgen.

Het toepassen van de verwerkingen en soorten persoonsgegevens die zijn vastgelegd, is hierbij noodzakelijk om Basis van ParnasSys op de gewenste manier te kunnen gebruiken.

16. b. Proportionaliteit en subsidiariteit

De onderwijsinstelling is verantwoordelijk voor het verzorgen van goed onderwijs, conform de bepalingen van de Wet op het Primair Onderwijs. Bij het gebruik van (digitale) systemen voor het waarborgen van een ononderbroken ontwikkelingsproces is de inbreuk op de persoonlijke levenssfeer beperkt en staat deze in verhouding tot de verwerkingsdoelen.

Als het autorisatiebeheer zorgvuldig wordt ingericht, hebben alleen medewerkers van de onderwijsinstelling, op basis van een ‘need-to-know’-principe, toegang tot gegevens van leerlingen binnen hun eigen groep. Hierdoor blijft de verwerking beperkt tot de professionals die direct betrokken zijn bij de ondersteuning van het ontwikkelingsproces van de leerlingen.

De onderwijsinstelling heeft een wettelijke verplichting om een administratie bij te houden en de prestaties van leerlingen te monitoren. Het gebruik van een leerlingadministratie- en onderwijsvolgsysteem zoals Basis van ParnasSys, draagt bij aan het veilig en verantwoord beheren van leerlinggegevens, wat efficiënter is dan handmatige verwerking of losse systemen per school.

De gegevensverwerking is proportioneel, aangezien uitsluitend de strikt noodzakelijke gegevens worden verwerkt, mits op de juiste manier beschreven, ingericht en toegepast. Bovendien zijn adequate technische en organisatorische beveiligingsmaatregelen beschikbaar om de persoonsgegevens te beschermen tegen onrechtmatige verwerking.

Behalve door het gebruik van een ander, vergelijkbaar systeem, bestaat er geen efficiënter alternatief voor het voeren van een leerlingadministratie- en onderwijsvolgsysteem.

17. Rechten van de betrokkenen

‘Art. 15, lid 1, van de AVG beschrijft dat iedere betrokkene het recht heeft om van de verwerkingsverantwoordelijke uitsluitend te verkrijgen over het al dan niet verwerken van

hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens³⁶.

De scholen die persoonsgegevens verwerken, bijvoorbeeld via Basis van ParnasSys, dienen op hun website een duidelijke privacyverklaring en een privacyreglement opgenomen te hebben, aangezien zij verwerkingsverantwoordelijke zijn. Hierin staat beschreven welke rechten betrokkenen hebben betreffende de verwerking van hun persoonsgegevens en hoe men hun rechten kan uitoefenen.

SIVON heeft onderzocht en vastgesteld dat, met betrekking tot de uitoefening van rechten van betrokkenen, scholen die Basis van ParnasSys gebruiken, zelfstandig kunnen voorzien in de afhandeling van verzoeken van betrokkenen (veelal van ouders).

Mocht een school hier niet uitkomen, dan ondersteunt Topicus de school bij het voldoen aan de verplichtingen van de verwerkingsverantwoordelijke inzake de rechten van betrokkenen. Verzoeken van de scholen worden via de telefonische helpdesk of via relatiebeheer in behandeling genomen. Daar wordt geverifieerd of de vragende instelling een accounthouder is bij ParnasSys.

Overigens kunnen ouders met gebruik van Parro (buiten scope voor deze DPIA) zelf de meeste gegevens inzien die door de onderwijsinstelling worden verwerkt in Basis van ParnasSys.

In het onderstaande tabel wordt aangegeven welke rechten het betreft en of er van enige beperking sprake is.

Tabel 17.1

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking ³⁷
Het recht op informatie	De onderwijsinstelling dient als verwerkingsverantwoordelijke te zorgen voor een: • Openbaar gepubliceerde privacyverklaring op de website; • Intern gepubliceerde privacyverklaring; • Publicatie in de schoolgids.	n.v.t.
Het recht van inzage	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht op rectificatie	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht op gegevenswissing	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht op beperking van de verwerking	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.

³⁶ Zie Hoofdstuk III van de AVG 'Rechten van de betrokkene', artikel 12 – 23 AVG.

³⁷ Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, of in de AVG direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving. Uitzonderingen op de rechten van betrokkenen zijn, onder meer, geregeld in artikel 23 AVG en artikel 41 UAVG.

Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht op overdraagbaarheid van gegevens	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht van bezwaar	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit	Dit is niet aan de orde. De onderwijsinstelling neemt de uitkomsten van de leer- en toetsresultaten mee in de eigen beoordeling van de leerling.	n.v.t.

18. Beoordeling verwerkersovereenkomst

Voor leveranciers die deelnemer (of medestander) zijn van het [Convenant Digitale Onderwijsmiddelen en Privacy 4.0](#) (ook wel: Privacyconvenant Onderwijs, hierna: Convenant) of van de opvolger daarvan namelijk het keurmerk Edu-V (hierna: Edu-V) en gebruik maken van de daarbij horende model verwerkersovereenkomst, vindt een toetsing plaats welke wordt afgezet tegen de vereisten van het Convenant/Edu-V. Dit wordt de theoretische toets genoemd. Aanvullend hierop vindt ook, mede aan de hand van de inzichten die deze DPIA heeft gebracht, een praktische toets plaats. Hierbij is een vergelijk gemaakt tussen de in de theorie genoemde afspraken en de verwerkingen die in de praktijk plaatsvinden. De gebruikte toetsingskaders zijn via [de SIVON-website](#) terug te vinden.

Na de bespreking van de bevindingen via het Toetsformulier en het doorvoeren van verbeteringen in de verwerkersovereenkomst en/of het maken van eventuele afspraken daartoe, wordt uiteindelijk een definitief Toetsrapport opgeleverd die via de Dienst Verwerkersovereenkomsten van Kennisnet of op de leverancierswebsite ontsloten wordt.

De toets van de verwerkersovereenkomst voor ParnasSys van Topicus Education B.V. is uitgevoerd op de laatste versie, versie 4.1 (25-04-2025). De belangrijkste bevindingen van de toets van deze verwerkersovereenkomst zijn in de onderstaande tabel samengevat:

Tabel 18.1

Toets - Verwerkersovereenkomst	Opgenomen (volledig en juist)? JA/NEE	Toelichting
Verschillen geconstateerd tov Edu-V Model verwerkersovereenkomst 4.1?	Ja, want	Er zijn verschillen geconstateerd.
Zo ja, opgenomen in Bijlage 3: Wijzigingenbijlage	Ja, want	Verschillen zijn netjes opgenomen in Bijlage 3.
Toets - Bijlage 1: Privacybijsluiter	Opgenomen (volledig en juist)?	Toelichting
• Link naar productpagina (website/URL)	Ja, want	Productpagina is opgenomen bij 'Link naar Leverancier'. Bij 'link naar productpagina' is de inlogpagina opgenomen.
a. omschrijving van producten en/of diensten en bijbehorende Verwerkingen die een onlosmakelijk onderdeel vormen van het aangeboden product en/of de aangeboden dienst, inclusief de koppelingen en uitwisseling met derde partijen;	Ja, want	Hoewel in de online Privacybijsluiter (zie: https://www.parnassys.nl/juridisch/privacybijsluiter) alsnog niet expliciet is opgenomen dat de Basis van ParnasSys onlosmakelijk onderdeel is van ParnasSys, maakt de nieuwe tekst dat wel voldoende duidelijk.
b. omschrijving van aanvullende optionele producten en/of diensten en bijbehorende Verwerkingen die de	Ja, want	Hoewel in de online Privacybijsluiter (zie: https://www.parnassys.nl/juridisch/privacybijsluiter) niet expliciet is opgenomen welke onderdelen

Verwerker aanbiedt, inclusief de koppelingen en uitwisseling met derde partijen.		optioneel zijn, maakt de nieuwe tekst dat wel voldoende duidelijk. De vermelding van de (optionele) module Incidentenregistratie ontbrak, maar is nu netjes en transparant opgenomen. Hoewel deze module enkele jaren geleden is uitgefaseerd, is deze mogelijk nog wel actief bij scholen voor die periode.
In dit onderdeel wordt vastgelegd welke doeleinden, zoals vastgelegd in artikel 5 van het Convenant, van toepassing zijn op de Verwerking van Persoonsgegevens met behulp van de specifieke producten en/of diensten.	Ja, want	Standaard doeleinden rondom het verkrijgen van toegang en de beveiliging zijn ten opzichte van de vorige versie voor alle producten/modules opgenomen.
1. een omschrijving van de categorieën Betrokkenen (o.a. Onderwijsdeelnemers, ouders/verzorgers, medewerkers) over wie Persoonsgegevens worden verwerkt, en de te verwerken categorieën Persoonsgegevens van deze Betrokkenen, en	Ja, want	Dit is netjes per product/module gespecificeerd via de online Privacybijsluiter (zie: https://www.parnassys.nl/juridisch/privacybijsluiter).
2. door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen).	Ja, maar	Verwerker heeft toegezegd ook concreet te zijn over de bewaartermijn bij beëindiging van de overeenkomst, zoals bedoeld in Artikel 12, lid 2 van de Verwerkersovereenkomst, namelijk: <i>Verwerker zal de verwerkte gegevens in de eerste maand van het volgende kalenderjaar met behulp van een beveiligde online omgeving ter beschikking stellen. De gegevens blijven hier beschikbaar tot het einde van de daaropvolgende maand. Daarna worden de gegevens verwijderd en niet verder verwerkt.</i> Deze passage inclusief de toevoeging 'of eerder op schriftelijk verzoek van Onderwijsinstelling' dient nog opgenomen te worden in een nieuwe versie van de verwerkersovereenkomst.
Onder G. wordt vastgelegd wat de plaats(en)/land(en) van opslag en Verwerking van de Persoonsgegevens zijn.	Ja, want	Dit is samengevoegd met onderdeel H.
Verwerker legt hier vast van welke Subverwerkers hij ten tijde van het afsluiten van de Verwerkersovereenkomst gebruikmaakt.	Ja, want	Subverwerkers zijn gekoppeld aan producten/modules (en daarmee aan verwerkingen van persoonsgegevens). Bij mogelijke verwerkingen buiten de EER zijn extra waarborgen benoemd. Cloudflare en Focus PO stonden al in de online Privacybijsluiter, maar zijn voor de volledigheid ook toegevoegd in de verwerkersovereenkomst zelf.
Toets - Bijlage 2: Beveiligingsbijlage	Opgenomen (volledig en juist)?	Toelichting
Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden. Verwerker gebruikt hiervoor in beginsel het 'Certificeringsschema informatiebeveiliging en privacy ROSA' (te vinden op www.edustandaard.nl) als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy.	Ja, want	Getroffen maatregelen (uitleg) zijn helder beschreven.
Inlogpagina	Ja, want	URL naar de inlogpagina inloggen.parnassys.net is nu opgenomen.
Beschikbaarheid (alleen opnemen, indien niet voldaan of bij vragen/opmerkingen over de uitleg)	Ja, want	Er is toegelicht wat er is geregeld en hoe. Ten opzichte van de vorige versie is ook opgenomen of voldaan wordt aan de maatregelen.
Integriteit (alleen opnemen, indien niet voldaan of bij vragen/opmerkingen over de uitleg)	Ja, maar	Er is toegelicht wat er is geregeld en hoe. Ten opzichte van de vorige versie is ook opgenomen of voldaan wordt aan de maatregelen. Bij de eerste 'Onweerlegbaarheid' dient de bewaartermijn van 3 naar 13 maanden aangepast te worden. De tweede 'Onweerlegbaarheid' lijkt een kopie van de

		eerste, terwijl daar iets anders mee wordt bedoeld (zie ROSA). Hier dient '(Toepassing)' als tekst in de verwerkersovereenkomst toegevoegd te worden en de toelichting waarschijnlijk aangepast te worden.
Vertrouwelijkheid (alleen opnemen, indien niet voldaan of bij vragen/opmerkingen over de uitleg)	Ja, want	Er is toegelicht wat er is geregeld en hoe. Ten opzichte van de vorige versie is ook opgenomen of voldaan wordt aan de maatregelen.
Toets - Bijlage 3: Wijzigingenbijlage (indien van toepassing)	Opgenomen (volledig en juist)?	Toelichting
1. Beschrijving noodzakelijke afwijkingen Model Verwerkersovereenkomst incl. Bijlagen	Ja, want	Afwijkingen zijn netjes opgenomen, helder toegelicht en acceptabel.

De bevindingen uit deze tabel zijn uitgewerkt in de risicotabel van hoofdstuk 19.

7. Deel C: Beschrijving en beoordeling risico's voor de betrokkenen

In dit hoofdstuk vindt de Risicoanalyse plaats: de gegevensverwerkingsanalyse (Deel A), aangevuld met een beoordeling van de rechtmatig (Deel B) worden afgewogen tegen de rechten en vrijheden van betrokkenen. De risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden beschreven en beoordeeld. Hierbij wegen de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen mee.

Beoordelingskader risico's

Alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden beschreven en afgewogen. Het gaat hierbij om de negatieve gevolgen die de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, de oorsprong van deze gevolgen, de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden: kans (waarschijnlijkheid) X impact (ernst) = risico.

De methodiek die wordt gevolgd om risico's te classificeren, is beschreven door de Britse toezichthouder³⁸. Hierbij wordt een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade). Zie ook bijlage 2.

Onderstaande matrix toont op een gestructureerde manier de classificatie van risico's:

RISICO	Kans Laag (1)	Kans Midden (2)	Kans Hoog (3)
Impact Hoog (3)	Risico Midden (Score: 3)	Risico Hoog (Score: 6)	Risico zeer hoog (Score: 9)
Impact Midden (2)	Risico Laag (Score: 2)	Risico Midden (Score: 4)	Risico Hoog (Score: 6)
Impact Laag (1)	Risico Zeer laag (Score: 1)	Risico Laag (Score: 2)	Risico Midden (Score: 3)

NB: een score van 1 levert dus een zeer laag risico op, terwijl een score van 9 een zeer hoog risico oplevert.

Het gaat hier om een risicogerichte benadering en beoordelingsproces dat bestaat uit de volgende drie stappen:

1. risico's identificeren;

³⁸ Zie voor de meest recente matrix van de ICO: '[How do we identify and assess risk](#)'. De matrix zoals opgenomen in dit DPIA model is een eerder, nog steeds gevalideerd model om risico's te classificeren en wordt nog gebruikt ten behoeve van consistentie met eerdere DPIA's uitgevoerd door SIVON.

2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

In het volgende hoofdstuk (deel D: maatregelen) worden de geconstateerde risico's aangevuld met 2 vervolgstappen:

4. Mitigeren risico's: maatregelen die de aangetroffen risico's voorkomen of verminderen (mitigeren);
5. Herbeoordeling risico's: restrisico.

19. Risico's

In onderstaande risicotabel worden de risico's beschreven. Per risico worden de mogelijke oorzaken en gevolgen aangegeven met daarbij de kans dat het zich voordoet en de impact. Tevens is aangegeven of het risico betrekking heeft op een proces waarbij Basis van ParnasSys wordt ingezet of dat het risico het systeem zelf betreft (de applicatie).

Toelichting MAPGOOD-methode

De MAPGOOD methode helpt om inzicht te krijgen in de verschillende risico's van de verwerking. Via deze methode wordt aan de hand van verschillende invalshoeken naar de risico's gekeken. Het MAPGOOD-model biedt houvast om de risico's te inventariseren. Zo zijn er verschillende invalshoeken die je kunt gebruiken om naar bedreigingen en risico's te kijken om zo beveiligingsmaatregelen in kaart te brengen:

- **Mens** – de mensen die nodig zijn om het informatiesysteem te beheren en gebruiken, denk aan: directe en indirecte gebruikers, en functioneel en technisch applicatiebeheer.
- **Apparatuur** – de apparatuur die nodig is om het informatiesysteem te laten functioneren, denk aan: webserver, applicatieserver, beheer van werkplekken en werkplekken van gebruikers.
- **Programmatuur** – de programmatuur waaruit het informatiesysteem bestaat, denk aan: de diverse applicaties die gebruikt worden.
- **Gegevens** – de gegevens die door het systeem worden verwerkt, denk aan: basisregistraties, financiële verantwoording en vergunningen.
- **Organisatie** – de organisatie die nodig is om het informatiesysteem te laten functioneren, denk aan: beheer-, gebruikers- en ontwikkelorganisatie.
- **Omgeving** – de omgeving waarbinnen het informatiesysteem functioneert, denk aan: locatie, serverruimte en werkplekken.
- **Diensten** – de externe diensten die nodig zijn om het systeem te laten functioneren, denk aan: technisch systeembeheer, netwerkinfrastructuur en onderhoudscontracten met externe dienstverleners.

Tabel 19.1 Risico's:

De volgorde waarin de risico's worden gepresenteerd, is afgestemd op de volgorde van de onderzochte aspecten en impliceert geen prioritering naar belangrijkheid.

Risico's	Mapgord	Risico-omschrijving	Oorzaak	Gevolg	Kans	Impact	Risico	Proces en/of systeem-risico+ verantwoordelijke
1	P M O	Ongeoorloofde inzage in (bijzondere) persoonsgegevens. Er wordt geen 'privacy by default' toegepast.	Autorisaties worden niet by default beperkt op basis van 'need to have'. Applicatiebeheerder kan alles inzien.	Dit kan leiden tot discriminatie of reputatieschade.	3	3	9	Systeem (Topicus)
2	P G	Onvoldoende transparantie over inzage in BSN.	Niet ingericht op basis van 'need to have'; niet gespecificeerd in het rollen en rechten-overzicht op schoolniveau tot welke gegevens (en dus rechten en rollen) BSN behoort.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	2	3	6	Systeem (Topicus)
3	P	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregelen toegepast. De 'Vertrouwelijkheid' van de BIV-classificatie in het ROSA certificeringsschema is als 'Hoog' gekwalificeerd, er wordt een ontoereikende alternatieve maatregel toegepast.	Onvoldoende encryptie op de database 'at rest', er ontbreekt een tweede encryptielaag.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	3	3	9	Systeem (Topicus)
4	P M O	Onrechtmatige toegang tot persoonsgegevens. Exportfunctionaliteit is standaard beschikbaar zonder beperkingen, waardoor onbedoeld persoonsgegevens kunnen worden geëxporteerd (geen 'privacy by design').	Downloaden staat niet 'by default' uit en er is geen mogelijkheid om de exportfunctie uit te schakelen.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	2	3	6	Systeem (Topicus)

		Het risico is dat er door het gebruik van de export- en/of downloadfunctie mogelijk (bijzondere) persoonsgegevens buiten de applicatie terecht komen wat verlies van controle over deze data tot gevolg heeft.						
5	P M O	Onrechtmatige toegang tot persoonsgegevens. Er wordt geen ‘ <i>privacy by default</i> ’ toegepast bij exports/downloads.	De kleur van sommige keuzevelden bij exporteren werkt ‘nudging’ in de hand. Er is niet op alle functies een “voorvertoning”-mogelijkheid (tijdelijk browsertabblad). Hierdoor worden onnodig gegevens gedownload voordat deze bijvoorbeeld worden geprint.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	2	3	6	Systeem (Topicus)
6	P M O	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregelen toegepast. De ‘Integriteit’ van de BIV-classificatie in het ROSA certificeringsschema is als ‘Hoog’ gekwalificeerd, er wordt een ontoereikende alternatieve maatregel toegepast.	Er vindt onvoldoende preventieve, geautomatiseerde monitoring plaats op bijv. overmatig/afwijkend gebruik door gebruikers in het algemeen, en op afwijkend gedrag inzake exports in het bijzonder. Monitoring door de onderwijsinstelling zelf kan, echter nog onvoldoende verdiepend (exports en wijziging cijfers).	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	2	3	6	Systeem (Topicus)
7	P M O	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregelen toegepast en geen ‘ <i>privacy by default</i> ’.	Er wordt geen 2FA voor beheerders en andere gebruikers <i>by default</i> afgedwongen.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	3	3	9	Systeem (Topicus)
8	O	Ontoereikende afspraken in de verwerkersovereenkomst over de verwerking van de persoonsgegevens.	Bewaartermijn van 13 maanden is geïmplementeerd, maar nog niet opgenomen in de nieuwe versie verwerkersovereenkomst (ROSA). Hier dient ook de	Dit is een risico voor de rechten en vrijheden van betrokkenen	2	2	4	Proces (Topicus)

			paragraaf over Onweerlegbaarheid (Toepassing) aangepast te worden. Dit geldt ook voor de informatie over verwijdering na beëindiging contract.					
--	--	--	---	--	--	--	--	--

8. Deel D: Beschrijving voorgenomen maatregelen

Dit hoofdstuk bevat de maatregelen die zijn of worden genomen om de geconstateerde risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen (Deel C) te beperken.

Beoordelingskader maatregelen

De AVG geeft in artikel 5 lid 1 sub f als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat de persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. De verschillende maatregelen betreffen:

- Maatregelen die al zijn/worden genomen door de betrokken partijen die direct betrekking hebben op de risico's van de gegevensverwerkingen. Bijvoorbeeld, beveiligingsbeleid dat direct van toepassing is op de gegevensverwerkingen.
- Maatregelen die nog zullen worden genomen om de risico's van de gegevensverwerkingen zoveel mogelijk te mitigeren. Het betreft hier reeds voorgenomen maatregelen, of maatregelen die naar aanleiding van deze DPIA nog zullen worden genomen.

Hierbij wordt aangesloten bij de methodiek van de Franse toezichthouder (CNIL): verwerkingsverantwoordelijke en verwerker stellen bij onacceptabele risico's (los van de vraag of deze laag, middel of hoog zijn) gezamenlijk een actieplan op. Dit wordt een verbeterplan genoemd. Het verbeterplan vermeldt – met een planning – de voorgenomen maatregelen om de risico's te mitigeren. Dit betreffen waarborgen, maatregelen en beveiligingsmechanismen om de bescherming van persoonsgegevens te waarborgen en de naleving van de AVG aan te tonen. Hierbij worden alleen maatregelen in aanmerking genomen waarvan het zeker is dat deze maatregelen genomen zullen (gaan) worden en dus de beschreven risico's daadwerkelijk zullen voorkomen of beperken. De maatregelen moeten met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn.

Risico's kunnen worden beperkt door maatregelen te nemen. Deze maatregelen zullen de kans en/of impact verkleinen. Daarmee blijft er een risico over: het restrisico. Rekenkundig uitgelegd betekent dit: [kans (waarschijnlijkheid) X impact (ernst)] -/- [risico-mitigerende maatregelen] = **restrisico**.

Het schoolbestuur moet beschrijven hoe tot het restrisico is gekomen en waarom deze aanvaardbaar wordt geacht.

Gedacht kan worden aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- Fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- Opslag van gegevens in een kluis;
- Project-, risico- en incidentenmanagement;
- Data opsplitsen;
- Dataminimalisatie;
- Back-ups;
- Integriteitscontroles;
- 2FA/MFA;
- Monitoring en logging;
- Controle van toegekende bevoegdheden;
- Privacybewustzijn- en beveiligingstrainingen;
- Managementrapportages over risicobeheer;
- Beperken inzageniveau;
- Periodiek een audit of hack- of penetratietest uitvoeren;
- Richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- Resonable-disclosurebeleid;
- Geheimhoudingsverklaringen;
- Service level agreements (met boeteclausules);
- Verwerkersovereenkomsten.
- Screening personeel en VOG-verklaring.

20. Maatregelen

Hierna wordt beschreven welke technische en organisatorische maatregelen in redelijkheid (kunnen) worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Daarbij is opgenomen welke maatregel welk risico aanpakt en wat het eventuele restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, is een motivering opgenomen waarom het restrisico acceptabel is.

20.1 Maatregellentabel:

R i s i c o n r .	Omschrijving risico (steekwoord)	R i s i c o	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (leverancier /school)	R e s t r i s i c o	Toelichting aanvaardbaarheid restrisico	(datum) maatregel geïmplemente erd?
1	Ongeoorloofde inzage in (bijzondere) persoonsgegevens (autorisaties)	9	Admin geen standaard toegang verlenen tot persoonsgegevens / database. (technisch) Onderwijsinstelling: Beperken van de admin- accounts. Tevens admin een geheimhoudingsverklaring laten ondertekenen. (organisatorisch)	Topicus Onderwijsins telling	2	Topicus neemt geen verdere maatregelen inzake admin-rechten. Momenteel is het ontwerp-uitgangspunt binnen ParnasSys dat de eerste superuser de rollen en rechten toekent en op die manier de toegang tot data voor overige gebruikers afbakt op een 'need to know' basis. Als de onderwijsinstelling de gesuggereerde maatregelen doorvoert, is het restrisico aanvaardbaar.	Maatregelen te nemen op niveau onderwijsinstelli ng
2	Onvoldoende transparantie over inzage in BSN.	6	In het rollen en rechten- overzicht op schoolniveau opnemen tot welke gegevens (en dus rechten en rollen) BSN behoort. (organisatorisch)	Topicus	0	Er is na het doorvoeren van de maatregelen geen restrisico	Uiterste datum gereed: eind 2025 (Topicus)
3	Er worden onvoldoende beveiligingsmaatre gelen toegepast. (dubbele encryptie)	9	Aantoonbaar inregelen 2e encryptielaag. (technisch)	Topicus	1	Er is na het doorvoeren van de maatregelen een minimaal en aanvaardbaar restrisico	Uiterste datum gereed: 1 september 2026 (Topicus)
4	Onrechtmatige toegang tot persoonsgegevens . (exporteren/down loaden <i>by default</i> aan)	6	Inbouwen van een mogelijkheid export/downloadfunctie aan/uit te zetten. Vervolgens deze functie <i>by default</i> uitzetten. Exporteren/downloaden zichtbaar maken in de logging (zie ook bij punt 6)	Topicus	2	Topicus treft geen maatregelen om exporteren/downloaden aan/uit te kunnen zetten en <i>by default</i> op 'uit' aan te bieden. De loggingfunctionaliteit wordt wél aangepast en	Monitoring van de logging op exports en wijzigingen cijfers mogelijk maken voor de onderwijsinstelli ng zelf is op de ontwikkelagend a geplaatst.

			Onderwijsinstelling: afspraken maken over het maken en gebruiken van exports en hier controle op uitoefenen (door logfiles via Topicus op te vragen). Tevens afdwingen dat de downloadmap automatisch wordt geschoond (dagelijks en bij afsluiten browser), alsmede verbieden inzet privé-devices. (organisatorisch)	Onderwijsinstelling		uitgebreid (zie ook bij punt 6). Als ook de onderwijsinstelling de gesuggereerde maatregelen doorvoert, is het restrisico aanvaardbaar. Aanvullend: SIVON is van oordeel dat deze maatregelen als onderdeel van 'privacy by design/default' moet worden gezien en standaard moet worden aangeboden. Het is op dit moment niet mogelijk de exportfunctie uit te schakelen. In de volgende DPIA op deze applicatie wordt dit wederom beoordeeld.	Uiterste datum gereed: december 2026. (Topicus) + Maatregelen te nemen op niveau onderwijsinstelling
5	Onrechtmatige toegang tot persoonsgegevens . (exporteren/download nudging, voorvertoning)	6	Op alle functies voor zover technisch mogelijk een "voorvertoning"-mogelijkheid (tijdelijk browsertabblad) aanbieden. Kleurstellingen aanpassen, zodat er geen 'nudging' is. (technisch)		1	Er is na het doorvoeren van de maatregelen een minimaal en aanvaardbaar restrisico	Uitbreiding van voorvertoning op alle functies (waar technisch mogelijk) is op de ontwikkelagenda geplaatst. Uiterste datum gereed: december 2026 Opheffen van nudging is op de ontwikkelagenda geplaatst. Uiterste datum gereed: december 2026 (Topicus)
6	Er worden onvoldoende beveiligingsmaatregelen toegepast. (logging, monitoring)	6	Automatisch monitoren van logfiles binnen Topicus implementeren. Extra (log)functionaliteit beschikbaar stellen aan de onderwijsinstelling zelf voor het preventief, geautomatiseerd	Topicus	2	Topicus is bereid maatregelen te treffen inzake beschikbaar stellen van verdiepende logfiles aan de onderwijsinstelling zelf, specifiek waar het informatie over exports	Monitoring van de logging op exports en wijzigingen cijfers mogelijk maken voor de onderwijsinstelling zelf is op de ontwikkelagenda

			monitoren op overmatig/afwijkend gedrag door gebruikers in het algemeen, en op afwijkend gedrag inzake exports en cijferwijzigingen in het bijzonder. (technisch) Onderwijsinstelling: Inregelen van monitoring van de huidige, voor henzelf al beschikbare logfiles en hier controle op uitoefenen (en eventueel verdiepende logfiles via Topicus opvragen). (organisatorisch)	Onderwijsinstelling		en cijferwijzigingen betreft. Als Topicus en de onderwijsinstelling de gesuggereerde maatregelen doorvoeren, is het restrisico aanvaardbaar.	a geplaatst. Uiterste datum gereed: december 2026 (Topicus) + Maatregelen te nemen op niveau onderwijsinstelling
7	Onrechtmatige toegang tot persoonsgegevens (2FA)	9	Gebruik 2FA <i>by default</i> instellen (technisch) Onderwijsinstelling: 2FA instellen en afdwingen. Daarbij ook via SSO bijv. Office 365 en Google meenemen. (technisch en organisatorisch)	Topicus	2	Topicus is niet bereid maatregelen te treffen inzake 2FA <i>by default</i> inzetten. Als de onderwijsinstelling de gesuggereerde maatregelen doorvoert, is het restrisico aanvaardbaar. Aanvullend: SIVON is van oordeel dat deze maatregel als onderdeel van 'privacy by design/default' moet worden gezien en standaard moet worden aangeboden. In de volgende DPIA op deze applicatie wordt dit wederom beoordeeld.	Maatregelen te nemen op niveau onderwijsinstelling
8	Ontoereikende afspraken in de verwerkersovereenkomst (bewaartermijnen en verwijdering na einde contract)	4	"Verwerker zal de verwerkte gegevens in de eerste maand van het volgende kalenderjaar met behulp van een beveiligde online omgeving ter beschikking stellen. De gegevens blijven hier beschikbaar tot het einde van de daaropvolgende maand. Daarna worden de	Topicus	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Naar verwachting eind 2025 (afhankelijk van vaststellen nieuw model door Edu-V).

		gegevens verwijderd en niet verder verwerkt.”				
		Deze overeengekomen passage inclusief de toevoeging 'of eerder op schriftelijk verzoek van Onderwijsinstelling' opnemen in een nieuwe versie van de verwerkersovereenkomst.				
		De bewaartermijn van 3 naar 13 maanden vastleggen in het ROSA-schema, alsook de tekst van de alinea over Onweerlegbaarheid (Toepassing) actualiseren.				

9. Deel E: MODEL lokale DPIA

Dit hoofdstuk bevat de afweging die ieder individueel schoolbestuur zelf moet maken. Het gaat om de rechtmatigheid van de voorgenomen verwerkingen, geconstateerde risico's en genomen en nog te nemen maatregelen om de gevolgen van die risico's te beperken.

Daarnaast benoemt het schoolbestuur – indien van toepassing – extra risico's en aanvullende maatregelen die van toepassing zijn binnen het eigen schoolbestuur.

De tekst van deze bijlage kan gebruikt worden als model/rapportage voor de lokale DPIA.

A. Uitvoering lokale DPIA

Binnen [NAAM SCHOOLBESTUUR] is op basis van de door SIVON uitgevoerde centrale DPIA op ParnasSys een lokale DPIA uitgevoerd in de periode [PERIODE].

Bij de beoordeling in deze lokale DPIA zijn betrokken:

- Bijvoorbeeld [ict-afdeling]
- [lid IBP-team]
- [privacy officer]
- [key-user/gebruiker]
- [vertegenwoordiging betrokkenen]

B. Overwegingen over centrale DPIA

[Bij de uitvoering van de lokale DPIA, worden de volgende onderdelen in de centrale DPIA overwogen:

- beschrijving kenmerken gegevensverwerking;
- beoordeling rechtmatigheid gegevensverwerkingen;
- beschrijving en beoordeling risico's voor de betrokkenen;
- beschrijving voorgenomen maatregelen]

Het team dat betrokken is bij de lokale DPIA heeft de in de centrale DPIA benoemde gegevensverwerking, rechtmatigheid, risicobeoordeling en voorgenomen maatregelen beoordeeld en overgenomen. Hierbij gelden de volgende uitzonderingen en/of toevoegingen: [...].

C. Organisatiespecifieke- en algemene applicatierisico's

Om tot een goede en volledige overweging te komen om onderdeel D te vullen dient er inzicht te komen in de aanwezigheid van basale privacyvereisten binnen het schoolbestuur. Onderstaande tabellen bieden een kader om inzicht te krijgen op de aan- of afwezigheid van belangrijke basismaatregelen. Betrek de bevindingen bij de risicobeoordeling en voer maatregelen door waar nodig.

Risicotabel 1. Organisatiespecifieke risico's

Veilige gegevensverwerking omvat meer dan alleen de verwerkingsomgeving van Basis van ParnasSys. Het vergt ook dat de basis op orde is voor o.a. het besturingssysteem waarop het draait, de kennis en kunde van de gebruiker en het hebben en toepassen van relevant beleid.

Nr.	Beheersmaatregel	Uitgevoerd ?	Opmerking/toelichting
1	Het bestuur heeft een eigen privacycoördinator of privacy officer aangesteld.		
2	De bestuur heeft een (externe) Functionaris Gegevensbescherming aangesteld.		
3	Het bestuur heeft de volgende formele structuren geïmplementeerd: een autorisatiebeleid, toegangsbeheer, toewijzing van verantwoordelijkheden en eigenaarschap betreffende gegevensverwerking.		
4	Het bestuur beschikt over een gedetailleerd autorisatiebeleid, inclusief een autorisatiematrix, specificeert welke toegangs niveaus en rechten per medewerker of rol vereist zijn om hun taken uit te voeren. Het autorisatiebeleid wordt regelmatig geëvalueerd en bijgewerkt om te blijven voldoen aan de veranderende behoeften en veiligheidsvereisten van de school.		
5	Het bestuur beschikt over een datalekprotocol/beleid en past dit actief toe.		
6	Het bestuur beschikt over een wachtwoordbeleid en past dit actief toe.		
7	Het bestuur beschikt over een bewaartermijnenbeleid en protocol opschonen en past dit actief toe.		
8	Het bestuur beschikt over een actueel IBP beleid en heeft deze laten vaststellen.		
9	Het bestuur beschikt over een procedure rechten van betrokkenen en past dit actief toe.		
10	Het bestuur beschikt over een DPIA beleid en laat minimaal eens per drie jaar DPIA's herbeoordelen.		
11	Het bestuur beschikt over een gedragscode met richtlijnen hoe gebruikers op een verantwoorde en veilige manier gebruik mogen maken van ICT-middelen en internet en past dit actief toe. Daarbij is specifieke aandacht voor het opslaan, printen, e-mailen en andere vormen van uitwisseling van gedownloade bestanden vanuit de applicatie.		
12	Het bestuur werkt volgens een PDCA-cyclus m.b.t. de AVG waarbij er periodiek wordt gekeken of men compliant is en wat er verbeterd kan worden.		
13	Het bestuur voldoet aan de transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over het gebruik van digitale leermiddelen.		
14	Het bestuur voldoet aan de transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over de wijze waarop de ouders (of leerlingen > 16 jaar) hun rechten kunnen uitoefenen.		

Risicotabel 2. Algemene applicatiespecifieke risico's

Deze risicotabel presenteert een overzicht van beheersmaatregelen die bedoeld zijn om de algemene risico's, die inherent zijn aan de verwerking, te adresseren. Deze maatregelen zijn tevens van toepassing op vergelijkbare verwerkingen bij andere leveranciers. Ze omvatten diverse aspecten, zoals het afsluiten van passende verwerkersovereenkomsten en het

verstrekken van instructies aan medewerkers over het invullen van gegevens in open velden.

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	Het bestuur heeft de Verwerkersovereenkomst met verwerker beoordeeld, getekend en gearchiveerd. Hier zijn onder meer afspraken vastgelegd over bewaartermijnen en de wijze waarop partijen elkaar informeren in het geval van een datalek.		
2	Het bestuur heeft de verwerking van persoonsgegevens middels de applicatie, opgenomen in het register van verwerkingen van zowel leerlingen als medewerkers.		
3	Het bestuur heeft duidelijke afspraken gemaakt over de invoer bij open velden. Dit kan bijvoorbeeld aan de hand van vastgesteld beleid of protocollen zijn geïmplementeerd. Hierin is vastgesteld of het gebruik van vrije invulvelden noodzakelijk is en zo ja voor welke informatie. Over deze uitgangspunten is duidelijk gecommuniceerd met alle medewerkers die gebruik maken van de applicatie.		
4	Het bestuur houdt rekening met dataminimalisatie voor verwerken van persoonsgegevens in de applicatie.		
5	Het bestuur controleert periodiek de gebruikersaccounts op de juistheid en actualiteit van <u>toegekende toegangsrechten(rollen)</u> . De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
6	Het bestuur voert periodieke controles uit op de inrichting van gebruikersaccounts, met speciale aandacht voor het uitsluitend toestaan van <u>persoonlijk identificeerbare accounts</u> . De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
7	Het bestuur heeft autorisaties ingericht op basis van 'need to know' (role based access).		
8	Het bestuur voert periodieke controles uit op de actualiteit en kwaliteit van persoonsgegevens van medewerkers, leerlingen en ouders/verzorgers in de applicatie. De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
9	Het bestuur schoont periodiek de leerlingen- en medewerkersdossiers op waarvan de bewaartermijn is verlopen, conform de geldende wetgeving. De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
10	Het bestuur controleert periodiek de logbestanden. De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
11	Het bestuur heeft een verantwoordelijke (proceseigenaar) binnen de organisatie aangewezen, die periodiek rapporteert aan het bestuur over de uitgevoerde controles, waarbij een overzicht van afwijkingen wordt gedeeld en mogelijke verbeteringen worden voorgesteld.		
12	Het bestuur heeft bij het uitvoeren van de lokale DPIA de betrokkenen om hun mening gevraagd over de verwerking en deze meegenomen in de DPIA (artikel 35 lid 9 AVG). Dit kan bijvoorbeeld via de medezeggenschapsraad.		
13	Het bestuur heeft een functioneel beheerder aangewezen voor de applicatie.		
14	Persoonsgegevens worden niet op verkeerde plekken opgeslagen omdat regels en/of bekendheid met ParnasSys dit voorkomt. Er is daarom geen sprake van een schaduwadministratie op verschillende schijven en mappen van medewerkers.		
15	Het bestuur neemt verantwoordelijkheid voor het veilig koppelen van ParnasSys met andere koppelpartijen.		
16	Het bestuur neemt verantwoordelijkheid dat gebruikers van de applicatie afdoende zijn/worden getraind in het gebruik ervan.		

Risicotabel 3. Op schoolniveau te mitigeren risico's.

Specifieke risico's en maatregelen voortgekomen uit de praktijkbeoordeling van het gebruik van Basis van ParnasSys.

Risico	Te nemen maatregel	Uitgevoerd?	Opmerking/toelichting
Risico op onjuiste of onrechtmatige verwerking van leerlinggegevens.	De onderwijsinstelling biedt medewerkers een gerichte instructie of training aan over het juist verwerken van persoonsgegevens in de applicatie, met speciale aandacht voor gevoelige en bijzondere gegevens, zoals leerresultaten, medische informatie en rubrieken met vrije invulvelden en leerlingnotities.		
Risico op verzending van (bijzondere) persoonsgegevens zonder passende beveiligingsmaatregelen.	De onderwijsinstelling zal gebruikers instrueren over het juiste gebruik van de e-mailfunctie binnen de applicatie en worden op de hoogte gesteld van het aanwezige veilig alternatief voor het versturen van berichten met gevoelige of bijzondere persoonsgegevens naar derden.		
Risico op organisatorische kwetsbaarheid.	De onderwijsinstelling beschikt over een taak – en werkprocesbeschrijving voor de accountbeheerder(s) en applicatiebeheerder(s) van de applicatie en daarnaast is er nagedacht over een back-up voorziening voor het bovenschoolse applicatiebeheer.		
Risico op onvoldoende naleving van de procedures.	De onderwijsinstelling heeft middels een <i>'Inrichtingsdocument'</i> specifiek de regels vastgelegd omtrent de inrichting, gebruik, beheer en controles van de applicatie.		
Risico op onduidelijkheid over eindverantwoordelijk.	De onderwijsinstelling heeft een proceseigenaar voor de applicatie aangesteld.		
Risico op verwerking zonder geldige rechtsgrondslag.	De organisatie heeft afzonderlijke verwerkersovereenkomsten met de koppelpartners beoordeeld, ondertekend en gearchiveerd.		
Risico op het uitwisselen van teveel gegevens met derde partijen.	De onderwijsinstelling controleert vooraf het koppelvlak op inhoud en noodzaak.		
Risico op het uitwisselen van teveel persoonsgegevens met derde partijen.	De onderwijsinstelling voert periodiek controles uit, op de actualiteit van de koppelvlakken (Slapende - nieuwe – openstaande aanvragen). De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
Risico op overtreding van het beginsel van gegevensbeperking	De onderwijsinstelling hanteert standaard groepsautorisatie voor alle gebruikersaccounts en bepaalt zelf, afhankelijk van de rol, of de mogelijkheid om deze tijdelijk op te heffen aan of uit staat.		
Risico op ongeautoriseerde of onrechtmatige toegang tot persoonsgegevens.	De onderwijsinstelling controleert periodiek de opgegeven reden voor tijdelijke opheffing van een groepsautorisatie. De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
Risico op ongeautoriseerde toegang.	De onderwijsinstelling voert periodieke controles uit op gebruikersaccounts (Slapende, accounts zonder actieve aanstelling – accounts zonder 2FA) en onderneemt actie of verwijdert deze		

	indien nodig. De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
Risico op onrechtmatige gegevensoverdracht.	De inhoud van het OSO-dossier is samengesteld volgens de richtlijnen van het Besluit uitwisseling leer- en begeleidingsgegevens. Medewerkers zijn geïnstrueerd om de juiste keuzes te maken en registreren de ouderinzage van het OSO-dossier in de applicatie.		
Risico op onrechtmatige of onnodige verwerking van persoonsgegevens	De onderwijsinstelling heeft duidelijke afspraken vastgelegd over het invoeren van gegevens in open velden en over dataminimalisatie. Dit kan bijvoorbeeld aan de hand van vastgesteld beleid of protocollen die zijn geïmplementeerd. Hierin is bepaald of het gebruik van vrije invulvelden noodzakelijk is en zo ja voor welke informatie. Ook is gedefinieerd wat wordt verstaan onder dataminimalisatie. Over deze uitgangspunten is duidelijk gecommuniceerd met alle medewerkers die gebruik maken van de applicatie.		
Risico op ongeautoriseerde toegang.	De onderwijsinstelling heeft technische of organisatorische beheersmaatregelen genomen om ervoor te zorgen dat de downloadmap van elke lokale computer regelmatig wordt geleegd.		
Risico op ongeautoriseerde toegang.	De onderwijsinstelling heeft standaard tweefactorauthenticatie (2FA) ingeschakeld voor alle medewerkersaccounts met toegangsrechten, inclusief de beheerdersaccountants.		
Risico van onopgemerkt verlies van bescherming.	De onderwijsinstelling controleert periodiek de instellingen voor het inschakelen van 2FA-authenticatie voor gebruikers.		
Risico van te ruime toegang tot (gevoelige) gegevens.	De vastgestelde autorisaties zoals (stapel-)rollen en rechten binnen de onderwijsinstelling worden periodiek gecontroleerd op het juist toepassen hiervan of passend bij de actuele werkzaamheden (met name stapelrollen).		
Risico op geen sluitend autorisatiebeheer en verhoogd risico op datalek.	De onderwijsinstelling heeft een einddatum ingesteld voor tijdelijke krachten, afgestemd op de noodzakelijke duur, met een maximum van één schooljaar.		
Risico op schending van bewaartermijn en het beginsel van minimale gegevensverwerking	Bij het opschonen van persoonsgegevens, na verlopen bewaartermijn, worden gegevens verwijderd uit het leerlingdossier, maar niet uit de groepsdocumenten in de Groepsmap.		
Risico op schending van bewaartermijn en het beginsel van minimale gegevensverwerking	Adresgegevens van (oud-)leerlingen worden door de school uitsluitend met toestemming van de leerling bewaard (buiten ParnasSys) voor het organiseren van reünies.		

D. Overwegingen implementatie en lokale DPIA: aanvullende risico's en maatregelen

In aanvulling op de in de centrale DPIA gevonden risico's en maatregelen, heeft de implementatie en gebruik van ParnasSys binnen [NAAM SCHOOLBESTUUR] verdere gevolgen voor de rechten en vrijheden van de betrokkenen.

[Overweeg hierna de mogelijke impact op de rechten en vrijheden van betrokkenen en eventuele schade of zelfs (fysiek of emotioneel) letsel die het gebruik van ParnasSys kan veroorzaken. Weeg hierbij mogelijk risico's mee op het gebied van:

- onvermogen om rechten uit te oefenen (inclusief maar niet beperkt tot privacyrechten);
- onvermogen om toegang te krijgen tot diensten of kansen;
- verlies van controle over het gebruik van persoonsgegevens;
- discriminatie;
- identiteitsdiefstal of fraude;
- financieel verlies;
- reputatieschade;
- verlies van vertrouwelijkheid;
- heridentificatie van gepseudonimiseerde gegevens; of
- elk ander significant economisch of sociaal nadeel
- gevolgen en risico's voor de beveiliging van ParnasSys.

[NAAM SCHOOLBESTUUR] identificeert een aantal aanvullende risico's. Deze worden beoordeeld aan de hand van de kans (waarschijnlijkheid) als de impact (ernst). Het risico wordt beoordeeld aan de hand van de volgende indeling en berekening:

$$\text{kans (waarschijnlijkheid)} \times \text{impact (ernst)} = \text{risico}$$

Om een objectieve inschatting maken van de risico's wordt gebruik gemaakt van de volgende gestructureerde matrix van risicoclassificatie:

RISICO	Kans Laag (1)	Kans Midden (2)	Kans Hoog (3)
Impact Hoog (3)	Risico Midden (Score: 3)	Risico Hoog (Score: 6)	Risico zeer hoog (Score: 9)
Impact Midden (2)	Risico Laag (Score: 2)	Risico Midden (Score: 4)	Risico Hoog (Score: 6)
Impact Laag (1)	Risico Zeer laag (Score: 1)	Risico Laag (Score: 2)	Risico Midden (Score: 3)

NB een score van 1 levert dus een zeer laag risico op, terwijl een score van 9 een zeer hoog risico oplevert.

Risico's kunnen worden beperkt door maatregelen te nemen. Deze maatregelen zullen de kans en/of impact verkleinen. Daarmee blijft er een risico over: het restrisico. Rekenkundig uitgelegd betekent dit:

$$[\text{kans (waarschijnlijkheid)} \times \text{impact (ernst)}] - [\text{de risico-mitigerende maatregelen}] = \text{restrisico}$$

De in de lokale DPIA geconstateerde risico's betreffen:

[RISICO]						
[toelichting risico]						
Risico-afweging	kans		impact		Risico	
Maatregel/maatregelen	[beschrijving maatregel]					
Eigenaar maatregel	[wie is verantwoordelijk voor uitvoeren maatregel: benoem de eigenaar]					
Maatregelen geïmplementeerd?	[is de maatregel al gepland, zo niet wanneer wordt deze gepland]					
IRisico-afweging <u>RESTRISICO</u>	kans		impact		<u>RESTRISICO</u>	
NB: het restrisico betreft het risico indien de maatregel <u>wel</u> wordt uitgevoerd. Zonder maatregel resteert het oorspronkelijke risico.						

[dupliceer de tabel zo vaak als nodig om aanvullende risico's te beschrijven]

E. Verklaring en advies functionaris voor gegevensbescherming (FG)

De FG heeft kennis genomen van de in de door SIVON uitgevoerde centrale DPIA, geconstateerde risico's en aanbevolen maatregelen.

De FG is [wel/niet] betrokken geweest bij uitvoering en opstellen van de lokale DPIA voor [NAAM SCHOOLBESTUUR]. [beschrijving rol fg schoolbestuur bij deze DPIA]

Het advies van de FG is [...].

F. Visie betrokkenen

In het kader van dit DPIA zijn de betrokkenen, te weten [leerlingen, hun ouders en medewerkers] [betrokken/geïnformeerd] over de uitkomst.

[Zijn de betrokkenen, op wie de verwerking betrekking heeft, geraadpleegd over dit DPIA en wat is hun mening over de verwerking? Zo nee, waarom niet?]

De concept DPIA wordt aan (G)MR voorgelegd, waarbij de (G)MR als vertegenwoordiging van betrokken kan aangeven of de gegevensverwerking aansluit bij hun verwachting en of hierover zorgen bestaan.

G. Conclusie

Op basis van het onderzoek dat in het kader van de centrale DPIA, alsmede de lokale DPIA is uitgevoerd, zijn de gevolgen voor de rechten en vrijheden van deze betrokkenen door de verwerking van persoonsgegevens van onderwijsdeelnemers en medewerkers in ParnasSys - na toepassing van risico-mitigerende maatregelen – in [onvoldoende/voldoende/goede] mate beheerst.

Deze conclusie wordt anders als de in deze DPIA genoemde maatregelen door het schoolbestuur niet of onvoldoende worden uitgevoerd.

De genomen en te nemen maatregelen, waarborgen, veiligheidsmaatregelen en mechanismen die binnen ParnasSys de bescherming van persoonsgegevens garanderen, zijn [onvoldoende/voldoende/goed] gericht op het beperken van de risico's voor de rechten en vrijheden van betrokkenen.

Er is [wel/niet] gebleken van hoge risico's voor de rechten en vrijheden van betrokkenen die moet leiden tot een 'voorafgaande raadpleging' zoals omschreven in artikel 36 AVG.

H. Risico-mitigerende maatregelen schoolbestuur

Bij deze beoordeling zijn een aantal risico's geïdentificeerd waarbij de leverancier een aantal maatregelen neemt. Hiernaast moet het schoolbestuur maatregelen nemen of treffen om de benoemde risico's te beperken. Het betreffen de hierna te noemen maatregelen waarbij de verantwoordelijkheid voor de implementatie bij het schoolbestuur (de verwerkingsverantwoordelijke) ligt.

Het schoolbestuur moet daarom zorgen voor:

1. goede gebruiksinstructies voor beheerder en gebruikers (op school) van ParnasSys, om verkeerd gebruik, misbruik of beveiligingsincidenten te voorkomen. Hierbij wordt gebruikt gemaakt van het ParnasSys kennisportaal en de beleiddocumenten onderwijsinstelling.
2. het inregelen van de correcte autorisaties in ParnasSys. Zorg hierbij voor functiescheiding waarbij in geval van autorisatieverlening gewerkt wordt met het vier-ogenprincipe.
3. het informeren de leerlingen, hun ouders en medewerkers over deze DPIA en de (mogelijke) gevolgen voor de rechten en vrijheden die deze betrokkenen.
4. [BESCHRIJF HIER DE MAATREGELEN ZOALS OPGENOMEN BIJ HET ONDERDEEL "Overwegingen implementatie en lokale DPIA"]

De onder de nummers [NUMMER] genoemde punten moeten op een termijn van [TERMIJN] worden uitgevoerd.

I. Aanbevelingen

Naast de hiervoor genoemde bevindingen en maatregelen, zijn er een aantal aanbevelingen die buiten scope van deze DPIA vallen omdat zij niet binnen de invloedssfeer van (de leverancier van) ParnasSys liggen, terwijl deze aanbevelingen cq. maatregelen in beeld zijn gekomen bij deze DPIA en/of wel bijdragen aan het beperken van risico's:

- A. ...
- B. ...

J. Verklaring schoolbestuur

Het schoolbestuur, aangemerkt als vertegenwoordiging van verwerkingsverantwoordelijke [NAAM SCHOOLBESTUUR], overwegende de conclusies, risico-mitigerende maatregelen en het aanbevelingen, verklaart hierbij:

- I. kennis te hebben genomen van inhoud en uitkomsten van deze centrale en lokale DPIA;
- II. in te stemmen met de in de rapportage genoemde beheersmaatregelen;
- III. opdracht te geven voor het uitvoeren van de beheersmaatregelen (zie hiervoor onder H.) binnen de daarbij genoemde termijnen;
- IV. de - in dit rapport - vermelde resterende risico's te aanvaarden;
- V. deze DPIA na een periode van [PERIODE/JAAR] te laten herzien, of eerder indien nodig;
- VI. [wel/geen] voorafgaande raadpleging bij de Autoriteit Persoonsgegevens in te dienen;
- VII. het DPIA-team decharge te verlenen.

EN BESLUIT [NA (HER)OVERWEGING] HET GEBRUIK VAN [SYSTEEM] [WEL/NIET] TE [GEBRUIKEN/CONTINUEREN].

Naam bestuurder(s):

Plaats:

Datum:

Ondertekening:

Bijlage 1: Gebruikte termen en definities

Alle type gegevens worden beschouwd als persoonsgegevens als ze direct of indirect tot een persoon te herleiden zijn. Deze definitiebepalingen hebben tot doel om consistentie te bieden bij het begrijpen van verschillende (wettelijke) termen en concepten die worden gebruikt bij de naleving van de AVG.

Anonieme gegevens Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Relevante privacy wet- en regelgeving zijn niet van toepassing op deze gegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie de persoonsgegevens betrekking hebben, niet (meer) identificeerbaar is. Let op: het anonimiseren van persoonsgegevens als handeling is een verwerking van persoonsgegevens en valt wel onder privacy wet- en regelgeving.

Betrokkenen personen waarop de gegevens betrekking hebben Betrokkenen zijn alle geïdentificeerde of identificeerbare natuurlijke personen binnen de gegevensverwerkingen, oftewel de personen over wie de persoonsgegevens worden verwerkt. Denk hierbij aan: leerlingen, medewerkers, cliënten, zakelijke contacten, gebruikers en bezoekers.

Bijzondere persoonsgegevens mogen alleen verwerkt worden als je een beroep kunt doen op een uitzondering. Voor het onderwijs geldt bijvoorbeeld dat gezondheidsgegevens alleen gebruikt mogen worden als dat noodzakelijk is voor het geven van onderwijs en het begeleiden van een leerling. Ze zijn bijzonder omdat het gebruik van deze gegevens iemands privacy ernstig kan beïnvloeden. Voorbeelden zijn gezondheidsgegevens, levensovertuiging, lidmaatschap van de vakbond, ras of etnische afkomst.

Diagnostische gegevens zijn gegevens over het individuele gebruik van de diensten. Bijvoorbeeld: hoe vaak je inlogt, welk soort documenten je opslaat, leest etc.. Deze gegevens komen in logbestanden terecht van de clouddienst. [Deze data wordt ook soms servicegegevens genoemd.] **Metadata** is een andere categorie gegevens die ook over gebruik gaan, zoals de locatie van gebruik, tijdstip, en device type.

Functionele gegevens zijn gegevens die een (cloud)dienst nodig heeft om de dienst te kunnen leveren.

Gevoelige persoonsgegevens gaan over gegevens die volgens de Autoriteit Persoonsgegevens (AP) snel inbreuk (kunnen) maken op de persoonlijke levenssfeer. Het gaat bijvoorbeeld om leerresultaten van kinderen, omdat daar conclusies aan kunnen worden verbonden met gevolgen voor het latere maatschappelijke leven. Of het gaat om grote verzamelingen van informatie van (zeer) jonge kinderen, gegevens over (problematische) gezinssituatie of³⁹ zwaardere eisen gesteld aan de beveiliging van de gegevens.

³⁹ https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf

Inhoudelijke gegevens is de inhoud van bijvoorbeeld een document dat je online opslaat.

Kwetsbare groepen De categorieën van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere betrokkenen. Denk hierbij aan minderjarigen en etnische minderheden. De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader.

Nationale identificatienummers

Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. Het gebruik van deze nummers dient dus met uiterste zorgvuldigheid plaats te vinden en de noodzakelijkheid om deze nummers te gebruiken dient goed onderbouwd te zijn. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijkt en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormt. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers. Denk hierbij aan:

- Burgerservicenummer (BSN)
- BIG-nummer (beroepen in de individuele gezondheidszorg),
- A-nummer (basisregistratie personen),
- Onderwijsnummer of Persoonsgebonden nummer (PGN),
- Strafrechtketennummer

Persoonsgegevens Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. De term ‘natuurlijke personen’ betekent hier levende mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in principe geen persoonsgegevens. Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.

Hieronder staan voorbeelden van categorieën persoonsgegevens en type persoonsgegevens die binnen die categorie vallen:

- Naam (voornaam, achternaam, voorvoegsel, initialen)
- Contactgegevens (huisadres, telefoonnummer, e-mailadres)
- Demografische gegevens (leeftijd, geboortedatum en -plaats, geslacht, nationaliteit, opleiding, IQ)
- Apparaat- en internetgegevens (IP-adres, MAC-adres, metadata, locatie-informatie en geografische informatie)
- Financiële gegevens (bankrekeningnummer en -saldo, inkomens- en vermogensgegevens, loonschaal, kredietwaardigheid, winst eenmanszaak)
- Werk gerelateerde gegevens (KvK-nummer, verslag van een functioneringsgesprek,

documentatie over negatief gedrag op de werkvloer)

- Overige persoonsgegevens (voertuigidentificatienummer, persoonlijke voorkeuren)

Ook metadata zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Over het algemeen is een type metadata op zichzelf niet voldoende identificerend, maar meestal worden meerdere type metadata verzameld van gebruikers. Al deze gegevens gecombineerd met elkaar kan leiden tot identificeerbaarheid van een individu.

Pseudonieme persoonsgegevens Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eisen verbonden dat de sleutels apart worden bewaard en dat maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld. Of pseudonieme gegevens door de ontvanger (verwerker) als persoonsgegevens aangemerkt moeten worden hangt af van de omstandigheden van het geval. Het uitvoeren van een toets zal kunnen uitwijzen in hoeverre deze door de leverancier te herleiden zijn tot persoonsgegevens⁴⁰.

⁴⁰ Het Gerecht EU 23 april 2023, T557/20, ECLI:EU:T:2023:219

Bijlage 2: Uitleg risico's

Negatieve gevolgen van de gegevensverwerking zijn bijvoorbeeld (het risico op):

- onvermogen om rechten uit te oefenen (inclusief maar niet beperkt tot privacyrechten);
- onvermogen om toegang te krijgen tot diensten of kansen;
- verlies van controle over het gebruik van persoonsgegevens;
- discriminatie;
- identiteitsdiefstal of fraude;
- financieel verlies;
- reputatieschade;
- lichamelijk letsel;
- verlies van vertrouwelijkheid;
- heridentificatie van gepseudonimiseerde gegevens; of
- elk ander significant economisch of sociaal nadeel
- Inbreuk op de rechten van kinderen (kinderrechten).

Om te beoordelen wat het risico is, wordt de kans dat het risico zich voordoet (waarschijnlijkheid) gewogen tegenover de ernst van de mogelijke schade. Schade hoeft niet onvermijdelijk te zijn om als risico of hoog risico te kwalificeren. Het moet meer dan ver weg zijn, maar elke significante kans op zeer ernstige schade kan nog steeds voldoende zijn om als een hoog risico te kwalificeren. Evenzo kan een grote kans op wijdverspreide maar meer kleine schade nog steeds als een hoog risico gelden.

Hulpmiddel beoordelen score laag, midden en hoog

Laag	Midden	Hoog
Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende meerdere dagen brengt geen merkbare (meetbare) schade toe. Blijvende juistheid van informatie (vanaf de bron tot het laatste gebruik) is gewenst, maar hoeft niet gegarandeerd te zijn.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een of meerdere dagen brengt merkbare schade toe. Sommige afwijkingen in data zijn toelaatbaar, juistheid data is belangrijk maar niet kritisch.	Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe. Juistheid informatie moet gegarandeerd zijn, noodzakelijk dat data correct is.
Weinig tot geen schade	Enige schade, invloed of gevolgen	Grote – onvermijdelijke –ernstige schade, nadeel en gevolgen; imago.
Kans = gebeurt bijna nooit; 1 maal per school jaar of minder <u>Kleine kans</u>	Kans = gebeurtenis kan zich voordoen; meerdere malen per schooljaar <u>Een redelijke kans</u>	Kans = deze gebeurtenis zal zich bijna zeker voordoen; per maand, week of zelfs dag De kans dat het zich voordoet is groter, dan de kans dat het niet gebeurt

Bijlage 3: Document Topicus inzake versleuteling (encryptie)

Versleuteling Data ParnasSys

03-2025

In de security documentatie van ParnasSys, welke inzichtelijk is geweest voor geautoriseerde auditors, staat onderbouwd hoe er *zorgvuldige maatregelen* zijn ter preventie van het ontvreemden van data langs:

1. Fysieke toegang tot databases
2. Logische/digitale toegang tot databases

Naar aanleiding van deze DPIA, enkele aanvullende toelichtingen:

Versleuteling en data in rust

ParnasSys maakt gebruik van state-of-the-art encryptie methoden, waaronder encryptie van data in rust, en is toegewijd aan het voortdurend versterken van de veiligheidsmaatregelen. Deze zorgvuldige marktconforme maatregelen reflecteren onze inzet om de gegevens van onze klanten volledig te beschermen.

Extra toelichting

Data in transit is encrypted en er is encryptie van data in rust. Er is extra hardware-level encryptie op de database servers. En ook database backups zijn op de daarvoor bestemde storage versleuteld in rust.

Data is niet direct vanuit het internet te benaderen en beschermd met een multi-tier beveiligingslaag. Toegang is uitsluitend via specifieke stepping stones met geautoriseerde toegang mogelijk.

Dit levert samen met:

- De meerlaags firewalls,
 - IDP en IPS,
 - En de hoogwaardige fysieke beveiliging in afgesloten ruimte in een Tier3+ datacentrum, conform o.a. ISO27001, NEN7510, SOC2.
- (Voor volledigheid zie <https://previder.nl/certificeringen>)

Een passend en zeer laag netto risico op (volgens ons, maar ook de hierbij betrokken partners en experts).

Dit weerhoudt ons niet om verder te kijken en extra lagen van beveiliging te onderzoeken.

Voortdurend versterken van de veiligheidsmaatregelen

Richtingen waarin Topicus.Education de ontwikkelingen volgt en kansrijke verbeteringen ook test, uitprobeert en bij succes implementeert komen uit de breedte van de markt.

Waarbij NIST een belangrijk adviesorgaan is. Zie ook:

<https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines> voor thema's die we volgen ten aanzien van encryptie.