|  |
| --- |
| DPIA ParnasSysLeerlingadministratiesysteem (LAS) |
| **[naam schoolbestuur]****[maand] [jaar]** |

Inhoud

[Managementsamenvatting 3](#_Toc67325808)

[1. Inleiding 5](#_Toc67325809)

[1.1. Wat is een DPIA? 5](#_Toc67325810)

[1.2. Waarom een DPIA? 5](#_Toc67325811)

[1.3. Aanpak DPIA 5](#_Toc67325812)

[1.4. Leeswijzer 5](#_Toc67325813)

[2. Beschrijving van de gegevensverwerking 6](#_Toc67325814)

[2.1. Algemeen 6](#_Toc67325815)

[2.2. Periode en afbakening DPIA 6](#_Toc67325816)

[2.3. Technieken en methoden 6](#_Toc67325817)

[2.4. Juridisch / beleidsmatig kader 6](#_Toc67325818)

[2.5. Te verwerken persoonsgegevens 7](#_Toc67325819)

[2.6. Doeleinden en grondslagen 8](#_Toc67325820)

[2.7. Betrokken partijen 8](#_Toc67325821)

[2.8. Gegevens Verwerker(s) 9](#_Toc67325822)

[3. Beoordeling rechtmatigheid van de verwerking 11](#_Toc67325823)

[3.1. Bijzondere persoonsgegevens 11](#_Toc67325824)

[3.2. Verwachting en mening betrokkenen 11](#_Toc67325825)

[3.3. Borging van rechten van de betrokkenen 11](#_Toc67325826)

[3.4. Verwerkersovereenkomst 11](#_Toc67325827)

[3.5. Noodzaak en evenredigheid 11](#_Toc67325828)

[4. Beoordeling risico’s 12](#_Toc67325829)

[4.1. Berekening risicoscore 12](#_Toc67325830)

[4.2. Geïnventariseerde risico’s 12](#_Toc67325831)

[5. Beschrijving van aanbevolen maatregelen 18](#_Toc67325832)

[5.1. Beleid en organisatie 18](#_Toc67325833)

[5.2. Personeel, leerlingen en gasten 19](#_Toc67325834)

[5.3. Ruimten en apparatuur 20](#_Toc67325835)

[5.4. Continuïteit 20](#_Toc67325836)

[5.5. Vertrouwelijkheid en integriteit 21](#_Toc67325837)

[5.6. Controle en logging 23](#_Toc67325838)

[6. Conclusie, aanvaarding en goedkeuring 25](#_Toc67325839)

[6.1. Algemene conclusie 25](#_Toc67325840)

[6.2. Conclusie beoordeling rechtmatigheid 25](#_Toc67325841)

[6.3. Aanvaarding restrisico’s 25](#_Toc67325842)

[6.4. Advies Functionaris Gegevensbescherming 25](#_Toc67325843)

[6.5. Raadpleging verwerker 25](#_Toc67325844)

[6.6. Raadpleging betrokkenen 25](#_Toc67325845)

[6.7. Follow up 25](#_Toc67325846)

[7. Vaststelling en aanvaarding 26](#_Toc67325847)

[8. Verklaring begrippen en afkortingen 27](#_Toc67325848)

[Bijlage A – Instructie controle en aanvulling DPIA-rapport 29](#_Toc67325849)

**Colofon**

**Versie** 1.2 (april 2021)

**Bronnen** Algemene Verordening Gegevensbescherming / GDPR (Europees Parlement, 2016)

Guidelines on Data Protection Impact Assessment (WP29, 2017)

Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming (Ministerie van Justitie en Veiligheid, 2018)

Handreiking Data Protection Impact Assessment (NOREA, 2020)

Handreiking DPIA po/vo (Kennisnet, 2019)

Model gegevensbeschermingseffectbeoordeling Rijksdienst (Rijksoverheid, 2017)

Toetsingskader Privacy versie 3.1 (Kennisnet, saMBO-ICT, 2020)

**Auteurs** De vertegenwoordigers van de volgende schoolbesturen: SKPO, Onderwijsgroep Buitengewoon, ASKO, Catent en INOS. Binnen het Netwerk Informatiebeveiliging en privacy po/vo.

**Met dank aan** Kennisnet en SIVON. Ondersteund door Privacy op School, Berenschot en Vos juridisch advies.

**Licentie** Creative Commons 3.0 Nederlands (CC BY 3.0 NL)

De gebruiker mag deze publicatie kopiëren, verspreiden, doorgeven, remixen en afgeleide werken maken onder de voorwaarde van het vermelden van de naam en bron.

*Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s) geen aansprakelijkheid voor eventuele fouten, onvolkomenheden of schade als gevolg van het gebruik van dit document.*

# Managementsamenvatting

Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor

de rechten en vrijheden van natuurlijke personen, dan dient er voorafgaand aan de verwerking een

zogenaamde gegevensbeschermingseffectbeoordeling uitgevoerd te worden. In de praktijk wordt deze beoordeling ook wel Data Protection Impact Assessment (DPIA) genoemd. Een DPIA is bedoeld om inzicht te krijgen in de privacyrisico’s van verwerkingen van persoonsgegevens en de maatregelen die nodig zijn om deze risico’s te beperken (mitigeren). De schoolbestuurder is, als Verwerkingsverantwoordelijke, verantwoordelijk voor de inhoud en opvolging van het DPIA rapport.

Op basis van het onderzoek dat in het kader van de DPIA voor ParnasSys is uitgevoerd, is de conclusie dat de verwerking van persoonsgegevens een **hoog** risico inhoudt voor de rechten en vrijheden van de betrokkenen.

*Inzicht in riscio’s*

In deze rapportage leest u de risico’s die zijn geïnventariseerd rondom de gegevensverwerking in ParnasSys. De belangrijkste risico’s (score 6-9) betreffen de volgende:

1. Er worden meer rechten toegekend aan gebruikers dan noodzakelijk.
2. Het is niet mogelijk de gegevensuitwisseling die middels geautomatiseerde koppelingen gedeeld worden te wijzigen/filteren.
3. Het bekijken (downloaden) van bestanden in leerlingendossiers (op privé devices) zorgt voor een lokale kopie van het dossier.
4. Er wordt geen goed gebruik gemaakt van groepsgebaseerde toegang (groepsautorisatie of sublesgroepen)
5. Adresgegevens van medewerkers moeten verplicht ingevoerd worden
6. De toegekende autorisaties binnen scholen zijn niet vastgelegd in beleid.
7. Er is geen specifiek beleid met betrekking tot het beheren van accounts.
8. Wachtwoorden worden niet periodiek gewijzigd en zijn niet complex.
9. Informatie van leerlingen wordt buiten systeem om gedeeld door handmatige exports, printjes en via onbeveiligde mails of usb-sticks uitgewisseld.
10. Bijlagen bij OSO toevoegen (zonder inzage of toestemming) waardoor er meer wordt uitgewisseld dan toegestaan.
11. Wachtwoorden worden verkeerd gebruikt
12. De ontheffingsoptie van de groesautorisatie ‘tijdelijke toegang’ is niet bekend waardoor niet gekozen wordt om de groepsautorisatie toe te passen.
13. Bij het opschonen van persoonsgegevens, na verlopen bewaartermijn, worden gegevens verwijderd uit het leerlingdossier, maar niet uit de groepsdocumenten in de groepsmap.
14. De logging van gebruikersactiviteiten wordt niet (periodiek) gemonitord.

*Beperkende maatregelen*

Op basis hiervan worden de volgende maatregelen voorgesteld met de prioritering Hoog:

1. Persoonsgegevens worden opgeschoond volgens het vastgestelde beleid voor bewaren en opschonen (AVG art. 5).
2. Toegang tot persoonsgegevens wordt verleend volgens het vastgestelde toegangs-beveiligingsbeleid (ISO 5.1.1).
3. Medewerkers die gebruik maken van het LAS worden geschoold in het juist verwerken van persoonsgegevens (ISO 7.2.2).
4. Lokale kopieën van bestanden met persoonsgegevens worden opgeschoond (AVG art. 5).
5. Er mogen niet meer persoonsgegevens worden uitgewisseld via geautomatiseerde koppelingen dan strikt noodzakelijk en alleen op basis van grondslag en doelbinding (AVG art. 5, 6, 25).
6. Er mogen niet meer persoonsgegevens worden geregistreerd dan strikt noodzakelijk (AVG art. 5).
7. Er vinden periodieke controles plaats op het juist toepassen van het toegangsbeveiligingsbeleid (ISO 9.2.5).

*Uit te voeren beheersmaatregelen*

Het rapport biedt per bovengenoemd statement concrete beheersmaatregelen die door het schoolbestuur binnen een redelijk maar afzienbaar termijn geïmplementeerd moeten zijn om de restrisico te mitigeren tot een acceptabel niveau. In dat kader wordt aanbevolen om de volgende beheersmaatregelen op te nemen en uit te laten voeren door de Verwerker (Topicus):

1. Het periodiek wijzigen van wachtwoord en/of de complexiteit van het wachtwoord kan afgedwongen worden in de applicatie.
2. Groepsautorisaties kunnen bij bepaalde rollen als ‘default setting’ ingesteld worden
3. Er kan op leerlingniveau of onderdelen van een leerlingdossier autorisaties ingesteld worden.
4. Inactieve accounts van medewerkers kunnen inzichtelijk gemaakt en opgeschoond worden.
5. Geautomatiseerde koppelingen kunnen in het LAS door of op verzoek van het schoolbestuur ingezien en zo nodig gewijzigd worden op basis van noodzakelijkheid, grondslag en doelbinding.
6. Persoonsgegevens worden bij voorkeur vanuit het LAS uitgewisseld via beveiligde geautomatiseerde koppelingen in plaats van handmatige exports
7. Bestanden met persoonsgegevens kunnen vanuit de applicatie worden ingezien. Het downloaden hiervan wordt beperkt.
8. Het schoolbestuur moet zelf kunnen bepalen welke velden verplicht ingevuld moeten worden, dit moet niet door het LAS worden bepaald.
9. Geautomatiseerde koppelingen waarbij er persoonsgegevens worden uitgewisseld voldoen aan de actuele versie van de Edukoppeling transactie standaard en het Certificeringsschema.

De in hoofdstuk 5 opgenomen maatregelen garanderen in **voldoende** mate de bescherming van de persoonsgegevens van betrokkenen.

**De schoolbestuurder wordt als verwerkingsverantwoordelijke verzocht om de implementatie hiervan goed te keuren (zie hoofdstuk 7).**

# Inleiding

## Wat is een DPIA?

In de Algemene Verordening Gegevensbescherming (AVG), zijn Data Protection Impact Assessments (DPIA’s) verplicht gesteld voor bepaalde type verwerkingen. In de AVG wordt gesproken over Gegevensbeschermingseffectbeoordeling (art. 35 AVG). Doorgaans wordt hiervoor de Engelse afkorting gebruikt, zo ook voor dit document.

## Waarom een DPIA?

Een DPIA is bedoeld om inzicht te krijgen in de privacyrisico’s van verwerkingen van persoonsgegevens en de maatregelen die nodig zijn om deze risico’s te beperken (mitigeren). DPIA’s hoef je alleen uit te voeren voor verwerkingen die gepaard gaan met een hoog risico voor de beperking van de rechten en vrijheden van personen.

Een DPIA is volgens de AVG vereist, wanneer er sprake is van:

1. Een systematische en uitgebreide beoordeling van personen op basis van geautomatiseerde verwerking die gebruikt wordt voor besluitvorming, ook wel ‘profiling’ genoemd.
2. De verwerking van bijzondere persoonsgegevens (gezondheidsgegevens, ras, religie, etc.) of strafrechtelijke feiten of veroordelingen.
3. Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimtes (bijv. cameratoezicht)

Daarnaast heeft de Autoriteit Persoonsgegevens (AP) een lijst opgesteld van 17 verwerkingen waarvoor een DPIA verplicht is[[1]](#footnote-2). Ook zijn er Europese richtlijnen opgesteld[[2]](#footnote-3) en wordt er van een organisatie verwacht dat men zelf een risico-afweging maakt.

Vóór de uitvoering van een DPIA op het leerlingadministratiesysteem ParnasSys, is in een voortraject een pré-DPIA uitgevoerd op basis waarvan is vastgesteld dat een DPIA vereist is. Hieruit kwam naar voren dat er in ieder geval sprake is van vereiste b: De verwerking van bijzondere persoonsgegevens (gezondheidsgegevens, ras, religie, etc.) of strafrechtelijke feiten of veroordelingen.

## Aanpak DPIA

Binnen de onderwijssectoren po en vo worden een aantal leerlingadministratiesystemen (LAS’en) breed gebruikt. Daarom is gekozen voor een generieke aanpak voor het uitvoeren van een DPIA per LAS. Op deze manier worden schoolbesturen als Verwerkingsverantwoordelijken geholpen bij de uitvoering. Dit neemt niet weg dat er ook specifieke risico’s kunnen zijn die voor individuele schoolbesturen gelden. Daarnaast zijn de huidige risico’s met een beperkt aantal schoolbesturen geïnventariseerd. Het huidige rapport is dus niet uitputtend en moet daarom door het schoolbestuur worden gecontroleerd en aangevuld. Om deze reden is het rapport voorzien van een instructie om het DPIA rapport af te ronden (zie bijlage B). Het schoolbestuur is, als Verwerkingsverantwoordelijke, zelf verantwoordelijk voor de inhoud van het DPIA rapport.

## Leeswijzer

De rapportage is als volgt opgebouwd: In hoofdstuk 2 is de gegevensverwerking beschreven die plaatsvindt in ParnasSys. Vervolgens is in hoofdstuk 3 de beoordeling van de rechtmatigheid van deze verwerking beschreven. In hoofdstuk 4 en 5 worden respectievelijke de beoordeling van de risico’s en de te nemen maatregelen beschreven. In hoofdstuk 6 is een verklaring van de Verwerkingsverantwoordelijke (lees: schoolbestuur) en van andere betrokkenen opgenomen, waarmee de bestuurder verklaart kennis te hebben genomen van de uitkomsten van de DPIA, goedkeuring geeft aan de uitvoering van de voorgestelde maatregelen en aangeeft de restrisico’s te zullen accepteren. Tot slot is er in hoofdstuk 7 een lijst opgenomen met een verklaring van gebruikte begrippen en afkortingen.

# Beschrijving van de gegevensverwerking

Dit hoofdstuk kan beschouwd worden als een samenvatting van de gegevensverwerkingsanalyse die gedaan is als onderdeel van de pré-DPIA (bijlage B).

## Algemeen

Hieronder is algemeen omschreven wat de gegevensverwerking behelst en welke (hoofd)processen deze ondersteunt.

|  |
| --- |
| ParnasSys betreft in de basis 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 ParnasSys.Daarnaast bevat ParnasSys een digitaal leerlingvolgsysteem waarin scholen informatie invoeren die belangrijk is voor de school, zodat zij het onderwijs kunnen analyseren en concrete (verbeter)plannen kunnen opstellen. Alle gegevens van de leerlingen worden op individueel niveau vastgelegd (inclusief het ontwikkelingsperspectief) en op groepsniveau 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 ParnasSys.Afbakening: De koppelingen tussen ParnasSys en andere systemen vallen niet onder de scope van de verwerking waarvoor de DPIA is uitgevoerd. Dat geldt ook voor de koppeling en werking van de oudercommunicatie-app Parro. |

##

## Periode en afbakening DPIA

Een DPIA is een momentopname. Processen en systemen waarin de verwerking plaatsvindt, kunnen na verloop van tijd veranderen. Daarom is het van belang dat deze DPIA periodiek herzien en zo nodig bijgesteld wordt. Hieronder is opgenomen in welke periode de DPIA is uitgevoerd en de afbakening die is gehanteerd, zowel ten aanzien van het proces als de systemen.

**Periode uitvoering DPIA**

|  |
| --- |
| November t/m februari 2021 |

**Afbakening**

|  |
| --- |
| Voor de DPIA is met vertegenwoordigers van schoolbesturen met name gekeken naar de verwerking zoals die plaatsvindt in ParnasSys. Er is gericht gekeken naar de basisfuncties van ParnasSys zijnde de leerling administratie en niet specifiek naar de optionele modules en koppelingen. Er is dus niet expliciet gekeken naar WMK , Schoolkassa, Ouderportaal, Ultimview, ZIEN!, MijnSchoolteam, etc. Dat is ook niet gedaan voor specifieke koppelingen tussen ParnasSys en andere systemen, zoals BRON, MS365, Basispoort, OSO, etc. |

## Technieken en methoden

Hieronder is beschreven welke technieken en methoden worden gebruikt bij de gegevensverwerking.

|  |
| --- |
| ParnasSys betreft een zogenaamd Software-as-a-Service (SaaS) voor scholen in het primair en speciaal (basis)onderwijs. Het is dus een webbased applicatie die via de browser kan worden gebruikt. Het systeem bevat diverse gegevenskoppelingen (zowel webservices) met andere aanleverende en afnemende systemen. Daarnaast is het mogelijk om handmatige exports te maken.  |

##

## Juridisch / beleidsmatig kader

Hieronder is beschreven welke wet- en regelgeving, naast de AVG, nog meer van toepassing zijn op de gegevensverwerking.

|  |  |  |
| --- | --- | --- |
| **Specifieke wetgeving / beleid** | **Doeleinde** | **Gegevens** |
| Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra | BekostigingBeleidsvormingInschrijvingKwaliteitsverbeteringOnderwijsuitvoering | Leerlinggegevens |
| Wet onderwijstoezicht | ToezichtVerantwoording | Leerlinggegevens |
| Archiefwet | Bewaring en opschoning | Alle |
| Leerplichtwet | Doorgifte verzuimmeldingen | BSN, leerlingnamen en type verzuim |
| Auteurswet | Bescherming auteursrechten | Beeldmateriaal |
| Wetboek van Strafrecht | Rechtmatige verwerking | Alle |
| Wet Medezeggenschap op scholen | Instemming op de beleidsregels voor verwerking van persoonsgegevens | Medewerkersgegevens |

## Te verwerken persoonsgegevens

In onderstaand schema zijn het type gegevens beschreven die worden verwerkt inclusief de classificatie van de volgende kwaliteitsaspecten met betrekking tot de verwerking:

B = Beschikbaarheid: De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de dienstverlening waarborgen.

I = Integriteit: De mate waarin de beheersmaatregelen de juistheid, volledigheid en tijdigheid waarborgen.

V = Vertrouwelijkheid: De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type gegevens** | **Betrokkenen** | **Omvang**  | **B** | **I** | **V** |
| Algemene contactgegevens: naam, e-mail  | Ouders/verzorgers, leerlingen, medewerkers | Alle betrokkenen bij de school die in de kolom links genoemd worden | M | H | M |
| Persoonlijke kenmerken: geboortedatum en geslacht | Leerlingen | Idem als rij 1 | M | H | M |
| Overige contactgegevens: adres, postcode, woonplaats, telefoonnummer | Ouders/verzorgers, leerlingen, medewerkers | Idem als rij 1 | M | H | M |
| Contactgegevens in geval van nood | Ouders, familie, kennissen van het kind | Idem als rij 1 | M | H | M |
| Godsdienst (indien bijzonder onderwijs, op vrijwillige basis) | Ouders/verzorgers | Idem als rij 1 | M | H | M |
| Leerlingnummer | Leerlingen | Idem als rij 1 | M | H | M |
| Nationaliteit en geboorteplaats | Leerlingen en ouders | Idem als rij 1 | M | H | M |
| Gezondheidsgegevens | Leerlingen | Op eigen verzoek | M | H | H |
| Studievoortgang:* Resultaatgegevens
 | Leerlingen | Idem als rij 1 | M | M | M |
| * Advies VO (onderwijskundig rapport)
 | Leerlingen | Alleen leerlingen in groep 8  | M | H | M |
| * Onderwijsbegeleidingsgegevens
 | Leerlingen | Idem als rij 1 | M | M | M |
| * Zorgbegeleidingsgegevens
 | Leerlingen | Alleen leerlingen met zorg-arrangement | M | H | H |
| * Aanwezigheidsregistratie
 | Leerlingen | Idem als rij 1 | M | H | M |
| Verzuimregistratie | Leerlingen | Idem als rij 1 | M | H | M |
| Onderwijsorganisatie: groepsindeling, rooster, etc. | Leerlingen en medewerkers | Idem als rij 1 | M | H | M |
| Financiële (ouderbijdrage) of bekostigingsgegevens | Leerlingen, ouders/verzorgers | Idem als rij 1 | M | H | M |
| Beeldmateriaal | Leerlingen en medewerkers | Alleen indien toestemming. | M | H | H |
| BSN | Leerlingen | Idem als rij 1 | M | H | H |
| KetenID (t.b.v. technische werking) | Leerlingen | Idem als rij 1 | M | M | M |
| IP-adres (t.b.v. technische werking) | Medewerkers | Idem als rij 1 | M | H | M |
| Systeem-ID (t.b.v technische werking) | Leerlingen en Medewerkers | Idem als rij 1 | M | H | M |

## Doeleinden en grondslagen

Het type gegevens zoals hierboven beschreven, worden verwerkt voor de volgende doeleinden.

Gegevens leerlingen

|  |  |
| --- | --- |
| **Verwerkingsdoeleinden** | **Grondslag (artikel 6 AVG)** |
| 1. Gegevens ten behoeve van aanmelding en inschrijving;
 | Gerechtvaardigd belang (art. 6 lid 1 sub f) en wettelijke plicht (art. 6 lid 1 sub c) |
| 1. Verantwoorden aan DUO, Inspectie en Accountant;
2. Begeleiding in het kader van passend onderwijs (gezondheidsgegevens) en aanvragen/advisering ondersteuning (TLV/LWOO/PRO) en arrangementen;
 | Wettelijke plicht (art. 6 lid 1 sub c) |
| 1. Voorbereiden voor aanschaf en gebruik van (digitale) leermiddelen en toetsmaterialen;
2. Toestemming verwerken van de onderwijsdeelnemer (bijv. voor gebruik beeldmateriaal).
3. Communicatie van contactgegevens van de onderwijsdeelnemers met informatie van diens ouders en nood/contactpersonen.
 | Gerechtvaardigd belang (art. 6 lid 1 sub f) |
| 1. Didactische en/of pedagogisch dossier (voortgang en aanwezigheidsregistratie);
 | Wettelijke plicht (art. 6 lid 1 sub c) en toestemming bij delen met derden (art. 6 lid 1 sub a) |

Gegevens medewerkers (vast of tijdelijk)

|  |  |
| --- | --- |
| **Verwerkingsdoeleinden** | **Grondslag (artikel 6 AVG)** |
| 1. Voorbereiden voor gebruik van digitale leermiddelen en toetsmaterialen
 | Gerechtvaardigd belang (art. 6 lid 1 sub f) |
| 1. Communicatie
 | Gerechtvaardigd belang (art. 6 lid 1 sub f) |

Gegevens overige

|  |  |
| --- | --- |
| **Verwerkingsdoeleinden** | **Grondslag (artikel 6 AVG)** |
| 1. Gegevens ten behoeve van registratie, aanmelding en inschrijving;
2. Communicatie over voortgang onderwijs
 | Toestemming (art. 6 lid 1 sub a) en wettelijke plicht (art. 6 lid 1 sub c) |
| 1. Communicatie in geval van nood
 | Gerechtvaardigd belang (art. 6 lid 1 sub f) |

## Betrokken partijen

In onderstaand overzicht zijn de partijen beschreven die, betrokken zijn bij de verwerking.

|  |  |  |  |
| --- | --- | --- | --- |
| **Partij**  | **Intern of extern** | **Rol (AVG)** | **Toelichting** |
| Schoolbestuur | Intern | Verantwoordelijke | Medewerkers die het schoolbestuur vertegenwoordigen, denk aan bestuurder(s), beleidsmedewerkers, ict-medewerkers. |
| School(locatie of vestiging) | Intern | Verantwoordelijke | Medewerkers die de school vertegenwoordigen, denk aan directeur, IB-er, leerkrachten. |
| Medewerkers | Intern | Betrokkene | Medewerkers, over het algemeen betreft dit de schoolleiding, IB-er en de leerkrachten incl. de invallers voor langere duur. |
| Ouders/verzorgers | Intern | 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. |
| Leerlingen | Intern | Betrokkene | Onderwijsdeelnemers die zijn ingeschreven. Het kan ook gaan om de gegevens van oud-leerlingen in het kader van bewaarplicht of alumni-activiteiten. |
| Stagiaires | Extern | Betrokkene | Bijvoorbeeld studenten die voor langere tijd aan de school zin verbonden. |
| Topicus B.V. | Extern | Verwerker | De leverancier van ParnasSys |
| DUO | Extern | AndereVerantwoordelijke (derde) | De Dienst Uitvoering Onderwijs (Rijksoverheid) registreert beleids- en bekostigingsgegevens. ParnasSys is gekoppeld met o.a. de Basis Registratie Onderwijsdeelnemers (BRON). |
| Onderwijsinspectie | Extern | AndereVerantwoordelijke (derde) | De Onderwijsinspectie (Rijksoverheid) heeft geen directe koppeling, maar krijgt wel gegevens aangeleverd en zonodig toegang tot ParnasSys ten behoeve van onderwijs toezicht. |
| SamenwerkingsverbandPassend Onderwijs | Extern | AndereVerantwoordelijke (derde) | Samenwerkingsverbanden Passend Onderwijs ontvangen gegevens uit ParnasSys, vaak via een gezamenlijke informatievoorziening, zoals Kindkans of OnderwijsTransparant. |
| Gemeente | Extern | AndereVerantwoordelijke (derde) | Gezondheidsdiensten (GGD/JGZ) van de gemeente en leerplichtambtenaren ontvangen gegevens over de plaatsing en aan- of afwezigheid van leerlingen. |
| Hulp- of zorgverleners | Extern/intern | AndereVerantwoordelijke (derde) | Het kan hierbij gaan om bijvoorbeeld orthopedagogen, schoolmaatschappelijk werkers of logopedisten die al dan niet in dienst van de school gegevens verwerken. |
| Kennisnet | Extern | AndereVerantwoordelijke (derde) | 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. |
| Uitgeverijen enLeveranciers van digitaal leermateriaal, LVS-systemen of leerplatformen | Extern | Andere Verwerkers(derde) | Uitgeverijen ontvangen via Basispoort, een centrale voorziening voor toegang tot leermiddelen, gegevens. Daarnaast zijn er rechtstreekse koppelingen met leveranciers van leerlingvolgsystemen en leerplatformen. |

## Gegevens Verwerker(s)

Per verwerker staan hieronder de belangrijkste gegevens beschreven. De gegevens van andere verwerkers zijn niet opgenomen, omdat deze buiten de scope van de verwerking vallen.

|  |  |
| --- | --- |
| **ParnasSys - Topicus B.V.** |  |
| Hoofdvestiging | Nederland |
| Verwerking vindt plaats in | Nederland, Duitsland, Engeland Frankrijk, Ierland en Verenigde Staten (op basis van verwerkersovereenkomst versie 3.0, 30-4-2018) |
| Doorgifte buiten de EER? | Ja (zeer beperkt) |
| Verwerkersovereenkomst aanwezig? | Ja  |
| Aangesloten bij Privacy Convenant? | Ja  |
| Wordt de laatste versie van de model verwerkersovereenkomst gebruikt en op een juiste wijze toegepast? | Ja |
| ISO 27001 gecertificeerd? | Nee |
| Overige IBP certificering? | Ja, namelijk Certificeringsschema informatiebeveiliging en privacy ROSA. ISO 9001, ISO 14001 |
| Subverwerkers | Ja namelijk: Zie verwerkersovereenkomst (vanwege de vertrouwelijkheid is dit niet opgenomen in dit document).   |

# Beoordeling rechtmatigheid van de verwerking

## Bijzondere of gevoelige persoonsgegevens

|  |  |
| --- | --- |
| **Worden er identificatienummers, bijzondere of strafrechtelijke persoonsgegevens verwerkt? Zo ja, welke?** | **Ja** |
| BSN leerlingenLeerlingnummerGezondheidsgegevens |

## Verwachting en mening betrokkenen

|  |  |
| --- | --- |
| **Zijn de betrokkenen, op wie de verwerking betrekking heeft, geraadpleegd over deze DPIA en wat is hun mening over de verwerking? Zo nee, waarom niet?**  | **Ja / Nee**  |
| Het schoolbestuur kan contact opnemen met de (G)MR of leerlingenraad over de mening van de betrokkenen over hun privacy in relatie tot de verwerking van persoonsgegevens waar deze DPIA over gaat.  |

|  |  |
| --- | --- |
| **Verwachten betrokkenen dat hun gegevens worden verwerkt en bestaan er geen zorgen hierover bij betrokkenen?** | **Ja / Nee**  |
| Door het schoolbestuur te bepalen en in te vullen |

## Borging van rechten van de betrokkenen

|  |  |
| --- | --- |
| **Wordt er invulling gegeven aan de rechten van betrokkenen? Zo ja, op welke wijze?** | **Ja** |
| De rechten van betrokkenen kunnen in voldoende mate uitgevoerd worden middels ParnasSys. |

## Verwerkersovereenkomst

|  |  |
| --- | --- |
| **Zijn er een of meer verwerkersovereenkomsten afgesloten en voldoen die aan de wettelijke eisen?** | **Ja**  |
| Geen bijzonderheden. Er wordt gebruik gemaakt van de meest actuele versie van het Model Verwerkersovereenkomst van het Convenant Digitale Onderwijsmiddelen en Privacy. |

## Noodzaak en evenredigheid

|  |  |
| --- | --- |
| **Doel: Zijn alle verwerkingen noodzakelijk voor het bereiken van het doel? Kijk hierbij ook nadrukkelijk naar de gegevens in par. 3.1.** | **Ja / Nee** |
| De mogelijkheid bestaat dat er meer gegevens geregistreerd zijn dan noodzakelijk voor het doel, maar deze zijn met maatregelen afdoende te beperken. Bij medewerkers bestaat bijvoorbeeld een aantal verplichte velden (NAW-gegevens medewerker) waarvoor geen noodzaak bestaat, een maatregel als het invullen van een fake-adres of het schooladres, maakt dat de verwerking toch niet plaatsvindt.  |

|  |  |
| --- | --- |
| **Doelbinding: Worden persoonsgegevens verwerkt voor het doel waarvoor ze zijn verzameld?** | **Ja**  |
| Er zijn géén bevindingen waaruit blijkt dat dit niet het geval is. |

|  |  |
| --- | --- |
| **Dataminimalisatie: Zijn alle persoonsgegevens strikt noodzakelijk voor het bereiken van het doel?**  | **Ja** |
| Hiervan is sprake mits de school zich houdt aan het eigen beleid voor het bewaren en opschonen van gegevens, waarbij rekening wordt gehouden met de wettelijke bewaarplicht. |

|  |  |
| --- | --- |
| **Grondslag: Zijn de grondslagen (art. 6) voor de verwerking in voldoende mate aanwezig?** | **Ja** |
| Er zijn géén bevindingen waaruit blijkt dat dit niet het geval is. |

|  |  |
| --- | --- |
| **Proportionaliteit: Staat de inbreuk op de privacy van betrokkenen in verhouding tot de noodzaak tot de gegevensverwerking?** | **Ja** |
| Er zijn géén bevindingen waaruit blijkt dat dit niet het geval is. |

|  |  |
| --- | --- |
| **Subsidiariteit: Kan het verwerkingsdoel op een andere minder belastende manier worden verwezenlijkt?** | **Nee** |
| Er zijn géén manieren gevonden waaruit blijkt dat dit wel het geval is. |

# Beoordeling risico’s

##

## Berekening risicoscore

Voor de risicoscore is de volgende indeling en berekening gebruikt: Risicoscore = Kans (waarschijnlijkheid) X Impact (ernst).

Tabel H: *Risicoscore*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **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) |

## Geïnventariseerde risico’s

In onderstaande Tabel I (zie volgende pagina’s) zijn de risico’s benoemd die door het schoolbestuur zijn geïnventariseerd. De ID’s in de eerste kolom verwijzen naar een overzicht dat tijdens de workshops is gebruikt.

De risico’s zijn ingedeeld op basis van de MAPGOOD typologie, de afkorting staat voor: Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving, Diensten van derden. De risico’s zijn daarnaast gerangschikt op basis van de risicoscore (Zeer hoog naar Zeer laag).

Tabel I: *Geïnventariseerde risico’s*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Van toepassing | MAPGOOD | Omschrijving | Gevolgen | Oorzaak | Risicoscore (Kans x Impact) |
| 3 | Ja/nee | Organisatie | Er worden meer rechten toegekend aan gebruikers dan noodzakelijk. | Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie. | De hoeveelheid van rollen (en de rechten die men vanuit die rol heeft binnen het systeem) binnen ParnasSys is groot en onduidelijk. Daardoor ontoereikend. | 9 |
| 4 |  | Programma- tuur | Het is niet mogelijk de gegevensuitwisseling die middels geautomatiseerde koppelingen gedeeld wordt te wijzigen/filteren.  | Er worden meer gegevens gedeeld dan nodig en wenselijk. | Het wijzigen van de inhoud van geautomatiseerde berichtenverkeer door het schoolbestuur is niet mogelijk. De inhoud van koppelingen wordt met koppelpartners bepaald.  | 9 |
| 7 |  | Programmatuur Mensen | Het bekijken (downloaden) van bestanden in leerlingendossiers (op privé devices) zorgt voor een lokale kopie van het dossier.  | Persoonsgegevens blijven onbeheerd en zijn mogelijk toegankelijk voor anderen.  | Het moeten downloaden van bestanden om ze in te kunnen zien.Het niet verwijderen van lokale 'kopieën’. | 9 |
| 37 |  | Organisatie | Er kan geen of onvoldoende goed gebruik gemaakt worden van groepsgebaseerde toegang (groepsautorisatie of sublesgroepen) | Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie. | De hoeveelheid van rollen (en de rechten die men vanuit die rol heeft binnen het systeem) binnen ParnasSys is omvangrijk. Beperken van toegang (groepsautorisatie) is niet standaard ingesteld (privacy by default). Autorisaties kunnen niet op leerling-niveau of op onderdelen van dossiers ingesteld worden. | 9 |
| 39 |  | Programma- tuur | Gegevens van medewerkers moeten verplicht ingevoerd worden | Er worden meer gegevens vastgelegd dan noodzakelijk. | Het invoeren van o.a. adresgegevens wordt door de applicatie afgedwongen. | 9 |
| 1 |  | Organisatie | De toegekende autorisaties binnen scholen zijn niet vastgelegd in beleid. | Medewerkers hebben mogelijk meer toegang dan nodig. | Geen heldere afspraken over toegang die zijn vastgelegd en gecommuniceerd. | 6 |
| 2 |  | Organisatie | Er is geen specifiek beleid met betrekking tot het beheren van accounts.  | Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie.  | Accounts worden niet ingetrokken en/of worden toegekend aan personen die geen autorisatie zouden moeten krijgen. | 6 |
| 5 |  | Programma- tuur | Wachtwoord worden niet periodiek gewijzigd en zijn niet complex. | Wachtwoorden kunnen makkelijker geraden of gehackt worden. | Het gebruik van lange en complexe wachtwoorden wordt door de applicatie niet afgedwongen. Het gebruik van two-factor-authentication wordt door het schoolbestuur niet gebruikt. | 6 |
| 11 |  | Programmatuur Mensen | Informatie van leerlingen wordt buiten systeem om gedeeld door handmatige exports, printjes en via onbeveiligde mails of usb-sticks uitgewisseld. | Meer kans op datalekken doordat usb-sticks kwijtraken, printjes blijven liggen of mail niet veilig worden verzonden. | Informatie van leerling kan niet eenvoudig gedeeld worden vanuit de applicatie. | 6 |
| 18 |  | Mensen | Bijlagen bij OSO toevoegen (zonder inzage of toestemming) waardoor er meer wordt uitgewisseld dan toegestaan. | Niet voldoen aan wetgeving: Uitwisseling van het Onderwijskundig Rapport is verplicht, maar ouders hebben wel inzagerecht. Meer gegevens toevoegen dan opgenomen in het Besluit Uitwisseling Leer- en Begeleidingsgegevens is toestemmingsplichtig. | Onrechtmatig uitwisselen: Ouders kunnen hierover klachten indienen of rechtzaken aanspannen.  | 6 |
| 33 |  | Mensen | Wachtwoorden worden verkeerd gebruikt  | Wachtwoorden worden bekend bij derden, waardoor gegevens onbedoeld kunnen worden ingezien of gewijzigd. | Wachtwoorden worden niet (tijdig) vernieuwd, opgeslagen in de browser en/of opgeschreven of gedeeld met collega’s | 6 |
| 40 |  | Programma- tuur | De ontheffingsoptie van de groesautorisatie ‘tijdelijke toegang’ is niet bekend waardoor niet gekozen wordt om de groepsautorisatie toe te passen. | Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie. | De hoeveelheid van rollen (en de rechten die men vanuit die rol heeft binnen het systeem) binnen ParnasSys is groot en onduidelijk. Daardoor ontoereikend. | 6 |
| 43 |  | Organisatie | De logging van gebruikersactiviteiten wordt niet (periodiek) gemonitord. | Er kan niet aangetoond worden of het toegangsbeleid correct wordt uitgevoerd en of er onrechtmatig toegang is verkregen. Zie ook onderzoeksrapport AP. | Monitoring van logging ontbreekt. | 6 |
| 49 |  | Organisatie | De vastgestelde autorisaties binnen scholen worden niet gecontroleerd op het juist toepassen hiervan binnen de applicatie. | Er kan niet aangetoond worden of het toegangsbeleid correct wordt uitgevoerd en of er onrechtmatig toegang is verkregen. Zie ook onderzoeksrapport AP. | Controle op toepassen autorisaties ontbreekt. | 4 |
| 9 |  | Organisatie | Er worden meer persoonsgegevens vastgelegd dan noodzakelijk (opleiding en beroep ouders, godsdienst) | Persoonsgegevens worden onrechtmatig verwerkt. | Meer (kunnen) vastleggen in de applicatie dan noodzakelijk. | 4 |
| 10 |  | Organisatie | Onvoldoende kennis over mogelijkheden systeem | Onveilige opslag van persoonsgegevens buiten applicatie.Inzageverzoeken niet volledig. | Persoonsgegevens worden onnodig en onvoldoende beveiligd buiten de applicatie vastgelegd | 4 |
| 12 |  | Programma- tuur | Er kan wel gemaild worden, maar niet beveiligd bijv. door encryptie met wachtwoord, beperkte beschikbaarheidstermijn of het niet kunnen doorsturen of downloaden. | Mails kunnen onderschept worden. | Mailverkeer wordt onvoldoende beveiligd of beperkt in de applicatie. | 4 |
| 19 |  | Programma- tuur | Maken van handmatige exports van overzichten waarmee gegevens buiten de regie van het LAS komen en onbeveiligd gedeeld worden. | Meer kans op datalekken. | Overzichten kunnen niet eenvoudig gedeeld worden vanuit de applicatie. | 4 |
| 27 |  | Programma-tuurOrganisatie | Niet of te laat opschonen van accounts. Triggers hiervoor ontbreekt. Inactieve accounts van medewerkers onvoldoende inzichtelijk. Beheeraccounts kunnen niet verwijderd worden. | Account van (oud-)medewerkers en daarmee hun persoonsgegevens blijven zichtbaar. | Er ontbreekt beleid ten aanzien van het beheren van accounts en het opschonen van accounts is niet eenvoudig uitvoerbaar binnen de applicatie. | 4 |
| 59 |  | Organisatie | Er is geen geïmplementeerd beleid voor logische toegang (autorisaties), toegang tot systemen.  | Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie. | De hoeveelheid van rollen (en de rechten die men vanuit die rol heeft binnen het systeem) binnen ParnasSys is groot en onduidelijk. Daardoor ontoereikend. | 4 |
| 16 |  | Mensen | Verkeerde ouders/verzorgers mailen door verkeerd aanvinken. | Er worden mails met persoonsgegevens verstuurd naar de verkeerde ontvanger | Verkeerd aanvinken van geadresseerden binnen de applicatie | 3 |
| 42 |  | Programma- tuur | Bij het opschonen van persoonsgegevens, na verlopen bewaartermijn, worden gegevens verwijderd uit het leerlingdossier, maar niet uit de groepsdocumenten in de Groepsmap. | Er worden langer (gevoelige) gegevens bewaard dan is afgesproken en/of wettelijk is toegestaan. | Het opschonen van Groepsdocumenten wordt wel ondersteund, maar hiervoor zijn extra handelingen nodig.  | 2 |
| 8 |  | Organisatie | Kennis over applicatiebeheer bovenschools is belegd bij één persoon en verder niet vastgelegd.  | Kennis gaat verloren als degene ziek is of vertrekt. | Onvoldoende borging van de kennis en het ontbreken van procedures en werkprocesbeschrijvingen. | 2 |
| 14 |  | Organisatie | Bewaartermijnen voor opschonen zijn niet bekend of worden niet goed doorgevoerd conform wetgeving. | Persoonsgegevens worden niet tijdig opgeschoond. Er wordt niet voldaan aan de bewaar- en opschoonplicht. | Onbekend met bewaartermijn en/of het ontbreken van beleidsafspraken en/of het ontbreken van kennis over de wijze waarop dit uitgevoerd kan worden. | 2 |
| 21 |  | Gegevens | Meer informatie (niet-objectief) vastleggen in leerlingnotities (vrije velden) dan noodzakelijk. | Er wordt te veel informatie uitgewisseld met andere partijen (bij dossier uitwisseling). Inbreuk op rechten en vrijheden van andere betrokkenen (bij inzage verzoeken) | Er wordt te veel informatie vastgelegd. | 2 |
| 23 |  | Organisatie | Gegevens van ouders en leerlingen niet actueel (bijv. bij overdracht). | Er kunnen fouten gemaakt worden doordat persoonsgegevens niet juist zijn (adres, contactgegevens). | Persoonsgegevens worden niet periodiek gecontroleerd op juistheid. | 1 |
| 29 |  | Programma- tuurOrganisatie | Accounts voor invallers kunnen niet dezelfde dag aangemaakt worden, waardoor deze onder een ander account (van een collega) gaan werken of er is een invallersaccount, die ook na invalbeurt actief blijft. | Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie. | Ontbreken van beheer gebruikersaccounts invallers en doorlooptijd (24u.) bij aanmaken accounts | 1 |
| 26 |  | Programma- tuurOrganisatie | Stamkaarten met gevoelige gegevens kunnen downloaden. | Er ontstaan kopieën waar geen/beperkte regie op is, met vergrote kans op datalekken. | Stamkaarten kunnen gedownload worden. | 1 |
| 24 |  | Organisatie | OSO versturen zonder inzage door ouders | Ouders moeten gebruik kunnen maken van hun inzagerecht, voordat het onderwijskundig rapport wordt uitgewisseld. | De uitwisseling van het onderwijskundig rapport voldoet niet aan wet- en regelgeving. | 1 |
| 48 |  | Programmatuur | Gegevensuitwisselingen die middels geautomatiseerde koppelingen gedeeld worden, kunnen worden onderschept. | Gegevensuitwisselingen kunnen via ‘man-in-the-middle’ attacks worden onderschept. | Geautomatiseerde koppelingen zijn onvoldoende beveiligd. | 1 |
| 49 |  | ProgrammatuurMensen | Gegevens gaan verloren of worden onleesbaar gemaakt | Gegevens zijn niet meer beschikbaar, waardoor kritieke processen (onderwijs, bekostiging) niet uitgevoerd kunnen worden. | De gegevens worden onbedoeld verwijderd door menselijk handelen of worden door aanvallen van buiten onleesbaar gemaakt of vernietigd. | 1 |
| 50 |  | Programmatuur | Gegevens zijn voor onbepaalde periode niet beschikbaar. | Gegevens zijn niet meer beschikbaar, waardoor kritieke processen (onderwijs, bekostiging) niet uitgevoerd kunnen worden. | Er worden DDOS aanvallen uitgevoerd op de applicatie, waardoor deze (tijdelijk) niet beschikbaar is. | 1 |

|  |
| --- |
| **Generieke en schoolspecifieke risico’s**Bovenstaande tabel bevat generieke risico’s. Generiek wil zeggen voorkomend in de meeste schoolorganisaties. Dit moet uiteraard door het schoolbestuur gecontroleerd worden. Hieronder kunnen de schoolspecifieke risico’s worden opgenomen die de schoolorganisatie zelf moet aanvullen. In bijlage A is hiervoor een instructie opgenomen. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | MAPGOOD | Omschrijving | Gevolgen betrokkenen | Oorzaak | Risicoscore (Kans x Impact) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Beschrijving van aanbevolen maatregelen

In de volgende paragrafen worden de (voorgenomen) maatregelen geclusterd onder een bepaalde norm of statement, gebaseerd op wetgeving (AVG) of standaarden (bijv. ISO 27001). Deze statements zijn onderverdeeld naar 6 clusters, te weten:

1. Beleid en organisatie
2. Personeel, leerlingen en gasten
3. Ruimten en apparatuur
4. Continuïteit (Beschikbaarheid)
5. Vertrouwelijkheid en integriteit
6. Controle en logging.

De statements zijn waar mogelijk gerelateerd aan de ISO27002 normen of AVG-artikelen, maar kennen een eigen nummering en omschrijving ten gunste van de leesbaarheid. De statements zijn verder uitgewerkt in concrete beheersmaatregelen die gericht zijn op het mitigeren van de risico’s zoals beschreven in hoofdstuk 4. De risico’s die gerelateerd zijn aan de beheersmaatregelen, zijn eveneens bij ieder statement opgenomen.

Per statement is de urgentie bepaald op basis van de risicoscores van de gerelateerde risico’s, hoe hoger deze risicoscore hoe hoger de urgentie van de voorgestelde maatregelen. Bij elk statement is tevens een conclusie geformuleerd ten aanzien van het restrisico na de implementatie van de beheersmaatregelen. Er wordt uitgegaan van een beperkt restrisico wanneer de voorgestelde beheersmaatregelen worden toegepast. Indien de voorgestelde beheersmaatregelen niet worden toegepast en er geen andere maatregelen genomen zijn om het restrisico afdoende te mitigeren, dient bij een hoog restrisico voorafgaande raadpleging plaats te vinden bij de Autoriteit Persoonsgegevens[[3]](#footnote-4). De statements zijn geprioriteerd en per cluster gerangschikt van Hoog naar Laag.

## Beleid en organisatie

Dit cluster heeft betrekking op maatregelen die gericht zijn op de beschrijving van beleidsregels en de taken en verantwoordelijkheden die binnen de organisatie belegd moeten worden ten behoeve van de bescherming van persoonsgegevens.

|  |  |  |  |
| --- | --- | --- | --- |
| 5.1.1. | Toegang tot persoonsgegevens wordt verleend volgens het vastgestelde toegangsbeveiligingsbeleid (ISO 5.1.1). | Urgentie: | Hoog |
| Gerelateerde risico’s | 3. Er worden meer rechten toegekend aan gebruikers dan noodzakelijk. | 9 |
| 37. Er kan geen of onvoldoende goed gebruik gemaakt worden van groepsgebaseerde toegang (groepsautorisatie of sublesgroepen) | 9 |
| 1. De toegekende autorisaties binnen scholen zijn niet vastgelegd in beleid. | 6 |
| 2. Er is geen specifiek beleid met betrekking tot het beheren (intrekken, verstrekken en controleren) van accounts. | 6 |
| 5. Wachtwoorden worden niet periodiek gewijzigd en zijn niet complex. | 6 |
| 59. Er is geen geïmplementeerd beleid voor logische toegang (autorisaties) toegang tot systemen. | 4 |
| 29. Accounts voor invallers kunnen niet dezelfde dag aangemaakt worden, waardoor deze onder een ander account (van een collega) gaan werken of er is een invallersaccount, die ook na invalbeurt actief blijft. | 1 |
| Maatregelen | 1. De toegangsrechten zijn vastgesteld in op rol gebaseerde autorisatiematrices.
2. De verantwoordelijkheid voor het verstrekken, controleren en intrekken van gebruikersaccounts en bijbehorende rechten zijn belegd in de organisatie.
3. Het wachtwoordbeleid inclusief het gebruik van 2-factor-authentication is op basis van classificatie bepaald en gecommuniceerd met medewerkers.
4. Het periodiek wijzigen van wachtwoord en/of de complexiteit van het wachtwoord kan afgedwongen worden in de applicatie (indien er geen gebruik wordt gemaakt van 2-factor-authentication).
5. Groepsautorisaties kunnen bij bepaalde rollen als ‘default setting’ ingesteld worden.
6. Er kan op leerlingniveau of onderdelen van een leerlingdossier autorisaties ingesteld worden.
 |
| Eigenaar | Verwerkingsverantwoordelijke (a t/m c) Verwerker (d t/m f) |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.1.2. | Persoonsgegevens worden opgeschoond volgens het vastgestelde beleid voor bewaren en opschonen (AVG art. 5). | Urgentie: | Laag |
| Gerelateerde risico’s | 42. Bij het opschonen van persoonsgegevens, na verlopen bewaartermijn, worden gegevens verwijderd uit het leerlingdossier, maar niet uit de groepsdocumenten in de Groepsmap. | 2 |
| 14. Bewaartermijnen voor opschonen zijn niet bekend of worden niet goed doorgevoerd conform wetgeving. | 2 |
| Maatregelen | 1. Er zijn richtlijnen vastgesteld voor het bewaren en opschonen van persoonsgegevens, waarbij rekening is gehouden met wettelijke verplichtingen.
2. Er zijn procedures voor het opschonen van persoonsgegevens beschreven.
3. De verantwoordelijkheden voor het opschonen van persoonsgegevens zijn belegd in de organisatie.
4. Groepsdocumenten worden uit de groepsmap verwijderd zodra de bewaartermijn is verlopen.
 |
| Eigenaar | Verwerkingsverantwoordelijke  |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

## Personeel, leerlingen en gasten

Dit cluster heeft betrekking op maatregelen die gericht zijn op gedragsverandering bij personeel, leerlingen en gasten ten behoeve van de bescherming van persoonsgegevens.

|  |  |  |  |
| --- | --- | --- | --- |
| 5.2.1. | Medewerkers die gebruik maken van het LAS worden geschoold in het juist verwerken van persoonsgegevens (ISO 7.2.2). | Urgentie: | Hoog |
| Gerelateerde risico’s | 11. Informatie van leerlingen wordt buiten systeem om gedeeld door handmatige exports, printjes en via onbeveiligde mails of usb-sticks uitgewisseld. | 6 |
| 33. Wachtwoorden worden verkeerd gebruikt | 6 |
| 40. De ontheffingsoptie van de groesautorisatie ‘tijdelijke toegang’ is niet bekend waardoor niet gekozen wordt om de groepsautorisatie toe te passen. | 6 |
| 10. Onvoldoende kennis over mogelijkheden systeem | 4 |
| 8. Kennis over applicatiebeheer bovenschools is belegd bij één persoon en verder niet vastgelegd. | 2 |
| Maatregelen | 1. Medewerkers worden voorgelicht op het gebied van het juist formuleren en registreren van persoonsgegevens in het LAS, het beperken van het toevoegen en downloaden van bijlagen, het verwijderen van lokale kopieën en het omgaan met wachtwoorden.
2. Applicatiebeheerders worden opgeleid in het juist inrichten en beheren van het LAS met betrekking tot de verwerking van persoonsgegevens (privacy by default).
3. Er zijn voor de applicatiebeheerders werkprocessen beschreven voor het verstrekken, controleren en intrekken van accounts en het opschonen van persoonsgegevens.
 |
| Eigenaar | Verwerkingsverantwoordelijke |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.2.2. | Betrokkenen kunnen hun rechten uitoefenen met betrekking tot de verwerking van persoonsgegevens in het LAS (AVG art. 12). | Urgentie: | Laag |
| Gerelateerde risico’s | 24. OSO versturen zonder inzage door ouders | 1 |
| Maatregelen | 1. Aan ouders/verzorgers wordt inzage verleend in het onderwijskundig rapport voordat het wordt uitgewisseld met een andere school.
2. Ouders/verzorgers worden geïnformeerd over het doel en de grondslag voor de gegevensverwerking die plaatsvindt middels het LAS, het gebruik van hun privacy rechten, de bewaartermijn van de persoonsgegevens, en de wijze waarop hun gegevens worden beschermd.
 |
| Eigenaar | Verwerkingsverantwoordelijke |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

## Ruimten en apparatuur

Dit cluster heeft betrekking op maatregelen die gericht zijn op de beveiligd beheren van ruimten, netwerken, apparatuur waar(in) persoonsgegevens worden verwerkt.

|  |  |  |  |
| --- | --- | --- | --- |
| 5.3.1. | Lokale kopieën van bestanden met persoonsgegevens worden opgeschoond (AVG art. 5). | Urgentie: | Hoog |
| Gerelateerde risico’s | 7. Maken van handmatige exports, zorgt voor lokale kopieën van persoonsgegevens, waarop geen regie gevoerd kan worden | 6 |
| Maatregelen | 1. Waar mogelijk wordt de opslag van lokale kopieën beperkt of voorkomen.
2. Waar mogelijk wordt het opschonen van lokale kopieën geautomatiseerd uitgevoerd.
 |
| Eigenaar | Verwerkingsverantwoordelijke |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

## Continuïteit

Dit cluster heeft betrekking op maatregelen die gericht zijn op een onverstoorde voortgang van processen en systemen waarin persoonsgegevens worden verwerkt en het voorkomen van verlies van persoonsgegevens.

|  |  |  |  |
| --- | --- | --- | --- |
| 5.4.1. | Regelmatig behoort een back-up (kopie) van gegevens te worden gemaakt (ISO 12.3.1) | Urgentie: | Zeer laag |
| Gerelateerde risico’s | 49. De gegevens worden onbedoeld verwijderd door menselijk handelen of worden door aanvallen van buiten onleesbaar gemaakt of vernietigd.50. Er worden DDOS aanvallen uitgevoerd op de applicatie, waardoor deze (tijdelijk) niet beschikbaar is. | 1 |
| Maatregelen | 1. Er wordt periodiek (op basis van classificatie) een kopie van de gegevens in de applicatie gemaakt middels een beveiligde opslag.
2. Er is een procedure om in het geval van DDOS aanvallen de continuïteit te borgen.
 |
| Eigenaar | Verwerker (a en b)  |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

## Vertrouwelijkheid en integriteit

Dit cluster heeft betrekking op maatregelen die gericht zijn op het beveiligen van ruimten, netwerken, systemen en applicaties ten behoeve van het afschermen van persoonsgegevens en het borgen van de juistheid, actualiteit en volledigheid van persoonsgegevens.

|  |  |  |  |
| --- | --- | --- | --- |
| 5.5.1. | Er mogen niet meer persoonsgegevens worden uitgewisseld via geautomatiseerde koppelingen dan strikt noodzakelijk en alleen op basis van grondslag en doelbinding (AVG art. 5, 6, 25).  | Urgentie: | Hoog |
| Gerelateerde risico’s | 4. Het is niet mogelijk de gegevensuitwisseling die middels geautomatiseerde koppelingen gedeeld wordt te wijzigen/filteren.  | 9 |
| 18. Bijlagen bij OSO toevoegen (zonder inzage of toestemming) waardoor er meer wordt uitgewisseld dan toegestaan. | 6 |
| Maatregelen | 1. Geautomatiseerde koppelingen waarbij er meer gegevens worden uitgewisseld dan noodzakelijk worden niet gebruikt, met uitzondering van uitwisselingen die op basis van wettelijke verplichtingen moeten plaatsvinden (Privacy by design).
2. Geautomatiseerde koppelingen kunnen in het LAS door of op verzoek van het schoolbestuur ingezien en zo nodig gewijzigd worden op basis van noodzakelijkheid, grondslag en doelbinding.
 |
| Eigenaar | Verwerkingsverantwoordelijke (a) en Verwerker (b) |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.5.2. | Het maken van handmatige exports van persoonsgegevens is niet toegestaan, zonder voldoende waarborgen voor de bescherming van de persoonsgegevens (AVG art. 32).  | Urgentie: | Middel |
| Gerelateerde risico’s | 19. Maken van handmatige exports van overzichten waarmee gegevens buiten de regie van het LAS komen en onbeveiligd gedeeld worden. | 4 |
| Maatregelen | 1. Persoonsgegevens worden bij voorkeur vanuit het LAS uitgewisseld via beveiligde geautomatiseerde koppelingen in plaats van handmatige exports.
2. Er zijn gedragsregels en richtlijnen voor medewerkers voor het opslaan en uitwisselen van persoonsgegevens.
 |
| Eigenaar | Verwerker (a) en Verwerkingsverantwoordelijke (b) |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.5.3. | Het downloaden van bestanden met persoonsgegevens uit het LAS wordt beperkt (AVG art. 5, 32). | Urgentie: | Zeer laag |
| Gerelateerde risico’s | 26. Stamkaarten met gevoelige gegevens kunnen downloaden. | 1 |
| Maatregelen | 1. Bestanden met persoonsgegevens kunnen vanuit de applicatie worden ingezien. Het downloaden hiervan wordt beperkt.
 |
| Eigenaar | Verwerker  |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen gemitigeerd tot een acceptabel niveau. | **Ja** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.5.4. | Er mogen niet meer persoonsgegevens worden geregistreerd dan strikt noodzakelijk (AVG art. 5). | Urgentie: | Hoog |
| Gerelateerde risico’s | 39. Gegevens van medewerkers moeten verplicht ingevoerd worden. | 9 |
| 9. Er worden meer persoonsgegevens vastgelegd dan noodzakelijk (opleiding en beroep ouders, godsdienst). | 4 |
| 21. Meer informatie (niet-objectief) vastleggen in leerlingnotities (vrije velden) dan noodzakelijk. | 2 |
| Maatregelen | 1. Het schoolbestuur moet zelf kunnen bepalen welke velden verplicht ingevuld moeten worden, dit moet niet door het LAS worden bepaald.
2. Medewerkers moeten op de hoogte zijn welke persoonsgegevens voor welk doel vastgelegd moeten worden. Indien mogelijk kan het LAS hierin ondersteunen.
3. Er zijn gedragsregels en richtlijnen voor medewerkers voor het registeren en formuleren van leerlingnotities.
 |
| Eigenaar | Verwerker (a) en Verwerkingsverantwoordelijke (b en c) |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.5.5. | Geautomatiseerde koppelingen voor de uitwisseling van persoonsgegevens moeten voldoen aan de hiervoor geldende en actuele beveiligingsstandaarden (AVG art. 32). | Urgentie: | Zeer laag |
| Gerelateerde risico’s | 48. Gegevensuitwisselingen die middels geautomatiseerde koppelingen gedeeld worden, kunnen worden onderschept. | 1 |
| Maatregel | 1. Geautomatiseerde koppelingen waarbij er persoonsgegevens worden uitgewisseld voldoen aan de actuele versie van de Edukoppeling transactiesstandaard en het Certificeringsschema.
 |
| Eigenaar | Verwerker  |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.5.6. | Bijzondere of gevoelige persoonsgegevens worden beveiligd gemaild (AVG art. 32). | Urgentie: | Middel |
| Gerelateerde risico’s | 12. Er kan wel gemaild worden, maar niet beveiligd bijv. door encryptie met wachtwoord, beperkte beschikbaarheidstermijn of het niet kunnen doorsturen of downloaden. | 4 |
| 16. Verkeerde ouders/verzorgers mailen door verkeerd aanvinken. | 3 |
| Maatregel | 1. Persoonsgegevens kunnen vanuit het LAS worden uitgewisseld via een mailvoorziening die voldoet aan de standaarden voor beveiligd mailen (NTA7516 en/of ‘UBV Veilig en Betrouwbaar e-mailverkeer’).
2. Het verkeerd aanvinken van ontvangers wordt beperkt door gebruikers om een extra bevestiging (controle) te vragen.
 |
| Eigenaar | Verwerker  |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

## Controle en logging

Dit cluster heeft betrekking op maatregelen die gericht zijn op het vastleggen en controleren van het gebruik van ruimten, netwerken, systemen en applicaties waar(in) persoonsgegevens worden verwerkt en de naleving van de beleidsregels ten behoeve van de bescherming van persoonsgegevens.

|  |  |  |  |
| --- | --- | --- | --- |
| 5.6.1. | Er vinden periodieke controles plaats of het opschonen van persoonsgegevens gebeurd volgens het daarvoor vastgestelde beleid (ISO 18.2.2).  | Urgentie: | Middel |
| Gerelateerde risico’s | 27. Niet of te laat opschonen van accounts. Triggers hiervoor ontbreken. Inactieve accounts van medewerkers onvoldoende inzichtelijk. Beheeraccounts kunnen niet verwijderd worden. | 4 |
| Maatregel | 1. Er wordt minstens eenmaal per jaar gecontroleerd of de procedure voor het opschonen van persoonsgegevens en gebruikersaccounts op de juiste manier wordt uitgevoerd.
2. Inactieve accounts van medewerkers kunnen inzichtelijk gemaakt en opgeschoond worden.
 |
| Eigenaar | Verwerkingsverantwoordelijke (a) en Verwerker (b) |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.6.2. | Er vinden periodieke controles plaats op het juist toepassen van het toegangsbeveiligngs-beleid (ISO 9.2.5). | Urgentie: | Hoog |
| Gerelateerde risico’s | 43. De logging van gebruikersactiviteiten wordt niet (periodiek) gemonitord. | 6 |
| 49. De vastgestelde autorisaties binnen scholen worden niet gecontroleerd op het juist toepassen hiervan binnen de applicatie. | 4 |
| 23. Gegevens van ouders en leerlingen niet actueel (bijv. bij overdracht). | 1 |
| Maatregel | 1. Er wordt minstens eenmaal per jaar gecontroleerd of de vastgestelde autorisaties overeenkomen met de toegekende rollen en rechten in de applicatie. Hierover wordt gerapporteerd aan de Verantwoordelijke.
2. Er wordt minstens eenmaal per jaar aan betrokkenen gevraagd om relevante mutaties in de persoonsgegevens van leerlingen, ouders en medewerkers door te geven.
 |
| Eigenaar | Verwerkingsverantwoordelijke |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

|  |  |  |  |
| --- | --- | --- | --- |
| 5.6.3. | Er wordt periodiek een audit uitgevoerd op de beveiligingsmaatregelen die genomen zijn door de verwerker (ISO 18.2.2). | Urgentie: | Laag |
| Gerelateerde risico’s | 34. Audits op de beveiliging worden niet (periodiek) uitgevoerd. | 1 |
| Maatregel | 1. Er zijn met de verwerker afspraken gemaakt over de periodieke uitvoering van audits.
 |
| Eigenaar | Verwerkingsverantwoordelijke |
| Maatregelen geïmplementeerd? | Ja / Nee, te weten de volgende maatregelen:  |
| Conclusie restrisico | Het (hoge) risico is door de geïmplementeerde maatregelen beheerst en gemitigeerd tot een acceptabel niveau. | **Ja** |

# Conclusie, aanvaarding en goedkeuring

## Algemene conclusie

Op basis van het onderzoek dat in het kader van deze DPIA is uitgevoerd, is de conclusie dat de verwerking van persoonsgegevens een **hoog** risico inhoudt voor de rechten en vrijheden van de betrokkenen.

De door het schoolbestuur in hoofdstuk 5 besproken maatregelen garanderen in **voldoende** mate de bescherming van de persoonsgegevens van betrokkenen. De maatregelen zijn gericht op het beperken van de risico’s voor de rechten en vrijheden van betrokkenen.

Opnemen restrisico.

## Conclusie beoordeling rechtmatigheid

|  |  |
| --- | --- |
| **Is de verwerking waarvoor de DPIA is uitgevoerd rechtmatig?****Zo nee, waarom niet?** | **Ja / Nee** |
|  |

##

## Aanvaarding restrisico’s

|  |  |
| --- | --- |
| **Bevatten de restrisico’s nog hoge risico’s?Zo ja, wordt de Autoriteit Persoonsgegevens geraadpleegd?** | **Ja / Nee** |
|  |

##

## Advies Functionaris Gegevensbescherming

|  |  |
| --- | --- |
| **Is de FG betrokken bij de DPIA en/of is er advies van de FG?Zo ja, hoe luidt het advies?** | **Ja / Nee** |
|  |

##

## Raadpleging verwerker

|  |  |
| --- | --- |
| **Is of zijn de verwerker(s) geraadpleegd bij de uitvoering van de DPIA?Zo nee, waarom niet?** | **Ja** |
| De definitieve rapportage is in maart 2021 voorgelegd aan de verwerker, waarop deze een officiële reactie heeft kunnen geven.  |

##

## Raadpleging betrokkenen

|  |  |
| --- | --- |
| **Is de (G)MR of andere betrokkenen (bijvoorbeeld een leerlingenraad) geraadpleegd bij de uitvoering van de DPIA, of is de (concept) DPIA gedeeld met de (vertegenwoordiging van de) betrokkenen? Zo nee, waarom niet?** | **Ja / Nee** |
|  |

##

## Follow up

|  |  |
| --- | --- |
| **Wordt de DPIA-rapportage (of de managementsamenvatting) gepubliceerd?****Zo nee, waarom niet?** | **Ja / Nee** |
| intern |

|  |  |
| --- | --- |
| **Wanneer wordt de DPIA-rapportage herzien/heroverwogen?** ***(Advies: Herhaal de DPIA om de drie jaar of bij grote wijzigingen in processen of systemen)*** |  |
| De DPIA wordt om de drie jaar of bij grote wijzigingen in processen of systemen herhaald |

# Vaststelling en aanvaarding

De verwerkingsverantwoordelijke van <naam schoolbestuur>, overwegende de conclusie en het advies in het voorgaande hoofdstuk, verklaart hierbij:

* Kennis te hebben genomen van inhoud van de Rapportage DPIA – ParnasSys
* De - in dit rapport - vermelde restrisico’s te aanvaarden
* In te stemmen met de uitvoering van de in de rapportage voorgestelde beheersmaatregelen
* De DPIA na een periode van 3 jaar te laten herzien of eerder indien nodig
* Wel / geen voorafgaande raadpleging bij de Autoriteit Persoonsgegevens in te dienen
* Het DPIA-team decharge te verlenen

Naam:

Datum:

Handtekening:

# Verklaring begrippen en afkortingen

**AVG**

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wet bescherming persoonsgegevens (Wbp) geldt niet meer. De AVG is ook wel bekend onder de Engelse naam: General Data Protection Regulation (GDPR).

**Betrokkene**

De natuurlijke persoon op wie de gegevens betrekking hebben, wordt de betrokkene genoemd.

**BIV-classificatie**

Een BIV-classificatie of BIV-indeling is een indeling waarbij de kwaliteitsaspecten beschikbaarheid (B), integriteit (I) en vertrouwelijkheid (V) van gegevens en systemen wordt aangegeven.

Beschikbaarheid: De mate waarin beheersmaatregelen de beschikbaarheid en ongestoorde voortgang van de dienstverlening waarborgen.

Integriteit: De mate waarin de beheersmaatregelen de juistheid, volledigheid en tijdigheid waarborgen.

Vertrouwelijkheid: De mate waarin uitsluitend geautoriseerde personen, programmatuur of apparatuur gebruik kunnen maken van de gegevens of programmatuur, al dan niet gereguleerd door (geautomatiseerde) procedures en/of technische maatregelen.

**DPIA**

Een beoordeling van de effecten van een voorgenomen verwerkingsactiviteit op de bescherming van persoonsgegevens en de rechten en vrijheden van betrokkenen. Een DPIA of gegevensbeschermingseffectbeoordeling is een instrument om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis hiervan worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of te verkleinen. Ook toont u met een gegevensbeschermingseffectbeoordeling aan dat u aan de vereisten van de Verordening hebt voldaan voor die verwerkingsactiviteit.

**EER**

De Europese Economische Ruimte (EER) is het resultaat van een in 1992 gesloten akkoord tussen de landen van de Europese Gemeenschap (EG) (later de Europese Unie, EU) en de Europese Vrijhandelsassociatie (EVA). Het EER-akkoord trad in werking op 1 januari 1994. Bij de Europese Economische Ruimte (EER) horen alle EU-landen plus Liechtenstein, Noorwegen en IJsland.

**FG**

De Verordening kent een belangrijke rol toe aan de functionaris voor gegevensbescherming (in het Engels

data protection officer, afgekort DPO). De functionaris voor gegevensbescherming (FG) houdt intern toezicht op

en adviseert over de toepassing en naleving van de Verordening door uw organisatie. Ook is de FG het

aanspreekpunt voor de betrokkene. In een aantal gevallen is het aanstellen van een FG verplicht.

**GDPR**

Zie AVG.

**Gegevensbeschermingseffectbeoordeling**

Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor

de rechten en vrijheden van natuurlijke personen, dan dient u voorafgaand aan de verwerking een

zogenaamde gegevensbeschermingseffectbeoordeling uit te voeren. In de praktijk wordt deze beoordeling ook wel Privacy Impact Assessment (PIA) of Data Protection Impact Assessment (DPIA) genoemd. Zie DPIA.

**UAVG**

Hoewel het doel van de Verordening een geharmoniseerd gegevensbeschermingsrecht is, biedt de

Verordening de lidstaten toch op een heel aantal punten ruimte om specifieke bepalingen op te nemen of

uitzonderingen te maken. Het gaat dan bijvoorbeeld om de regels omtrent de verwerking van bijzondere

categorieën van persoonsgegevens en de invulling van de rechten van de betrokkenen. In Nederland zijn

deze specifieke bepalingen vastgelegd in de Uitvoeringswet Algemene verordening gegevensbescherming (de

‘Uitvoeringswet’ of ‘UAVG’) en ook in sectorale wetten die bepalingen bevatten over de verwerking van

persoonsgegevens op het terrein dat zij bestrijken.

**Verwerkingsverantwoordelijke**

De verwerkingsverantwoordelijke is degene die ‘doel en middelen’ bepaalt voor de verwerking. Met

andere woorden, de verwerkingsverantwoordelijke bepaalt hoe en waarom er persoonsgegevens worden

verwerkt. De verwerkingsverantwoordelijke is de (rechts)persoon die letterlijk de verantwoordelijkheid

heeft voor het naleven van de Verordening.

**Verwerker**

De verwerker handelt in opdracht van de verwerkingsverantwoordelijke bij het verwerken van persoonsgegevens, zonder onder diens rechtstreeks gezag te staan. Op de verwerker rust de plicht om de instructies van de verwerkingsverantwoordelijke op te volgen.

# Bijlage A – Instructie controle en aanvulling DPIA-rapport

Binnen de onderwijssectoren po en vo worden een aantal leerlingadministratiesystemen (LAS’en) breed gebruikt. Daarom is gekozen voor een generieke aanpak voor de uitvoeren van een DPIA per LAS. Op deze manier worden schoolbesturen als Verwerkingsverantwoordelijken geholpen bij de uitvoering. Dit neemt niet weg dat er ook specifieke risico’s kunnen zijn die voor individuele scholen gelden. Daarnaast zijn de huidige risico’s met een beperkt aantal schoolbesturen geïnventariseerd. Het huidige rapport is dus niet uitputtend en moet daarom door het schoolbestuur worden gecontroleerd en aangevuld. Hiervoor zijn de volgende stappen per onderdeel in het rapport omschreven die doorlopen moeten worden.

Processtappen vooraf:

* Afweging om DPIA te doen (argumentatie)
* Planning workshop (dagdeel)
* Deelnemers DPIA uitnodigen:
	+ PO
	+ FG (adviseur / DPIA-uitvoerder)
	+ Stakeholders proces (verantwoordelijke/eigenaar, beheerders, gebruikers)
* Inlezen generieke rapportage (FG/PO)
* Eventueel: Vooraf delen risico’s ter beoordeling

Processtappen achteraf:

* Raadplegen betrokkenen (GMR)
* Afronden organisatiespecifieke rapportage
* Besluitvorming / vaststelling rapportage
* Plan van aanpak (evt.) voorgestelde maatregelen

Processtappen DPIA-workshop LAS:

Voorblad

* Voeg de naam van het schoolbestuur toe
* Voeg de maand en jaartal toe

Colofon

* Wijzig de versiedatum en voeg de co-auteur(s) toe

1. Inleiding

* Verwijder paragraaf 1.3 Aanpak DPIA
* Geef toelichting op DPIA aan de deelnemers

2. Beschrijving van de gegevensverwerking

* Vul de juiste periode in en wijzig zo nodig de afbakening in paragraaf 2.2.
* Controleer de BIV classificatie en rode teksten in paragraaf 2.5 en pas deze zo nodig aan.
* Controleer de teksten in paragraaf 2.8 en pas deze zo nodig aan.

3. Beoordeling rechtmatigheid van de verwerking

* Controleer de paragrafen in hoofdstuk 3 en in het bijzonder de rode teksten in paragraaf 3.1, 3.2 en 3.4. Pas deze zo nodig aan.
* Ga na of er niet meer gegevens worden verwerkt dan noodzakelijk en vul dit aan in paragraaf 3.5.

4. Geïnventariseerde risico’s

* Controleer de risicoscore in paragraaf 4.2 en pas deze zo nodig aan. Zorg er dan ook voor dat de risico’s in volgorde van Hoog naar Laag worden gepresenteerd. Let op: De risicoscore is ook van invloed op de urgentie van de te nemen maatregelen in hoofdstuk 5.
* Verwijder het kader met toelichting over specifieke risico’s en vul de tabel daaronder zo nodig aan.

5. Beschrijving van aanbevolen maatregelen

* Pas de urgentie aan, indien de risicoscore in paragraaf 4.2 is gewijzigd. Zorg er dan ook voor dat de maatregelen per cluster in volgorde van Hoog naar Laag worden gepresenteerd.
* Geef per statement in paragraaf 5.1 t/m 5.6 aan of de beheersmaatregelen zijn geïmplementeerd. Zo ja, laat de conclusie ten aanzien van de restrisico’s ongewijzigd. Zo nee, pas de conclusie ten aanzien van de restrisico’s aan en geef aan of dit gemitigeerd is tot een acceptabel niveau.

6. Conclusie, aanvaarding en goedkeuring

* Controleer de conclusie (rode tekst) in paragraaf 6.1 en pas deze aan naar onvoldoende, indien de restrisico’s in hoofdstuk 5 niet zijn gemitigeerd tot een acceptabel niveau. Let op! Je zult bij een onvoldoende ook een melding hiervan moeten doen bij de Autoriteit Persoonsgegevens. Kijk dus goed of je nog andere maatregelen kunt nemen.
* Beantwoord de vragen in paragraaf 6.2 t/m 6.8 en voeg een verklaring toe als hierom wordt gevraagd op basis van het gegeven antwoord. Paragraaf 6.7 vul je pas in op het moment dat het rapport door de bestuurder is vastgesteld.

Managementsamenvatting

* Werk de rode teksten in de managementsamenvatting bij als je in hoofdstuk 4 en 5 wijzigingen hebt aangebracht. In de managementsamenvatting worden alleen de risico’s getoond met een score Hoog (6-9), de maatregelen met urgentie Hoog en de beheersmaatregelen die met de Verwerker afgestemd dienen te worden.

Inhoudsopgave

* Pas de paginanummering van de inhoudsopgave indien nodig aan (Klik op de inhoudsopgave met je rechtermuisknop en kies voor Veld bijwerken).

Vaststellen en ondertekening

* Laat de bestuurder de DPIA vaststellen, d.w.z. de restrisico’s aanvaarden en de voorgestelde beheersmaatregelen goedkeuren (zie hoofdstuk 7).

# Bijlage B – GegevensverwerkingsanalyseGegevensverwerkingsanalyse Parnassys

**Uitleg**

Een DPIA of gegevensbeschermingseffectbeoordeling begint met de **gegevensverwerkingsanalyse**. Dat is een systematische beschrijving welke processen worden onderzocht, welke systemen daarbij betrokken zijn, welke gegevens worden verwerkt en hoe deze gegevens zijn geclassificeerd. Daarbij wordt ook ingegaan op zaken zoals het doel en de grondslag van de verwerking en de eventuele betrokkenheid van andere partijen, zoals leveranciers. Het gaat hier om een feitelijke rapportage en analyse. Vervolgens wordt op basis van richtlijnen van de toezichthouder bepaald of er een risicoanalyse (DPIA) moet worden uitgevoerd. Mocht een DPIA niet nodig zijn, dan is dat hiermee een weloverwogen en gemotiveerd besluit.

**Invulinstructie**

De vragenlijst gegevensverwerkingsanalyse wordt beantwoord door de onderwijsinstelling. Bij voorkeur wordt het ingevuld door medewerkers die inhoudelijk betrokken zijn bij of kennis hebben van de applicatie die onderzocht wordt (denk bijvoorbeeld aan de functioneel applicatiebeheerder). Alle vragen in deze gegevensverwerkingsanalyse worden **vanuit het perspectief van de eigen onderwijsinstelling** beantwoord. Dus geef antwoord over de eigen software, organisatie, uitwisseling van gegevens, etc.

De gegevensverwerkingsanalyse geeft in 8 stappen een goed beeld van het gegevensverwerkende proces (de software of proces). De doorgaans lastige vragen bij een DPIA zijn opgesplitst in kortere eenvoudige vragen. Hiervoor zijn er weliswaar meer vragen, maar zijn deze vragen gemakkelijker in te vullen door medewerkers die geen of beperkte kennis hebben van privacy.

**Opbouw vragenlijst (onderdelen)**

De gegevensverwerkingsanalyse bestaat, naast algemene informatie, uit de volgende 8 stappen, gevolgd door de beoordeling of een DPIA noodzakelijk is:

1. Beschrijving van het gegevensverwerkende proces

2. Verwerkte persoonsgegevens

3. Verwerkingsdoeleinden

4. Betrokken partijen

5. Bewaartermijnen

6. Beoordeling van de rechtmatigheid

7. Globale beoordeling van de risico’s

8. Beveiligingsmaatregelen

9. Beoordeling noodzaak DPIA

**0. Algemene informatie**

In dit onderdeel vul je de algemene informatie in zoals de naam van de organisatie, de naam van het (deel)proces en de naam van de invuller.

1. Naam van de organisatie

2. Naam van de invuller

3. Datum

4. Naam van het (deel)proces

5. Omschrijving van het (deel)proces

6. Versie-aanduiding van het geraadpleegde verwerkings-/dataregister

**1. Beschrijving van het gegevensverwerkende proces**

In dit onderdeel beschrijf je in algemene bewoordingen het proces, de gebruikte systemen, de koppelingen en de gegevensstromen van en binnen de onderwijsinstelling. Het gaat er hier vooral om een beeld te schetsen van de scope van de gegevensverwerkingsanalyse en de eventueel hierop volgende DPIA. Maak hiervoor gebruik van een referentiearchitectuur (FORA[[4]](#footnote-5) of Route 21[[5]](#footnote-6)):

7. Procesbeschrijving

*Een korte beschrijving van het gegevensverwerkende proces waarop de analyse en DPIA ziet. Het gaat hierbij om een beschrijving op hoofdlijnen waar het proces over gaat: om welke bedrijfsfunctie gaat het. In de FORA gaat het om een proces binnen het bedrijfsfunctiemodel: een processen binnen de school.*

* Digitaal leerlingadministratiesysteem waarin alle gegevens van de leerlingen worden ingevoerd die van belang zijn om een goede administratie te kunnen voeren.
* Digitaal leerlingvolgsyteem waarin scholen informatie invoeren die belangrijk is voor de school zodat zij kunnen deze kunnen analyseren en concrete plannen kunnen opstellen. Alle gegevens van de leerlingen worden op individueel niveau vastgelegd (inclusief het [ontwikkelingsperspectief](https://www.parnassys.nl/producten/parnassys/ontwikkelingsperspectief)) en op groepsniveau 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 ParnasSys.

8. Applicatielandschap

*Een korte beschrijving van het applicatielandschap van de onderwijsinstelling. Dat is een overzicht van alle applicaties en systemen binnen de (eigen) onderwijsinstelling. Voeg via een link eventuele schema’s toe.*



<https://www.wikixl.nl/wiki/fora/index.php/Modellen_voor_DPIA#Applicatielandschap>

1. Koppelingen

*Een korte beschrijving van de van toepassing zijnde (externe) koppelingen van het onderzochte systeem of proces. Waar is het mee gekoppeld? Of staat het systeem los? Voeg via een link eventuele schema’s toe. Benoem de koppelvlakken / sleutelvelden waarop wordt gekoppeld. Bij onderdeel 4 (Betrokken partijen, vanaf vraag 27) geef je aan met welke partijen er koppelingen bestaan, dat hoeft niet hier. Bij deze vraag 9. worden de koppelingen vanuit technisch en functioneel perspectief beschreven.*

* BRON
* OSO
* Verzuimregister
* Zie ook gegevensstromen onder genoemd 10)
1. Beschrijving gegevensstromen

*Een korte beschrijving van de gegevensstromen, op hoofdlijnen, volgens de systematiek input – verwerking - output. Als er gegevensstroom diagrammen zijn, voeg die dan via een link toe.*



<https://www.wikixl.nl/wiki/fora/index.php/Modellen_voor_DPIA#Gegevensstromen>

**2. Verwerkte persoonsgegevens**

In dit onderdeel onderzoek je welke categorieën persoonsgegevens worden verwerkt binnen de onderwijsinstelling en controleer je of dit in overeenstemming is met het huidige verwerkingsregister/dataregister.

1. Worden er persoonsgegevens van onderwijsdeelnemers en/of medewerkers verwerkt?

X Ja

* + Nee

1. Categorieën persoonsgegevens onderwijsdeelnemers

*Welke categorieën van persoonsgegevens van onderwijsdeelnemers worden verwerkt binnen het proces. Vink aan wat van toepassing is.*

X Contactgegevens: naam, e-mail en org.eenheid

X Contactgegevens: geboortedatum en geslacht

X Studentennummer/leerlingnummer

X Nationaliteit en geboorteplaats

X Medische gegevens (op eigen verzoek)

X Studievoortgang (exam.,traject voortg., begeleiding, medisch dos., klas leerj. opleid.)

X Onderwijsorganisatie (roosters, boekenlijsten, etc.)

Financiën (volledige cyclus)

X Beeldmateriaal (b.v. pasfoto, camera beelden enz.)

X Docenten, mentoren en mbo adviseur

X BSN

1. Worden er persoonsgegevens van medewerkers verwerkt?

X Ja

* + Nee

1. Categorieën persoonsgegevens medewerker

*Welke categorieën van persoonsgegevens van medewerkers worden verwerkt binnen het proces. Vink aan wat van toepassing is.*

X Contactgegevens: naam, e-mail en org.eenheid

? Contactgegevens volledig

* + Personeelsnummer
	+ Nationaliteit en geboorteplaats
	+ Medische gegevens (op eigen verzoek)
	+ Ervaringen (werkervaringen en opleidingen)
	+ R&O gesprekken (Resultaat en ontwikkeling)
	+ Financiën (volledige cyclus)
	+ Beeldmateriaal (b.v. pasfoto, camera beelden enz.)
	+ BSN

1. Worden er persoonsgegevens anders dan van studenten of medewerkers verwerkt?

X Ja

* + Nee

1. Categorieën persoonsgegevens van overige betrokkenen

*Welke categorieën van persoonsgegevens van overige betrokkenen worden verwerkt binnen het proces?*

* Contactgegevens ouders, financiën i.v.m. vrijwillige ouderbijdrage
* Gegevens noodnummers (bijv. opa. oma, oppas)

1. Zijn de opgegeven categorieën persoonsgegevens in overeenstemming met het dataregister?

*Zijn de categorieën van persoonsgegevens opgenomen en verwerkt binnen in het dataregister of register van verwerkingen?*

* + Ja

X Nee

1. Licht je antwoord hier toe

Het betreffende register verwerkingen richt zich op de verwerking van gegevens van de leerlingen.

1. Is de vertrouwelijkheid van een of meer categorieën persoonsgegevens ingeschaald als ‘hoog’? *De categorieën persoonsgegevens worden geclassificeerd volgens de BIV-classificatie, zie hiervoor het dataregister. De beschikbaarheid, integriteit en vertrouwelijkheid kunnen laag, midden of hoog zijn.*

X Ja

* + Nee

1. Eventuele aanvullende opmerkingen over dit onderdeel 'Verwerkte persoonsgegevens'

**3. Verwerkingsdoeleinden**

In dit onderdeel specificeer je de verwerkingsdoeleinden met betrekking tot onderwijsdeelnemers, medewerkers en/of overige betrokkenen. Deze vragen hangen samen met onderdeel 6 (beoordeling rechtmatigheid, vanaf vraag 41).

1. Verwerkingsdoeleinden (onderwijsdeelnemers)

*Als je had opgegeven dat er persoonsgegevens van onderwijsdeelnemers worden verwerkt, geeft dan hieronder de verwerkingsdoeleinden aan.*

X Gegevens ten behoeve van registratie, aanmelding en inschrijving (informatiedagen, informatieverzoeken over opleidingen, open dagen, etc)

X Komen tot een Onderwijsovereenkomst (OOK)

Komen tot een Praktijkovereenkomst (POK)

X Verantwoorden aan DUO, Inspectie en Accountant (bijlage OOK)

X Voorbereiden voor aanschaf en gebruik van (digitale) leermiddelen en toetsmaterialen

X Didactische en/of pedagogisch dossier (voortgang, examineren en aanwezigheid registratie)

X Begeleiding in het kader van passend onderwijs (gezondheidsgegevens) en aanvragen/advisering ondersteuning (TLV/LWOO/PRO) en arrangementen

X Toestemming verwerken van de onderwijsdeelnemer (bijv. voor gebruik beeldmateriaal)

Anders: nvt

1. Verwerkingsdoeleinden (medewerkers)

*Als je had opgegeven dat er persoonsgegevens van medewerkers worden verwerkt, geeft dan hieronder de verwerkingsdoeleinden aan.*

* + Komen tot een arbeidsovereenkomst
	+ Voldoen aan de wettelijke verplichtingen (Belasting, pensioen, etc.)
	+ Overeenkomsten met externe verwerkers (ADP, QMP, Office365, etc.)

X Voorbereiden voor aanschaf en gebruik van (digitale) leermiddelen en toetsmaterialen

* + Regelingen op het gebied van secundaire arbeidsvoorwaarden
	+ Begeleiding medewerkers (Arbodienst, bedrijfsarts, re-integratie, coaching, etc)
	+ Toestemming voor gebruik beeldmateriaal
	+ Anders:

1. Verwerkingsdoeleinden (overig)

*Als je had opgegeven dat er persoonsgegevens van overige betrokkenen worden verwerkt, geeft dan hieronder de verwerkingsdoeleinden aan.*

Communicatie van contactgegevens van de onderwijsdeelnemers met informatie van diens ouders en nood/contactpersonen.

1. Zijn de opgegeven verwerkingsdoeleinden in overeenstemming met het verwerkingsregister/dataregister?

X Ja, voor wat betreft de verwerking van leerlinggegevens

* + Nee, of onbekend

1. Licht je antwoord hier toe

Zie antwoord bij vraag 18.

1. Eventuele aanvullende opmerkingen over dit onderdeel 'Verwerkingsdoeleinden'

 Zie antwoord bij vraag 18.

**4. Betrokken partijen**

In dit gedeelte geef je aan welke partijen allemaal betrokken zijn bij de gegevensverwerking. Het gaat daarbij om (mede)verwerkingsverantwoordelijken, verwerkers, derden (verstrekkers en ontvangers van persoonsgegevens). Bij het antwoord op vraag 9. is bijvoorbeeld beschreven of er koppelingen zijn met het onderzochte systeem of proces, bij deze vraag worden de partijen benoemd inclusief hun rol in het gegevensverwerkende proces.

1. Is er naast de eigen organisatie nog een andere partij betrokken in de rol van verwerkingsverantwoordelijke?

X Ja

* + Nee

1. Welke verwerkingsverantwoordelijke(n) betreft het?

*Met korte toelichting m.b.t. de samenwerking en rolverdeling. Het gaat bijvoorbeeld om een samenwerkingsverband, andere onderwijsinstelling of OCW of DUO*

***BRON (DUO)***

Het Basisregister Onderwijs (BRON) is een verzameling van leerlinggegevens aangeleverd door onderwijsinstellingen in Nederland. Alle scholen in Nederland in het primair onderwijs (po) en alle scholen en instellingen in het voortgezet onderwijs (vo), het hoger onderwijs (hbo en wo) en het beroepsonderwijs en volwasseneneducatie (bve), zijn aangesloten op BRON. Scholen en instellingen wisselen leerlinggegevens uit met BRON. De gegevens van scholen en instellingen staan geregistreerd in de Basisregistratie Instellingen (BRIN). Bij een inschrijving op een school worden de volgende persoonsgegevens geregistreerd en uitgewisseld met BRON:

* persoonsgebonden nummer (Burgerservicenummer of onderwijsnummer);
* geboortedatum;
* geslacht;
* officiële achternaam;
* voorvoegsel(s) (indien van toepassing);
* officiële voornaam/voornamen (in de juiste volgorde);
* actueel adres (straatnaam, huisnummer, huisnummer toevoeging, postcode, plaatsnaam)

Dit is het 12-cijferige NHR vestigingsnummer dat aangeeft waar de leerling (het grootste gedeelte van) zijn of haar opleiding volgt. Het doel van BRON is het verlichten van de administratieve lasten voor scholen. Scholen hoeven hun gegevens aan steeds minder partijen te leveren, omdat DUO deze gegevens via BRON verstrekt.

De gegevens uit BRON worden onder andere gebruikt voor het volgende:

* DUO gebruikt geanonimiseerde gegevens uit BRON voor het berekenen en toekennen van de bekostiging aan scholen. De overheid krijgt hierdoor meer controle op de rechtmatigheid van de bekostiging.
* Het recht op mogelijke tegemoetkoming studiekosten en/of studiefinanciering wordt geverifieerd met de leerlinggegevens uit BRON.
* De gegevens uit BRON leveren beleidsinformatie op voor het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).
* De gegevens uit BRON leveren waardevolle managementinformatie op voor het ministerie van OCW, voor scholen en vo

DUO hanteert de volgende bewaartermijnen:

* Meldingen in het verzuimregister worden 2 jaar bewaard.
* Gegevens van overleden personen worden 2 jaar bewaard.
* Gegevens over studenten in het hoger onderwijs worden 25 jaar bewaard.
* Gegevens over leerlingen in het primair onderwijs, voortgezet onderwijs en middelbaar beroepsonderwijs worden bewaard tot 5 jaar na de laatste inschrijving van de onderwijsloopbaan.
* Examenresultaten in het diplomaregister worden 60 jaar bewaard, tenzij de betrokkene eerder overlijdt.

De gegevens worden vernietigd in het jaar na het aflopen van de bewaartermijn.

Vestigingsplaats: Nederland

***Verzuimregister***

Scholen in het primair onderwijs melden verzuim via hun leerlingenadministratiesysteem (LAS).

De verzuimmelding komt in het verzuimregister bij DUO. DUO zorgt dat de melding terechtkomt bij de gemeente waar de leerling woont. Vervolgens haalt een leerplichtambtenaar de melding op uit het verzuimregister. Het doel is om de leerling zo snel mogelijk weer naar school te laten gaan. In het LAS, Mijn DUO of administratiepakket is te zien wat de leerplichtambtenaar doet met de melding.

Veilige verbinding

Voor een veilige verbinding tussen de LAS en het verzuimregister maakt DUO gebruik van Software as a Service (SaaS).

Vestigingsplaats: Dienst Uitvoering Onderwijs (DUO) Zakelijk, Groningen

Bewaartermijn gegevens:

Meldingen in het verzuimregister worden 2 jaar bewaard.

De gegevens worden vernietigd in het jaar na het aflopen van de bewaartermijn.

INVOEGEN: UITWISSELING MET SAMENWERKINGSVERBANDEN (benoem systemen zoals Kindkans, 1Loket, etc, wie geeft toestemming voor evt. koppeling met ParnasSys?

1. Welke verwerkers zijn betrokken bij de gegevensverwerking?

*Het gaat hierbij om verwerkers volgens art 28/29 van de AVG, en om partijen die mogelijk op een andere manier betrokken zijn bij het proces en zo bijvoorbeeld inzage in persoonsgegevens zouden kunnen krijgen. Geef voor elke externe partij de vestigingsplaats, aard van de werkzaamheden aan en -indien bekend- of deze die werkzaamheden in de rol van verwerker of als andere dienstverlener uitvoert.*

Leverancier van ParnasSys is Topicus, Singel 9, 7411 HV Deventer

1. Worden er gegevens verwerkt buiten de E.E.R.?

*Wanneer gegevens buiten de Europese Economische Ruimte (lees EU) worden verwerkt dan zijn aanvullende waarborgen vereist.*

X Ja

* + Nee
1. Welke gegevens worden -door welke verwerkers- buiten de E.E.R. verwerkt?

*Het gaat bijvoorbeeld om persoonsgegevens die worden aangeleverd door de aanleverende school, DUO,. etc*

Nederland, Duitsland, Engeland Frankrijk, Ierland en Verenigde Staten (op basis van verwerkersovereenkomst versie 3.0, 30-4-2018)

1. Worden er ook uitsluitend categorieën persoonsgegevens **van** of **via** externe partijen ontvangen? Dus niet van de medewerkers of onderwijsdeelnemer zelf.

*Het gaat bijvoorbeeld om persoonsgegevens die worden aangeleverd door de aanleverende school, DUO etc.*

X Ja

* + Nee
1. Van welke externe partijen worden persoonsgegevens ontvangen en met welk doel?

DUO, met als doel controle en aanvullen ontbrekende gegevens

OSO overstap leerlingen oude school naar nieuwe school (PO-PO; PO-VO; PO-(s)bo)

1. Worden er persoonsgegevens **aan** externe partijen verstrekt?

*Het gaat daarbij om partijen die niet genoemd zijn als verwerker (zie boven) maar partijen die een zelfstandige taak en verantwoordelijkheid hebben. Denk daarbij aan DUO (studenten) en het UWV (medewerkers).*

X Ja

* + Nee
1. Aan welke partijen worden persoonsgegevens verstrekt?

Zie ook antwoord bij 33:

DUO zakelijk (BRON en Verzuimregister)

OSO

Externe ondersteuners zoals psycholoog, orthopedagoog etc, hulpverlening leerling

Uitgeverijen en leveranciers van digitaal leermateriaal, LVS-systemen of leerplatformen

Kennisnet (single sign on-voorziening)

Basispoort (single sign on-voorziening)

Gemeente – leerplicht

Onderwijsinspectie

Samenwerkingsverbanden passend onderwijs

Andere onderwijsinstellingen

36.Eventuele aanvullende opmerkingen over dit onderdeel 'Betrokken partijen'

Nvt

**5. Bewaartermijnen**

In dit gedeelte wordt ingegaan op het beleid ten aanzien van bewaartermijnen en op welke manier die bewaartermijnen worden bewaakt.

1. Worden de bewaartermijnen gehanteerd volgens het door de instelling vastgestelde beleid?

*Deze bewaartermijnen zijn opgenomen in het verwerkingenregister/dataregister. Let ook op ‘schaduwsystemen’ zoals Excel-exportbestanden etc.*

x Ja, daar waar het gaat over leerlingen

x Nee, daar waar het gaat over medewerkers

* + Niet van toepassing
	+ Onzeker/onbekend

1. Toelichting met betrekking tot de bewaartermijnen

*Licht hier toe waarom de bewaartermijnen niet in lijn zijn met het vastgestelde beleid of leg uit waarom je hierover onzeker bent.*

[toelichting over eigen beleid bewaartermijnen]

1. Op welke manier worden de bewaartermijnen bewaakt?

*Wordt dit door het proces/systeem ondersteund (privacy by design) bijvoorbeeld.*

Dit kan vanuit ParnasSys ingesteld worden. Dit is nog niet automatisch ingeregeld voor alle scholen en bovenschoolse modules.

LET OP: gegevens medewerkers worden niet verwijderd uit ParnasSys! Dit is kan nu alleen handmatig gewist worden door de school zelf.

1. Eventuele aanvullende opmerkingen over dit onderdeel 'Bewaartermijnen'

[toelichting over eigen beleid bewaartermijnen]

* Verwijderen dossier (muv NAW/in/uitstroom/verzuim) van alle leerlingen 5 jaar na uitschrijving.
	+ Let op handreiking bewaartermijnen voor verwijderen aparte categorieën na 2 of 3 jaar!
* NAW/in/uitstroom/ voorlopig helemaal niet verwijderen
* Verzuim 5 jaar n.a.v. richtlijn Inspectie

**6. Beoordeling van de rechtmatigheid**

In dit gedeelte geef je een globale inschatting van de grondslag, doel- en doelbinding en in hoeverre de gegevensverwerking noodzakelijk en transparant is. Hierbij is relevant om de antwoorden 21 t/m 26 (onderdeel 3. verwerkingsdoeleinden) bij het antwoord te betrekken.

1. Grondslag(en) voor de verwerking

*Geef aan op welke grondslag(en) de gegevensverwerkingen zijn gebaseerd. Meerdere opties mogelijk. Indien onbekend, vul dan niets in.*

X Wettelijke verplichting

* Taak van algemeen/publiek belang

X Uitvoering van een overeenkomst

X Gerechtvaardigd belang

X Toestemming van de betrokkene

* + Vitaal belang van de betrokkene

1. Toelichting met betrekking tot de grondslag(en) *Geef een toelichting op de grondslag.*

1. Doelbinding

*Als persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel dan of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.*

X De gegevens worden uitsluitend gebruikt voor het doel waarvoor ze oorspronkelijk waren verzameld

* + De gegevens worden ook gebruikt voor andere toepassingen dan het oorspronkelijke doel

1. Toelichting doelbinding: voor welke andere/nieuwe/afgeleide doelen worden de persoonsgegevens gebruikt?

*Geef aan voor welke nieuwe/afgeleide toepassingen worden de persoonsgegevens worden gebruikt en in hoeverre deze nieuwe vorm van gebruik verenigbaar is met het oorspronkelijke doel.*

Nvt

1. Noodzaak van de verwerking: is de gegevensverwerking noodzakelijk voor het realiseren van de verwerkingsdoeleinden (er zijn geen alternatieven denkbaar voor deze verwerking)?

x Ja

o Nee

1. Toelichting

Het gebruik van een leerlingadministratiesysteem is verplicht, het is vanuit het oogpunt van zorgvuldigheid belangrijk dat op de zelfde wijze met gegevens van leerlingen wordt omgegaan. Toegang tot gegevens wordt zo centraal geregeld op een veilige en verantwoorde wijze.

1. Evenredigheid van de verwerking

*Staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden en worden er niet te veel gegevens gevraagd of gebruikt?*

x Ja

o Nee

o Onzeker/Onbekend

1. Toelichting evenredigheid

De inbreuk van op de privacy staat in verhouding tot de gegevensverwerking. Het is verplicht gegevens op te slaan van en over leerlingen en hun studievoortgang. Op deze wijze kunnen gegevens centraal worden opgeslagen en gebruikt, toegang wordt centraal beheerd, beveiliging is georganiseerd. Het gebruik van dit LAS levert een bijdrage aan veilig en verantwoord gebruik van gegevens van de leerlingen in plaats van een handmatige verwerking of verwerking/systeem per school. Tegenover een kleine inbreuk op de privacy staan veel voordelen rondom beschikbaarheid, integriteit en vertrouwelijkheid.

1. Rechten van de betrokkenen

*Kunnen de betrokkenen via de onderwijsinstelling hun rechten uitoefenen bij deze verwerking, zoals het recht op inzage, correctie, verwijdering of geïnformeerd worden over de verwerking van hun persoonsgegevens?*

X Ja

* Nee
1. Eventuele aanvullende opmerkingen over dit onderdeel 'Rechtmatigheid'

De gegevensverwerking wordt als rechtmatig gezien.

**7. Globale risicobeoordeling**

In de (toelichting op de) AVG zijn een aantal scenario’s benoemd die worden aangeduid als risicovol. Vrij vertaald naar de onderwijspraktijk levert dat de onderstaande situaties. Geef aan of het betreffende scenario op de onderzochte gegevensverwerking van toepassing is.

1. Grootschalige verwerking

*Is er, gelet op het aantal betrokkenen en/of de hoeveelheid gegevens, sprake van een grootschalige verwerking. Als de verwerking is gericht op alle onderwijsdeelnemers en/of medewerkers is er al snel sprake van een grootschalige verwerking.*

X Ja

* + Nee
	+ Onzeker

1. Toelichting: grootschalige verwerking

Er is sprake van een grootschalige verwerking omdat deze is gericht op alle onderwijsdeelnemers en medewerkers.

53.Bijzondere persoonsgegevens

*Worden er binnen het proces bijzondere en/of gevoelige persoonsgegevens verwerkt. Bijvoorbeeld over de gezondheid (zoals een beperking als dyslexie), godsdienst, vakbondslidmaatschap, of de financiële situatie van de betrokkene?*

X Ja

* + Nee
	+ Onzeker/onbekend
1. Toelichting: bijzondere persoonsgegevens

Binnen ParnasSys worden bijzondere en/of gevoelige persoonsgegevens verwerkt, namelijk godsdienst; BSN nummer leerlingen; studievoortgang; extra begeleiding; OPP; medische gegevens leerlingen (vrijwillig, met toestemming van ouders); beeldmateriaal (vrijwillig, met toestemming van ouders) en bakrekeningnummer van de ouders m.b.t. innen van vrijwillige ouderbijdrage.

1. Toestemming van betrokkenen

*Is er sprake van toestemming van de betrokkene als rechtsgrond voor de verwerking (zie ook bij 'Grondslagen van de verwerking')*

X Ja

* + Nee

1. Toelichting: toestemming van betrokkenen

Bij de nr 54 genoemde bijzondere/gevoelige persoonsgegevens wordt toestemming gevraagd aan ouders voor het opnemen van medische gegevens van de leerlingen, en voor het maken/verwerken van beeldmateriaal. Voor de verwerking van de overige genoemde persoonsgegevens wordt geen toestemming gevraagd omdat deze verwerkt worden vanuit een wettelijke verplichting en (onderwijs)overeenkomst met als doel het organiseren of geven van onderwijs.

1. Evalueren en beoordelen

*Is er sprake van geautomatiseerd evalueren en beoordelen van betrokkenen, waaronder profileren. Denk daarbij aan vormen van learning analytics of andere vormen van geautomatiseerd meten en/of beoordelen van prestaties. Hieronder vallen ook gevallen waarbij door ict-toepassingen/software beslissingen worden genomen die van invloed zijn op de rechten en verplichtingen van onderwijsdeelnemers en/of medewerkers.*

* + Ja

X Nee

* + Onzeker/Onbekend
1. Toelichting: evalueren en beoordelen
2. Systematische observatie

*Is er sprake van observatie van betrokkenen, door bijvoorbeeld camera’s of door het monitoren van software/netwerkgebruik.*

* + Ja

X Nee

* + Onzeker/Onbekend

1. Toelichting: systematische observatie

Niet van toepassing.

1. Koppelen van gegevensbestanden: worden gegevens in- en extern gekoppeld?

*Worden er persoonsgegevens uit verschillende (interne en externe) bestanden aan elkaar gekoppeld waardoor nieuwe vormen/inzichten van data-analyse mogelijk worden?*

* + Ja

X Nee

* + Onzeker/Onbekend

1. Toelichting: koppelen van gegevensbestanden

Niet van toepassing

1. Nieuwe technologieën

*Worden de persoonsgegevens verwerkt met gebruikmaking van een nieuwe, tot nu toe nog onbewezen technologie?*

* + Ja

X Nee

* + Onzeker/Onbekend

1. Toelichting: nieuwe technologieën

 Niet van toepassing.

1. Is er sprake van een van de volgende grootschalige verwerkingen van persoonsgegevens rondom: de financiële situatie, biometrische persoonsgegevens (vingerafdruk, gezichtsscan), gezondheidsgegevens, samenwerkingsverbanden (samenwerkingen tussen onderwijsinstelling en gemeente/overheden/jeugdzorg), (flexibel) cameratoezicht, stelselmatige controle van werknemers, profilering of geautomatiseerde besluitvorming?

*Het betreft hier de opsomming van verwerkingen van persoonsgegevens waarvoor volgens de Autoriteit Persoonsgegevens altijd een DPIA noodzakelijk is.*

* + Ja

X Nee

* + Onzeker/Onbekend
1. Aanvullende risico’s

*Komen er uit deze inventarisatie aanvullend nog risico’s waarmee rekening gehouden moet worden.*

* Toegekende autorisaties binnen scholen: wordt op alle scholen het zelfde autorisatiebeleid eenduidig vastgesteld en toegepast?
* Hoe gaat het toekennen en afmelden van accounts en applicatiebeheerders: is dit centraal belegd of is daar specifiek beleid voor? Risico dat accounts niet worden afgemeld of worden toegekend aan personen die geen autorisatie zouden moeten krijgen.
* De hoeveelheid van rollen (en de rechten die men vanuit die rol heeft binnen het systeem) binnen ParnasSys is groot en onduidelijk. Daardoor onoverzichtelijk.
* Het is niet mogelijk als school om te sturen op de gegevensverwerking die binnen de koppelingen die mogelijk zijn binnen ParnasSys met externe partijen.
* Het is niet mogelijk om invloed uit te oefenen op het wachtwoordbeleid van ParnasSys; wordt per gebruiker ingesteld. Kan niet bovenschools geregeld worden. Wel via Single Sign On.
* Is voor beheerders 2Fa verplicht ingesteld?

**8. Beveiligingsmaatregelen**

In dit onderdeel wordt ingegaan op de beveiligingsmaatregelen op hoofdlijnen.

1. Op welke manier krijgen gebruikers toegang tot het gebruikte systeem en op welke wijze is de toegang beveiligd?

*Is de toegang tot het systeem gedefinieerd en opgenomen in een autorisatiematrix, op welke manier wordt identity- en access management toegepast?*

[autorisatie – of toegangsbeleid eigen schoolbestuur beschrijven, hoe is toegang tot ParnasSys geregeld voor nieuwe medewerkers, vertrekkende medewerkers]

1. Op welke wijze worden de gegevens opgeslagen en beveiligd?

*Draait de applicatie bijvoorbeeld ‘on premisse’ of is er sprake van een clouddienst bij de leverancier?*

Gegevens worden opgeslagen bij ParnasSys. ParnasSys is en saas-oplossing.

1. Als er gegevens worden uitgewisseld via gegevenskoppelingen, beschrijf dan op welke manier de gegevens tijdens de overdracht zijn beveiligd.

*Denk daarbij aan beveiligde webservices en/of toepassing van end-to-end encryptie.*

Er wordt gewerkt met beveiligde verbindingen. Gebruikers loggen met een versleutelde verbinding (256-bits SSL – te zien aan het slot-symbool in de browser).

1. Heeft of hebben de leverancier(s) certificeringen en worden (audit)rapportages aangeleverd?

*Voor informatiebeveiliging wordt vaak een ISO 27001 certificering gebruikt.*

Ja, ISO 27001, ISO 9001, ISO 14001.

1. Zijn er bij de onderwijsinstelling procedures beschikbaar om (security)incidenten pro- en reactief te melden bij of door de verantwoordelijke leverancier (en vice versa)?

[benoem en beschrijf eigen procedure datalekken]

1. Zijn er duidelijke afspraken over de back-up en restore van de data en de beschikking hierover?

[benoem en beschrijf de procedure voor back-up]

Voor het terugzetten van gegevens kan contact worden opgenomen met ParnasSys.

1. Worden acties van gebruikers binnen de onderzochte applicatie of programmatuur opgeslagen (logging)?

De activiteiten van medewerkers wordt gelogd maar er vindt geen actieve controle of monitoring op de logging plaats.

**9. Beoordeling noodzaak DPIA**

De invuller van de gegevensverwerkingsanalyse heeft de mogelijkheid om als afsluiting een advies, oordeel, opmerking, of toelichting te geven of er een DPIA moet worden uitgevoerd.

1. Moet er, naar jouw mening, op basis van bovenstaande informatie een DPIA worden uitgevoerd?

X Ja

o Nee

o Onzeker/Onbekend

1. Toelichting noodzaak DPIA

*Geef hieronder aan waarom er wel/geen DPIA wordt uitgevoerd*

Gezien de grote hoeveelheid persoonsgegevens van leerlingen onder de 16 jaar, waaronder bijzondere/gevoelige persoonsgegevens, die wordt verwerkt binnen ParnasSys, de bestaande koppeling met externe partijen en het feit dat de autorisaties binnen de scholen niet eenduidig worden toegekend binnen de scholen, is het noodzakelijk om een DPIA te doen op dit LAS/LVS systeem om zo risico’s aan het licht te brengen en hierop acties in te zetten om eventueel geconstateerde risico’s waar mogelijk weg te nemen of zo klein mogelijk te maken.

1. Als er een DPIA wordt uitgevoerd, zijn er dan specifieke risico’s die meegenomen moeten worden?

*Geef hieronder puntsgewijs aan wat de belangrijkste of specifieke risico’s zijn die bij een DPIA niet vergeten mogen worden*

Aandacht voor autorisaties, aandacht voor logging, aandacht voor beveiligingsmaatregelen.

**Hartelijk dank voor het invullen van deze gegevensverwerkingsanalyse. Verstuur deze ter accordering naar de FG. Mocht er een DPIA worden uitgevoerd, dan worden de gegevens van deze analyse daarin overgenomen en zo nodig gewijzigd/aangevuld. Wat er vervolgens wordt toegevoegd is een uitgebreide risicoanalyse en de bijbehorende maatregelen om de gevonden hoge risico’s te mitigeren.**

**Beoordeling**

*Op basis van de bovenstaande gegevens kan door de proceseigenaar en/of de FG worden beoordeeld of er een DPIA moet worden uitgevoerd.*

1. Moet er op basis van bovenstaande informatie een DPIA worden uitgevoerd?

X Ja

* + Nee
1. Toelichting noodzaak DPIA

Zie gegeven antwoord vraag 75

1. Akkoord/gezien FG

*De FG tekent voor gezien.*

1. <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667> [↑](#footnote-ref-2)
2. <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-europese-privacytoezichthouders-6668> [↑](#footnote-ref-3)
3. <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging> [↑](#footnote-ref-4)
4. <https://wwikixl.nl/wiki/fora/index.php/DPIA> [↑](#footnote-ref-5)
5. <https://www.sambo-ict.nl/route21/> [↑](#footnote-ref-6)