DPIA Magister

Leerlingadministratiesysteem (LAS)

[naam schoolbestuur]

[maand] [jaar]

Inhoud

Toelichting
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 per onderdeel in het rapport, in kaders zoals deze, invulinstructies opgenomen die doorlopen moeten worden om het rapport aan te passen naar de eigen schoolorganisatie.

Invulinstructie
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

Colofon

Versie 1.0 (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)

Met dank aan De vertegenwoordigers van de volgende schoolbesturen die een bijdrage hebben geleverd: Christiaan Huygens College, CVO Zuid-West Fryslân, Ons Middelbaar Onderwijs (OMO)

Auteur Privacy op School in opdracht van Kennisnet en SIVON

Managementsamenvatting

Invulinstructie
Werk de rode teksten in de managementsamenvatting pas bij nadat je in hoofdstuk 4 en 5 de wijzigingen hebt aangebracht. In de managementsamenvatting worden alleen de risico's getoond met een score Zeer hoog (score 9), de maatregelen met urgentie Zeer hoog en de beheersmaatregelen die door de Verwerker uitgevoerd dienen te worden.

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 privacy risico'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 Magister is uitgevoerd, is de conclusie dat de verwerking van persoonsgegevens een **hoog** risico inhoudt voor de rechten en vrijheden van de betrokkenen.

Inzicht in risico's
In deze rapportage leest u de risico's die zijn geïnventariseerd rondom de gegevensverwerking in Magister. De belangrijkste risico's, aangemerkt als Zeer hoog (score 9), betreffen de volgende:

- Er is geen specifiek beleid met betrekking tot toegangsbeveiliging. Toegangsbeveiliging omvat de toegang tot het ICT systeem en de toegang via autorisatie tot een applicatie dat draait binnen het ICT systeem. (ID2)
- Persoonsgegevens worden niet (tijdig) gewist (ID17).
- Juistheid van kritieke gegevens, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties, kan niet gegarandeerd worden (ID55).
- Koppelen van gegevensbestanden ten behoeve van managementrapportages leidt ertoe dat privacygevoelige gegevens herleidbaar zijn tot personen (ID37).
- De logging van gebruikersactiviteiten wordt niet (periodiek) gemonitord (ID56).
- Het bekijken (downloaden) van bestanden in leerlingendossiers (op privé devices) zorgt voor een lokale kopie van het dossier (ID8)
- De stringente voorwaarden waaronder bijzondere persoonsgegevens door een geselecteerde groep medewerkers kunnen worden verwerkt, worden niet of onvoldoende toegepast (ID59).
- Maken van handmatige exports van overzichten waarmee gegevens buiten de regie van het LAS komen en onbeveiligd gedeeld worden (ID21).
- Er kan wel gemaild worden, maar niet beveiligd bijv. door encryptie met wachtwoord, beperkte beschikbaarheidstermijn of het niet kunnen doorsturen of downloaden (ID14).
- Logboeknotities zijn toegankelijk voor te veel medewerkers (ID71).

Statements ten behoeve van passende beheersmaatregelen
Op basis van bovenstaande risico's zijn de volgende statements met de prioritering Zeer hoog ingebracht. De verschillende beheersmaatregelen behorende bij deze statements zijn uitgewerkt in hoofdstuk 5 evenals de overige beperkende maatregelen die nodig zijn om tot een acceptabel restrisico te komen. De statements zijn:.

- Toegang tot persoonsgegevens wordt verleend volgens het vastgestelde toegangsbeveiligingsbeleid (ISO 9.4.2.).
- Persoonsgegevens worden gewist volgens het vastgestelde beleid voor bewaren en wissen (AVG art. 5).
- Betrokkenen kunnen hun rechten uitoefenen met betrekking tot de verwerking van persoonsgegevens in het LAS (AVG art. 12).
- Er mogen niet meer persoonsgegevens worden uitgewisseld dan strikt noodzakelijk en alleen op basis van grondslag en doelbinding (AVG art. 5, 6, 25).
- Het maken van handmatige exports van persoonsgegevens is alleen toegestaan wanneer er afdoende waarborgen aanwezig zijn voor de bescherming van de persoonsgegevens (AVG art. 32).

- Het downloaden van bestanden met persoonsgegevens uit het LAS wordt beperkt (AVG art. 5, 32).
- Bijzondere of gevoelige persoonsgegevens worden beveiligd gemaild (AVG art. 32).
- De bescherming van de juistheid en de vertrouwelijkheid van persoonsgegevens wordt gewaarborgd. (AVG art. 5, 32).
- Bijzondere of gevoelige persoonsgegevens worden beveiligd gemaild (AVG art. 32).
- *Er vinden periodieke controles plaats op het juist toepassen van het toegangsbeveiligingsbeleid (ISO 9.2.5 en AVG art. 32).*

Uit te voeren beheersmaatregelen Verantwoordelijke en Verwerker
Het rapport biedt per statement concrete beheersmaatregelen die door het schoolbestuur, als Verantwoordelijke, binnen een redelijk maar afzienbaar termijn geïmplementeerd moeten zijn om de restrisico te mitigeren tot een acceptabel niveau. Deze maatregelen staan beschreven in hoofdstuk 5. In dat kader wordt tevens aanbevolen om de volgende beheersmaatregelen op te nemen en uit te laten voeren door de Verwerker (Iddink Group):

- Het periodiek wijzigen van wachtwoord en/of de complexiteit van het wachtwoord wordt afgedwongen in de applicatie (indien er geen gebruik wordt gemaakt van 2-factor-authentication).
- Groepsautorisaties worden bij bepaalde rollen als ‘default setting’ ingesteld.
- Er worden op leerlingniveau of onderdelen van een leerlingdossier autorisaties ingesteld.
- Er wordt periodiek (op basis van classificatie) een kopie (back-up) van de gegevens in de applicatie gemaakt middels een beveiligde opslag.
- 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.
- Persoonsgegevens worden bij voorkeur vanuit het LAS uitgewisseld via beveiligde geautomatiseerde koppelingen in plaats van handmatige exports.
- Het downloaden van bestanden wordt tegengegaan doordat bestanden met persoonsgegevens binnen de applicatie kunnen worden ingezien door medewerkers die daarvoor geautoriseerd zijn en er geen lokale kopieën nodig zijn..
- 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’).
- Het schoolbestuur moet zelf kunnen bepalen welke velden verplicht ingevuld moeten worden, dit moet niet door het LAS worden bepaald.
- Geautomatiseerde koppelingen waarbij er persoonsgegevens worden uitgewisseld voldoen aan de actuele versie van de Edukoppeling transactiestandaard en het Certificeringsschema ROSA.

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

De schoolbestuurder wordt als verwerkingsverantwoordelijke verzocht om de implementatie van voorgestelde maatregelen goed te keuren (zie hoofdstuk 7).

1. Inleiding

1.1. 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. 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.

1.2. Waarom een DPIA?

Een DPIA is bedoeld om inzicht te krijgen in de privacy risico'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:

a) Een systematische en uitgebreide beoordeling van personen op basis van geautomatiseerde verwerking die gebruikt wordt voor besluitvorming, ook wel 'profiling' genoemd.
b) De verwerking van bijzondere persoonsgegevens (gezondheidsgegevens, ras, religie, etc.) of strafrechtelijke feiten of veroordelingen.
c) 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], tot één van deze verwerkingen behoort het LAS. Ook zijn er Europese richtlijnen opgesteld[2] en wordt er van een organisatie verwacht dat men zelf een risico-afweging maakt.

Vóór de uitvoering van een DPIA op het leerlingadministratiesysteem Magister, is in een voortraject een pré-DPIA uitgevoerd op basis waarvan is vastgesteld dat een DPIA vereist is.

1.3. 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 niet uitputtend en moet door het schoolbestuur worden gecontroleerd en aangevuld. Om deze reden is het rapport voorzien van rode teksten en een invulinstructie per hoofdstuk om het DPIA-rapport af te ronden. Het schoolbestuur is, als Verwerkingsverantwoordelijke, zelf verantwoordelijk voor de inhoud van het DPIA-rapport.

1.4. Leeswijzer

De rapportage is als volgt opgebouwd:

- In hoofdstuk 2 is de gegevensverwerking beschreven die plaatsvindt in Magister.
- 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 de conclusie opgenomen en in hoofdstuk 7 is een verklaring van de Verwerkingsverantwoordelijke (lees: schoolbestuur), waarmee de bestuurder verklaart kennis te hebben

[1] [1] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667
[2] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-europese-privacytoezichthouders-6668

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 8 een lijst opgenomen met een verklaring van gebruikte begrippen en afkortingen.

2. Beschrijving van de gegevensverwerking

Invulinstructie

- Lees het hoofdstuk en pas de tekst aan indien gewenst, beoordeel hierbij in ieder geval de rode teksten en pas deze aan naar de situatie van de eigen organisatie.
- 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 rode teksten in paragraaf 2.8 en pas deze zo nodig aan.

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

2.1. Algemeen

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

Magister Suite betreft in de basis een digitaal onderwijsplatform bestaande uit administratieve verwerking van leerlinggegevens, cijfers en aan- en afwezigheid. Daarnaast wordt het onderwijsproces ondersteund met functionaliteiten als dagroosteren, lesdashboard, digitaal leren, ELO, managementrapportages en een leerlingvolgsysteem. Alle gegevens van de leerlingen worden op individueel niveau vastgelegd. Er kunnen digitale rapporten worden opgesteld waarmee de school inzicht krijgt in resultaten. Scholen kunnen eigen voorkeuren instellen voor het gebruik van Magister. Iddink Group werkt samen met andere leveranciers van onderwijssystemen en koppelt het Magister Platform onder andere aan Wintoets, Qlickview en digitaal lesmateriaal.

2.2. 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 maart 2021

Afbakening

Voor de DPIA is met vertegenwoordigers van schoolbesturen gekeken naar de verwerking zoals die plaatsvindt in Magister Suite. Hierbij is met name gekeken naar de basisfuncties van Magister zijnde de leerlingadministratie en het gebruik van Magister apps voor smartphone en tablets. Er is niet **specifiek** gekeken naar koppelingen met Microsoft365, Ephorus, MMP, Magnaview of met andere (externe) systemen, zoals BRON, Entree, OSO, etc.

2.3. Technieken en methoden

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

Magister betreft een zogenaamd Software-as-a-Service (SaaS) voor scholen in het primair en speciaal onderwijs. Magister bestaat als een webbased versie Magister Web, de Magister App en de Magister Desktop (RDP) versie. De applicatie bevat diverse gegevenskoppelingen (zowel webservices) met andere aanleverende en afnemende systemen. Tevens is het mogelijk om handmatige exports te maken. Met Magister hebben gebruikers toegang tot hun gegevens via het iOS-platform (iPhone, iPad) en het Android-platform.

2.4. Juridisch / beleidsmatig kader

Hieronder is beschreven welke wet- en regelgeving, naast de AVG, 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	Bekostiging Beleidsvorming Inschrijving Kwaliteitsverbetering Onderwijsuitvoering	Leerlinggegevens
Wet onderwijstoezicht	Toezicht Verantwoording	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

2.5. 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
• 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
• Centraal examen en rekentoets	Leerlingen	Idem als rij 1	M	H	H
Verzuimregistratie	Medewerkers	Idem als rij 1	M	H	M
In- en uitdienst	Medewerkers	Idem als rij 1	M	H	M
Onderwijsorganisatie: groepsindeling, rooster, etc.	Leerlingen en medewerkers	Idem als rij 1	M	H	M
Financiële of bekostigingsgegevens	Leerlingen, ouders/verzorgers	Idem als rij 1	M	H	M

Beeldmateriaal	Leerlingen en medewerkers	Idem als rij 1	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)	Leerlingen en 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

2.6. 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)
2) Verantwoorden aan DUO, Inspectie en Accountant; 3) 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)
4) Gebruik van (digitale) leermiddelen en toetsmaterialen; 5) Gebruik beeldmateriaal ter bevordering van de veiligheid op school 6) Communicatie van contactgegevens van de onderwijsdeelnemers met informatie van diens ouders en nood/contactpersonen ten behoeve van uitvoering van het curriculum.	Gerechtvaardigd belang (art. 6 lid 1 sub f)
7) Didactische en/of pedagogisch dossier bijhouden (voortgang, examineren 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) Gebruik van digitale leermiddelen en toetsmaterialen	Gerechtvaardigd belang (art. 6 lid 1 sub f)
2) Communicatie	Gerechtvaardigd belang (art. 6 lid 1 sub f)

Gegevens ouders/verzorgers

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)
3) Communicatie in geval van nood	Gerechtvaardigd belang (art. 6 lid 1 sub f)

2.7. Betrokken partijen

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

Partij	Intern of extern	Rol (AVG)	Toelichting
Schoolbestuur (Raad van Bestuur)	Intern	Verwerkings-verantwoordelijke	Medewerkers die het schoolbestuur vertegenwoordigen, denk aan de bestuurder(s).
Toezichthouders	Intern	Valt onder Verwerkings-verantwoordelijke	Denk aan Raad van toezicht, FG en accountant
School(locatie of vestiging)	Intern	Valt onder Verwerkings-verantwoordelijke	Medewerkers die de school vertegenwoordigen, denk aan directeur/rector, afdelings- en teamleiders, zorgcoördinator, docenten, etc.

Medewerkers	Intern	Betrokkene	Medewerker onderwijspersoneel en onderwijsondersteunend personeel.
Ouders/verzorgers	Intern	Betrokkene	Ouders/verzorgers van de ingeschreven leerlingen. Het kan soms ook gaan om een voogd.
Leerlingen (incl. aspirant- en oud-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. Leerlingen die 16 jaar of ouder kunnen zelf gebruik maken van hun privacyrechten.
Stagiaires	Extern	Betrokkene	Docent- of Leraar-in-opleiding (DIO/LIO)
Stagebedrijven	Extern	Andere Verwerkings-verantwoordelijke (derde)	Dit betreffen bedrijven waar leerlingen stage lopen.
Iddink Group	Extern	Verwerker	De leverancier van Magister.
DUO	Extern	Andere Verantwoordelijke (derde)	De Dienst Uitvoering Onderwijs (Rijksoverheid) registreert beleids- en bekostigingsgegevens. Magister is gekoppeld met o.a. de Basis Registratie Onderwijsdeelnemers (BRON).
Onderwijsinspectie	Extern	Andere Verantwoordelijke (derde)	De Onderwijsinspectie (Rijksoverheid) heeft geen directe koppeling, maar krijgt wel gegevens aangeleverd en zonodig toegang tot Magister ten behoeve van onderwijs toezicht.
Samenwerkingsverband Passend Onderwijs	Extern	Andere Verantwoordelijke (derde)	Samenwerkingsverbanden Passend Onderwijs ontvangen gegevens uit Magister, vaak via een gezamenlijke informatievoorziening.
Gemeente	Extern	Andere Verantwoordelijke (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	Andere Verantwoordelijke (derde)	Het kan hierbij gaan om bijvoorbeeld orthopedagogen, schoolmaatschappelijk werkers, etc. die al dan niet in dienst van de school gegevens verwerken.
Huiswerkbegeleiding-bureaus of -instituten	Extern	Andere Verantwoordelijke (derde)	Externe bureaus voor huiswerkbegeleiding die in opdracht van de school of ouders leerlingen extra studiebegeleiding bieden.
Kennisnet	Extern	Andere Verantwoordelijke (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.
Vervolgopleidingen	Extern	Andere Verantwoordelijke (derde)	Met name met MBO's worden gegevens uitgewisseld over leerlingen uit het VMBO, vaak via een centrale (regionale) informatievoorziening.
Uitgeverijen en Leveranciers van digitaal leermateriaal, ELO's of leerplatformen	Extern	Andere Verwerkers (derde)	Er zijn rechtstreekse koppelingen met leveranciers van ELO's, leerplatformen en uitgevers voor het gebruik van digitale leermiddelen.

2.8. Gegevens Verwerker(s)

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

Magister – Iddink Group	
Hoofdvestiging	Nederland
Verwerking vindt plaats in	Nederland (op basis van verwerkersovereenkomst versie 3.0, 30-4-2018 – versie 1.0)
Doorgifte buiten de EER?	Nee
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?	Ja (datacenters) en Cobit 4.1, de code voor informatiebeveiliging op basis van ISO27002:2007
Overige IBP-certificering?	Ja, namelijk: ▪ De report controls van SOC2 (AICPA), ▪ Certificeringsschema informatiebeveiliging en privacy ROSA
Subverwerkers	Ja, namelijk: Zie verwerkersovereenkomst (vanwege de vertrouwelijkheid is dit niet opgenomen in dit document).

3. Beoordeling rechtmatigheid van de verwerking

Invulinstructie

- Lees het hoofdstuk en pas de tekst aan indien gewenst, beoordeel hierbij in ieder geval de rode teksten en pas deze aan naar de situatie van de eigen organisatie.
- Controleer de rode teksten in paragraaf 3.2 en 3.4 en pas deze zo nodig aan.
- Ga na of er niet meer gegevens worden verwerkt dan noodzakelijk en vul dit aan in paragraaf 3.5.

3.1. Gevoelige en bijzondere persoonsgegevens

Worden er identificatienummers, bijzondere of strafrechtelijke persoonsgegevens verwerkt? Zo ja, welke?	**Ja**
BSN leerlingen Leerlingnummer Gezondheidsgegevens Godsdienst	

3.2. 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	

3.3. Borging van rechten van de betrokkenen

Wordt er invulling gegeven aan de rechten van betrokkenen? Zo ja, op welke wijze?	**Ja / Nee**
Magister maakt het mogelijk voor de school om afdoende tegemoet te kunnen komen aan de rechten die betrokkenen kunnen uitoefenen. Iddink heeft aangegeven dat er een functie om het dossier (als pdf) te downloaden bestaat binnen Magister.	

3.4. Verwerkersovereenkomst

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

3.5. Noodzaak en evenredigheid

Doel: Zijn alle verwerkingen noodzakelijk voor het bereiken van het doel?	**Ja / Nee**
Er zijn géén bevindingen waaruit blijkt dat dit niet het geval is (*beoordeel hierbij o.a. de toepassing van de voorgestelde maatregelen bij Statements 5.2.1 risico 19 en 5.5.2 risico 21*).	

Doelbinding: Worden persoonsgegevens verwerkt voor het doel waarvoor ze zijn verzameld?	**Ja / Nee**
Er zijn géén bevindingen waaruit blijkt dat dit niet het geval is (*beoordeel hierbij o.a. de toepassing van de voorgestelde maatregelen bij Statements 5.1.2, 5.5.2 en 5.5.6*).	

Dataminimalisatie: Zijn alle persoonsgegevens strikt noodzakelijk voor het bereiken van het doel?	**Ja / Nee**
Hiervan is sprake mits de school zich houdt aan het eigen beleid voor het bewaren en wissen van gegevens, waarbij rekening wordt gehouden met de wettelijke bewaarplicht (*beoordeel hierbij o.a. de toepassing van de voorgestelde maatregelen bij Statements 5.1.1. en 5.1.2*).	

Grondslag: Zijn de grondslagen (art. 6) voor de verwerking in voldoende mate aanwezig?	Ja / Nee
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 van de gegevensverwerking?	Ja / Nee
Er zijn géén bevindingen waaruit blijkt dat dit niet het geval is (*beoordeel hierbij o.a. de toepassing van de voorgestelde maatregelen bij Statements 5.1.1. en 5.1.2*).	

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.	

4. Beoordeling risico’s

Invulinstructie

- 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. Desgewenst kan hierbij gebruik gemaakt worden van het Excelbestand ‘Inventarisatieformulier Risico's LAS - DPIA Magister v1.0’.
- Verwijder het kader met toelichting over specifieke risico’s en vul de tabel daaronder zo nodig aan.
- De ID’s zijn afkomstig uit een inventarisatieformulier met risico’s die in het voortraject gebruikt zijn, pas deze desgewenst aan.

4.1. Risicoscore

Voor de risicoscore is de volgende indeling en berekening gebruikt:

Risicoscore = Kans (waarschijnlijkheid) X Impact (ernst).

	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)

4.2. Geïnventariseerde risico’s

In onderstaande tabel (volgende pagina’s) zijn de risico’s benoemd die door de school zijn geïnventariseerd. De risico’s zijn gerangschikt op basis van de risicoscore (Zeer hoog naar Zeer laag).

Risicoscore (Kans x Impact)	Omschrijving	Gevolgen	Oorzaak	ID
9	Er is geen specifiek beleid met betrekking tot toegangsbeveiliging. Toegangsbeveiliging omvat de toegang tot het ICT systeem en de toegang via autorisatie tot een applicatie dat draait binnen het ICT systeem.	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.	2
9	Persoonsgegevens worden niet (tijdig) gewist.	Gegevens worden langer bewaard dan noodzakelijk of wettelijk is bepaald.	Het wissen van gegevens is complex. Bewaartermijnen voor wissen zijn niet bekend bij de betreffende medewerkers op school of worden niet goed doorgevoerd conform wetgeving	17
9	Juistheid van kritieke gegevens, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties, kan niet gegarandeerd worden.	De data-integriteit, oftewel de juistheid van de gegevens, daar waar die geregistreerd worden in de applicatie, is niet op orde, waardoor de AVG niet wordt nageleefd. Indien informatie niet correct is, kan dit de organisatie en betrokkenen ernstige schade toebrengen.	Informatie wordt niet juist geregistreerd. Er vindt geen extra controle plaats op persoonsgegevens die met hoog geclassificeerd zijn op het gebied van data-integriteit (BSN, formatieve resultaatgegevens, etc.)	55
9	Koppelen van gegevensbestanden ten behoeve van managementrapportages leidt ertoe dat privacygevoelige gegevens herleidbaar zijn tot personen.	Er worden meer persoonsgegevens, gedeeld dan een medewerker o.b.v. 'need to know' nodig heeft.	Via de functionaliteit Magister Management Platform (MMP) wordt via data-analyse toegang verleend tot gegevens.	37
9	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.	Monitoring van logging ontbreekt.	56
9	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'.	8
9	De stringente voorwaarden waaronder bijzondere persoonsgegevens door een geselecteerde groep	De organisatie, instelling of betrokkene kan ernstige schade lijden indien	Autorisatiebeleid wordt niet of onvoldoende toegepast.	59

Risicoscore (Kans x Impact)	Omschrijving	Gevolgen	Oorzaak	ID
	medewerkers kunnen worden verwerkt, worden niet of onvoldoende toegepast.	informatie toegankelijk is voor ongeautoriseerde personen.	Medewerkers delen accountgegevens waardoor ook onbevoegden toegang krijgen tot informatie die beschermd moet blijven.	
9	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 of geautomatiseerd gedeeld worden vanuit de applicatie.	21
9	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.	14
9	Logboeknotities zijn toegankelijk voor te veel medewerkers.	Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie.	De autorisatie voor logboeknotities zijn standaard aangezet (opt-in), terwijl niet duidelijk is of de autorisatiegroepen toegang hiertoe moeten hebben.	71
6	Het is niet mogelijk de gegevensuitwisseling die middels geautomatiseerde koppelingen gedeeld wordt te wijzigen/filteren zonder hulp van de Verwerker.	Er worden meer gegevens gedeeld dan nodig en wenselijk.	Het wijzigen van de inhoud van geautomatiseerde berichtenverkeer is niet mogelijk voor de Verantwoordelijke.	5
6	Het leerlingdossier wordt uitgewisseld (VO-VO) zonder inzage door ouders/verzorgers	Onrechtmatige uitwisseling van gegevens.	Inzage is niet of onvoldoende geborgd in processen. De triggers hiervoor vanuit de applicatie ontbreken.	19
6	Inbreuk op rechten en vrijheden van betrokkenen (bij inzageverzoeken).	Er wordt te veel informatie uitgewisseld met andere partijen (bij dossier uitwisseling).	Meer informatie (niet-objectief) vastleggen in leerlingnotities (vrije velden) dan noodzakelijk.	24
6	Er worden te veel rollen toegekend aan gebruikers.	Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie.	Het ‘stapelen’ van rollen. Onvoldoende inzage en/of inzicht en/of vaardigheid zijn beschikbaar om het te veel rollen toekennen aan banden te kunnen leggen.	22
6	Gegevens worden onnodig op papier vastgelegd.	Retentie van gegevens is langer dan nodig. Dubbele registratie. Geen dataminimalisatie en minder regie.	Aanmeldgegevens kunnen voor inschrijving niet geregistreerd worden.	15

Risicoscore (Kans x Impact)	Omschrijving	Gevolgen	Oorzaak	ID
6	Persoonsgegevens worden onbeveiligd, buiten de applicatie om vastgelegd	Persoonsgegevens worden buiten de applicatie vastgelegd.	Onvoldoende kennis bij gebruikers en beheerders over de technische en functionele mogelijkheden van het LVS.	12
6	Het informatiebeveiligingsbeleid wordt niet periodiek geëvalueerd.	De organisatie is niet in control als het gaat om de risico's met betrekking tot de verwerkingen in de applicatie.	De toegepaste maatregelen ten aanzien van informatiebeveiliging worden niet beoordeeld of deze 'up to date' of 'passend' zijn omdat o.a. (periodieke) uitvoering van DPIA's niet wordt toegepast.	34
6	Onderhoud en update van software van derden wordt niet actief onderhouden.	De applicatie werkt niet meer naar behoren of werkt met extra veiligheidsrisico's.	Software van derden (zoals operating system of libraries) wordt niet actief onderhouden en up-to-date gehouden, denk aan verouderde browsers of besturingsplatforms.	50
6	Met onveilige wachtwoorden kan toegang verkregen worden tot de applicatie.	Er worden zwakke wachtwoorden gebruikt voor (zeer) lange periode, waardoor de kans op een 'hack' wordt vergroot.	De applicatie stelt standaard geen eisen aan het wachtwoord, bv. ten aanzien van het periodiek wijzigen van het wachtwoord, etc.	6
6	De toegang tot de Magister-app kan eenvoudig worden gedeeld door uitwisseling van wachtwoord-gebruikersnaam.	Verschillende leerling-accounts kunnen eenvoudig 'onderdak' vinden binnen de Magister-app. Leerlingen delen wachtwoord-gebruikersnaam o.a. om elkaars rooster te kunnen inzien (ongeoorloofde maar wellicht wel wenselijke verwerking). Ook andere ongeoorloofde en onwenselijke gegevensverwerkingen kunnen plaatsvinden.	Magister-app heeft geen 2-factor-authentication of andere functionaliteit om per gebruiker het aantal en type accounts te reguleren.	46
6	Wachtwoorden worden opgeschreven. Voor meerdere applicaties wordt hetzelfde wachtwoord gebruikt.	Het wachtwoord is te eenvoudig te vinden of in te zien en te stelen en dat vergemakkelijkt onrechtmatige toegang tot persoonsgegevens voor onbevoegden.	Wachtwoorden worden opgeschreven in agenda of op een post-it en zijn daardoor te gemakkelijk te vinden en te gebruiken Er wordt één wachtwoord gebruikt voor meerdere of zelfs alle systemen.	74

Risicoscore (Kans x Impact)	Omschrijving	Gevolgen	Oorzaak	ID
6	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.	52
4	De set persoonsgegevens die wordt uitgewisseld bij overstap naar een andere school binnen het bestuur, wordt niet beperkt tot enkel de vereiste gegevens.	Er worden meer gegevens uitgewisseld dan strikt noodzakelijk.	Er wordt binnen de applicatie een leerlingdossier overgezet naar een andere school binnen het schoolbestuur, maar niet via de procedure van OSO.	77
4	Kennis over applicatiebeheer binnen of bovenschools is te beperkt aanwezig, het is bijvoorbeeld belegd bij één persoon en/of niet vastgelegd in instructies of werkprocessen.	Kennis gaat verloren als degene ziek is of vertrekt.	Onvoldoende borging van de kennis en het ontbreken van procedures en werkprocesbeschrijvingen.	9
4	Rechten komen niet overeen met functies, rollen of taken binnen de organisatie.	Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie.	Er is geen proces ingericht voor het controleren of wijzigen van de rechten binnen de applicatie.	42
4	Standaardrollen sluiten onvoldoende aan bij sommige functies op school waardoor aan deze functies meerdere verschillende standaardrollen worden toegekend met als gevolg een surplus aan rechten die niet nodig zijn.	Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie.	Standaardrollen worden gestapeld op sommige functies in plaats van passend op de functie aangepast.	4
4	Er worden meer gegevens geregistreerd dan noodzakelijk.	Dataminimalisatie in de registratiesectie van de applicatie is niet op orde, waardoor de AVG niet wordt nageleefd.	Meer gegevens kunnen vastleggen dan noodzakelijk (bv. opleiding en beroep ouders, godsdienst, maar ook NAW-gegevens medewerkers). Velden die niet noodzakelijk zijn, worden aangeboden in de applicatie en worden daarom ook gevuld.	10
4	Het gebruikersbeheer wordt niet adequaat uitgevoerd of verschillend op locaties die binnen een bestuur vallen.	Het gebruiksbeheer (verstrekken en intrekken van accounts) is niet (altijd) actueel, dan wel niet altijd goed toegepast.	Er is geen centraal gebruikersbeheer en / of vastgesteld toegangsbeveiligings-beleid waardoor regie ontbreekt. Dit is met name het geval bij scholen met meerdere locaties.	3

Risicoscore (Kans x Impact)	Omschrijving	Gevolgen	Oorzaak	ID
4	Het niet of niet tijdig wissen of wissen van gebruikersaccounts en aanpassen naar de actuele functiegebonden status.	Gebruikers hebben (langer) toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie of hebben nog toegang nadat ze uit dienst zijn getreden.	Gebruikersaccounts worden niet tijdig gewist. Automatische 'triggers' in het proces of het systeem hiervoor ontbreken. Proces om inactieve accounts te traceren is niet (onvoldoende) bekend of wordt niet uitgevoerd.	29
4	Gegevens van ouders en leerlingen niet actueel (bijvoorbeeld bij overdracht)	De data-integriteit, oftewel de juistheid van de gegevens, in de registratiesectie van de applicatie is niet op orde, waardoor de AVG niet wordt nageleefd.	Persoonsgegevens worden niet periodiek gecontroleerd op juistheid. Wijzigingen in de gegevens worden niet doorgegeven of correct en tijdig verwerkt. Procesafspraken hierover ontbreken.	25
4	Er is geen geïmplementeerd beleid voor logische toegang tot de applicatie via autorisaties.	Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie.	De hoeveelheid van rollen binnen de applicatie is groot en onduidelijk. Medewerkers krijgen hierdoor meerdere rollen toebedeeld en dat maakt dat ze meer aan die rollen verbonden rechten krijgen dan strikt nodig voor uitoefening van de eigen functie.	61
4	Bepaalde rollen (kolomkiezer) geven gebruikers meer rechten dan op basis van 'need to know' nodig zijn.	Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie.	Kolomkiezer, iemand met rechten op de kolomkiezer, kan via deze rol toch bij gegevens waarvoor hij vanuit andere ro(len) niet geautoriseerd is. De autorisatie werkt dus niet door in de velden die je kunt oproepen in de kolomkiezer	78
4	Beveiligingsincidenten en datalekken worden niet als zodanig herkend en/of niet gemeld.	Het niet (onvoldoende) op de hoogte zijn van mogelijke bedreigingen of niet weten hoe datalekken gemeld moeten worden kan leiden tot datalekken of niet tijdig ingrijpen.	Medewerkers zijn zich onvoldoende bewust van informatiebeveiliging en privacy risico's en weten niet hoe te handelen bij een incident.	65
3	Bij aanmelding (bij meerdere scholen) wordt het onderwijskundig rapport (OKR) niet verwijderd als de leerling niet wordt ingeschreven.	Er worden meer persoonsgegevens geregistreerd dan wettelijk is toegestaan.	De gegevens van aangemelde leerlingen die niet worden ingeschreven worden niet gewist. Procesafspraken hiervoor ontbreken.	70

Risicoscore (Kans x Impact)	Omschrijving	Gevolgen	Oorzaak	ID
3	Onvoldoende kennis over mogelijkheden applicatie.	Onveilige opslag van persoonsgegevens buiten applicatie. Inzageverzoeken niet volledig.	Persoonsgegevens worden onnodig en onvoldoende beveiligd buiten de applicatie vastgelegd	43
3	De applicatie ondersteunt de mogelijkheid om adequaat uitvoering te geven aan inzageverzoeken, deze functie is niet of onvoldoende bekend bij de gebruikers.	Aan inzageverzoeken wordt onvoldoende tegemoet gekomen waardoor de school in gebreke blijft.	Het is complex om betrokkenen inzage te geven in hun persoonsgegevens en dit komt weinig voor waardoor het proces onvoldoende bekend is bij gebruikers.	45
3	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.	48
2	Bij de overdracht van leerlingdossier wordt meer informatie (in de vorm van bijlagen) toegevoegd (zonder toestemming) waardoor er meer wordt uitgewisseld dan toegestaan. Dit geldt ook voor uitwisseling binnen het schoolbestuur.	Ouders/verzorgers kunnen klachten indienen bij de school of de Autoriteit Persoonsgegevens.	Er wordt geen inzage verleend of toestemming gevraagd aan ouders voor de uitwisseling van informatie aan een andere school of organisatie.	20
1	Gegevens van leerlingen van andere scholen (binnen een bestuur) kunnen worden ingezien door medewerkers.	Gebruikers hebben toegang tot persoonsgegevens die niet noodzakelijk zijn voor het uitoefenen van hun functie.	Databases van verschillende scholen (binnen het bestuur) zijn niet gescheiden. NB. Dit verschilt per schoolbestuur.	72
1	Gegevensuitwisselingen die middels geautomatiseerde koppelingen gedeeld worden, kunnen worden onderschept.	Gegevensuitwisselingen kunnen via ‘man-in-the-middle’ attacks[3] worden onderschept.	Geautomatiseerde koppelingen zijn onvoldoende beveiligd.	73

[3] Een man-in-the-middle-aanval (MITM-aanval) is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben.

Specifieke 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.

Risicoscore (Kans x Impact)	Omschrijving	Gevolgen	Oorzaak	ID

5. Beschrijving van aanbevolen maatregelen

Invulinstructie

- Lees het hoofdstuk en pas de tekst aan indien gewenst, beoordeel hierbij in ieder geval de rode teksten en pas deze aan naar de situatie van de eigen organisatie.
- 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, zet de conclusie ten aanzien van de restrisico's op 'Ja'. Zijn niet alle maatregelen toegepast, pas dan de conclusie ten aanzien van de restrisico's aan en geef aan of dit gemitigeerd is tot een acceptabel niveau. En geef hierbij, bij 'Maatregelen geïmplementeerd?', met letters aan welke maatregelen zijn geïmplementeerd, welke zo spoedig mogelijk worden geïmplementeerd en welke niet worden geïmplementeerd en/of met andere maatregelen worden gemitigeerd.

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[4]. De statements zijn geprioriteerd en per cluster gerangschikt van Zeer hoog naar Zeer laag.

5.1. 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.

Statement 5.1.1.	**Toegang tot persoonsgegevens wordt verleend volgens het vastgestelde toegangsbeveiligingsbeleid (ISO 9.4.2).**	**Urgentie:**	**Zeer hoog**
Gerelateerde risico's	2. Er is geen specifiek beleid met betrekking tot toegangsbeveiliging. Toegangsbeveiliging omvat de toegang tot het ICT-systeem en de toegang via autorisatie tot een applicatie dat draait binnen het ICT systeem.		9
	71. Logboeknotities zijn toegankelijk voor te veel medewerkers.		9

[4] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging

	59. De stringente voorwaarden waaronder bijzondere persoonsgegevens door een geselecteerde groep medewerkers kunnen worden verwerkt, worden niet of onvoldoende toegepast	9
	22. Er worden te veel rollen toegekend aan gebruikers.	6
	6. Met onveilige wachtwoorden kan toegang verkregen worden tot de applicatie.	6
	74. Wachtwoorden worden opgeschreven. Voor meerdere applicaties wordt hetzelfde wachtwoord gebruikt.	6
	42. Rechten komen niet overeen met functies, rollen of taken binnen de organisatie.	4
	4. Standaardrollen sluiten onvoldoende aan bij sommige functies op school waardoor aan deze functies meerdere verschillende standaardrollen worden toegekend met als gevolg een surplus aan rechten die niet nodig zijn.	4
	3. Het gebruikersbeheer wordt niet adequaat uitgevoerd of verschillend op locaties die binnen een bestuur vallen.	4
	29. Het niet of niet tijdig wissen of wissen van gebruikersaccounts en aanpassen naar de actuele functiegebonden status.	4
	61. Er is geen geïmplementeerd beleid voor logische toegang tot de applicatie via autorisaties.	4
	78. Bepaalde rollen (kolomkiezer) geven gebruikers meer rechten dan op basis van 'need to know' nodig zijn.	4
	72. Gegevens van leerlingen van andere scholen (binnen een bestuur) kunnen worden ingezien door medewerkers.	1
Maatregelen	a. De toegangsrechten zijn vastgesteld en worden toegepast op rol gebaseerde autorisatiematrices. b. De verantwoordelijkheid voor het verstrekken, controleren en intrekken van gebruikersaccounts en bijbehorende rechten is belegd binnen de organisatie en wordt conform uitgevoerd. c. Het wachtwoordbeleid inclusief het gebruik van 2-factor-authentication is gecommuniceerd met medewerkers. d. Het periodiek wijzigen van wachtwoord en/of de complexiteit van het wachtwoord wordt afgedwongen in de applicatie (indien er geen gebruik wordt gemaakt van 2-factor-authentication). e. Groepsautorisaties worden bij bepaalde rollen als ‘default setting’ ingesteld. f. Er wordt op leerlingniveau of onderdelen van een leerlingdossier autorisaties ingesteld. g. Inactieve accounts van medewerkers worden (periodiek) inzichtelijk gemaakt en opgeschoond (indien van toepassing).	
Uit te voeren door:	Verwerkingsverantwoordelijke	
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 / Nee**

Statement 5.1.2.	Persoonsgegevens worden gewist volgens het vastgestelde beleid voor bewaren en wissen (AVG art. 5).	Urgentie:	Zeer hoog
Gerelateerde risico's	17. Persoonsgegevens worden niet (tijdig) gewist.		9
	70. Bij aanmelding (bij meerdere scholen) wordt het onderwijskundig rapport (OKR) niet verwijderd als de leerling niet wordt ingeschreven.		3
Maatregelen	a. Er zijn richtlijnen vastgesteld voor het bewaren, corrigeren en wissen van persoonsgegevens, waarbij rekening is gehouden met wettelijke verplichtingen. b. Er zijn procedures voor het bewaren, corrigeren en wissen van persoonsgegevens beschreven. c. De verantwoordelijkheden voor het bewaren, corrigeren en wissen van persoonsgegevens zijn belegd in de organisatie.		
Uit te voeren door:	Verwerkingsverantwoordelijke		
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 / Nee

5.2. 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.

Statement 5.2.1.	Betrokkenen kunnen hun rechten uitoefenen met betrekking tot de verwerking van persoonsgegevens in het LAS (AVG art. 12).	Urgentie:	Zeer hoog
Gerelateerde risico's	19. Het leerlingdossier wordt uitgewisseld (VO-VO) zonder inzage door ouders/verzorgers		6
	45. De applicatie ondersteunt de mogelijkheid om adequaat uitvoering te geven aan inzageverzoeken, deze functie is niet of onvoldoende bekend bij de gebruikers.		3
Maatregelen	a. Aan ouders/verzorgers wordt inzage verleend in het onderwijskundig rapport of leerlingdossier voordat het wordt uitgewisseld met een andere school. b. 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. Zo nodig wordt toestemming gevraagd en vastgelegd. c. De gebruikers weten hoe de functionaliteit van de applicatie voor het verlenen van inzage aan de betrokkenen is toe te passen.		
Uit te voeren door:	Verwerkingsverantwoordelijke		
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 / Nee

Statement 5.2.2.	Medewerkers die gebruik maken van het LAS worden geschoold in het juist verwerken van persoonsgegevens (ISO 7.2.2).	Urgentie:	Midden

Gerelateerde risico's	9. Kennis over applicatiebeheer binnen of bovenschools is te beperkt aanwezig, het is bijvoorbeeld belegd bij één persoon en/of niet vastgelegd in instructies of werkprocessen.	4
	43. Onvoldoende kennis over mogelijkheden applicatie.	3
Maatregelen	a. Medewerkers worden voorgelicht en getraind 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. b. Applicatiebeheerders worden opgeleid in het juist inrichten en beheren van het LAS met betrekking tot de verwerking van persoonsgegevens (privacy by default). c. Er zijn voor de applicatiebeheerders werkprocessen beschreven voor het verstrekken, controleren en intrekken van accounts en het wissen van persoonsgegevens.	
Uit te voeren door:	Verwerkingsverantwoordelijke	
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 / Nee**

5.3. 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. Er zijn in dit cluster geen risico's geconstateerd.

5.4. 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.

Statement 5.4.1.	**Er zijn passende maatregelen genomen om de continuïteit van het onderwijs te waarborgen (AVG art. 32)**	**Urgentie:**	**Hoog**
Gerelateerde risico's	50. Onderhoud en update van software van derden wordt niet actief onderhouden.		6
	52. Gegevens zijn voor onbepaalde periode niet beschikbaar.		6
	48. Gegevens gaan verloren of worden onleesbaar gemaakt		3
Maatregelen	a. Er zijn richtlijnen en procedures voor het uitvoeren van updates en patches aanwezig en deze worden gecontroleerd toegepast. b. Er wordt periodiek een kopie (back-up) van de gegevens in de applicatie gemaakt middels een beveiligde opslag. c. Er is een procedure om in het geval van DDOS aanvallen de continuïteit te borgen en deze wordt periodiek getoetst en zo nodig aangescherpt.		
Uit te voeren door:	Verwerkingsverantwoordelijke (a en c) en Verwerker (b)		
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 / Nee**

5.5. 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.

Statement 5.5.1.	**Er mogen niet meer persoonsgegevens worden uitgewisseld dan strikt noodzakelijk en alleen op basis van grondslag en doelbinding (AVG art. 5, 6, 25).**	**Urgentie:**	**Zeer hoog**
Gerelateerde risico's	37. Koppelen van gegevensbestanden ten behoeve van managementrapportages leidt ertoe dat privacygevoelige gegevens herleidbaar zijn tot personen.		9
	5. Het is niet mogelijk de gegevensuitwisseling die middels geautomatiseerde koppelingen gedeeld wordt te wijzigen/filteren zonder de Verwerker.		6
	46. De toegang tot de Magister-app is o.b.v. wachtwoord-gebruikersnaam.		6
	77. De set persoonsgegevens die wordt uitgewisseld bij overstap naar een andere school binnen het bestuur, wordt niet beperkt tot enkel de vereiste gegevens.		4
	20. Bij de overdracht van leerlingdossier wordt meer informatie (in de vorm van bijlagen) toegevoegd (zonder toestemming) waardoor er meer wordt uitgewisseld dan toegestaan. Dit geldt ook voor uitwisseling binnen het schoolbestuur.		2
Maatregelen	a. Geautomatiseerde koppelingen waarbij er meer gegevens worden uitgewisseld dan noodzakelijk worden niet gebruikt (Privacy by design), met uitzondering van uitwisselingen die op basis van wettelijke verplichtingen moeten plaatsvinden. b. 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.		
Uit te voeren door:	Verwerkingsverantwoordelijke (a) en Verwerker (b)		
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 / Nee**

Statement 5.5.2.	**Het maken van handmatige exports van persoonsgegevens is alleen toegestaan wanneer er afdoende waarborgen aanwezig zijn voor de bescherming van de persoonsgegevens (AVG art. 32).**	**Urgentie:**	**Zeer hoog**
Gerelateerde risico's	21. Maken van handmatige exports van overzichten waarmee gegevens buiten de regie van het LAS komen en onbeveiligd gedeeld worden.		9
Maatregelen	a. Persoonsgegevens worden vanuit het LAS/LVS uitgewisseld via beveiligde geautomatiseerde koppelingen. Het werken met handmatige exports is alleen beargumenteerd toegestaan met expliciete toestemming van de verwerkingsverantwoordelijke (het bevoegd gezag). b. Er zijn gedragsregels en richtlijnen voor medewerkers voor het opslaan en uitwisselen van persoonsgegevens en deze worden gecontroleerd toegepast.		
Uit te voeren door:	Verwerker (a) en Verwerkingsverantwoordelijke		
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 / Nee**

Statement 5.5.3.	Het downloaden van bestanden met persoonsgegevens uit het LAS wordt beperkt (AVG art. 5, 32).	Urgentie:	Zeer hoog
Gerelateerde risico's	8. Het bekijken (downloaden) van bestanden in leerlingendossiers (op privé devices) zorgt voor een lokale kopie van het dossier.		9
	12. Persoonsgegevens worden onbeveiligd, buiten de applicatie om vastgelegd.		6
Maatregelen	a. Waar mogelijk wordt de opslag van lokale kopieën beperkt of voorkomen. b. Het wissen van lokale kopieën wordt geautomatiseerd uitgevoerd of hierover worden controleerbare afspraken gemaakt met medewerkers. c. Bestanden met persoonsgegevens kunnen vanuit de applicatie alleen worden ingezien en/of gedownload door medewerkers die daarvoor geautoriseerd zijn.		
Belegd bij:	Verwerkingsverantwoordelijke (a en b) en Verwerker (c)		
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 / Nee

Statement 5.5.4.	De bescherming van de juistheid en de vertrouwelijkheid van persoonsgegevens wordt gewaarborgd. (AVG art. 5, 32).	Urgentie:	Zeer hoog
Gerelateerde risico's	55. Juistheid van kritieke gegevens, zoals de uitslagen van toetsen, examens, onomkeerbare financiële transacties, kan niet gegarandeerd worden.		9
	65. Beveiligingsincidenten en datalekken worden niet als zodanig herkent en/of niet gemeld.		4
	25. Gegevens van ouders en leerlingen niet actueel (bijvoorbeeld bij overdracht)		4
Maatregelen	a. Gegevens die met Hoog zijn geclassificeerd op het kwaliteitsaspect Data-integriteit worden ingevoerd op basis van het '4-ogen-principe. b. Persoonsgegevens worden voordat ze uitgewisseld worden voorgelegd aan betrokkene ter inzage en controle. c. Kritieke gegevens worden periodiek gecontroleerd op juistheid, door betrokkene en de organisatie. Er wordt minstens eenmaal per jaar aan betrokkenen (leerlingen, ouders, medewerkers) gevraagd om relevante mutaties in de persoonsgegevens door te geven.		
Uit te voeren door:	Verwerkingsverantwoordelijke		
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 / Nee

Statement 5.5.5.	Bijzondere of gevoelige persoonsgegevens worden beveiligd gemaild (AVG art. 32).	Urgentie:	Zeer hoog
Gerelateerde risico's	14. Er kan wel gemaild worden, maar niet beveiligd bijv. door encryptie met wachtwoord, beperkte beschikbaarheidstermijn of het niet kunnen doorsturen of downloaden.		9
Maatregel	a. 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').		

Uit te voeren door:	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 / Nee**

Statement 5.5.6.	**Er mogen niet meer persoonsgegevens worden geregistreerd dan strikt noodzakelijk (AVG art. 5).**	**Urgentie:**	**Hoog**
Gerelateerde risico's	24. Inbreuk op rechten en vrijheden van betrokkenen (bij inzageverzoeken).		6
	15. Gegevens worden onnodig op papier vastgelegd.		6
	10. Er worden meer gegevens geregistreerd dan noodzakelijk.		4
Maatregelen	a. Het schoolbestuur moet zelf kunnen bepalen welke velden verplicht ingevuld moeten worden, dit moet niet door het LAS worden bepaald. b. Medewerkers moeten op de hoogte zijn welke persoonsgegevens voor welk doel vastgelegd moeten worden. Indien mogelijk kan het LAS hierin ondersteunen. c. Er zijn gedragsregels en richtlijnen voor medewerkers voor het registreren en formuleren van leerlingnotities en deze worden gecontroleerd toegepast.		
Uit te voeren door:	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 gemitigeerd tot een acceptabel niveau.		**Ja / Nee**

Statement 5.5.7.	**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	73. Gegevensuitwisselingen die middels geautomatiseerde koppelingen gedeeld worden, kunnen worden onderschept.		1
Maatregel	a. Geautomatiseerde koppelingen waarbij er persoonsgegevens worden uitgewisseld voldoen aan de actuele versie van de Edukoppeling transactiestandaard en het Certificeringsschema ROSA.		
Uit te voeren door:	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 / Nee**

5.6. 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.

Statement 5.6.1.	**Er vinden periodieke controles plaats op het juist toepassen van het toegangsbeveiligingsbeleid (ISO 9.2.5 en AVG art. 32).**	**Urgentie:**	**Zeer Hoog**
Gerelateerde risico's	56. De logging van gebruikersactiviteiten wordt niet (periodiek) gemonitord.		9

	34. Het informatiebeveiligingsbeleid wordt niet periodiek geëvalueerd.	6
Maatregel	a. Er wordt minstens eenmaal per jaar gecontroleerd of de vastgestelde autorisaties overeenkomen met de toegekende rollen en rechten in de applicatie. b. Het informatiebeveiligingsbeleid wordt als onderdeel van een PDCA-cyclus geëvalueerd.	
Uit te voeren door:	Verwerkingsverantwoordelijke	
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 / Nee**

5.6.2.	**Er wordt periodiek een audit uitgevoerd op de beveiligingsmaatregelen die genomen zijn door de verwerker (ISO 18.2.2).**	**Urgentie:**	**Hoog**
Gerelateerde risico's	34. Het informatiebeveiligingsbeleid wordt niet periodiek geëvalueerd.		16
Maatregel	a. Er zijn met de Verwerker afspraken gemaakt over de periodieke uitvoering van audits aan de verwerkers kant. b. Er is een planning voor het periodiek uitvoeren van een audit door Verantwoordelijke.		
Uit te voeren door:	Verwerker (a) en Verwerkingsverantwoordelijke (b)		
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 / Nee**

6. Conclusie, aanvaarding en goedkeuring

Invulinstructie

- Lees het hoofdstuk en pas de tekst aan indien gewenst, beoordeel hierbij in ieder geval de rode teksten en pas deze aan naar de situatie van de eigen organisatie.
- 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.

6.1. 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 bij toepassing 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.

6.2. Conclusie beoordeling rechtmatigheid

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

6.3. Aanvaarding restrisico's

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

6.4. 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**

6.5. Raadpleging verwerker

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

6.6. 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**

6.7. Follow up

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

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

7. Vaststelling en aanvaarding

Invulinstructie

- Lees het hoofdstuk en pas de tekst aan indien gewenst, beoordeel hierbij in ieder geval de rode teksten en pas deze aan naar de situatie van de eigen organisatie.
- Laat de bestuurder de DPIA vaststellen, d.w.z. de restrisico's aanvaarden en de voorgestelde beheersmaatregelen goedkeuren.

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 – Magister
- 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:

8. 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.