CENTRALE DPIA

MAX

Uitgeverij L.C.G. Malmberg B.V.

Model versie 2.0 (Maart 2024)

Malmberg MAX DPIA Versie 1.0

Colofon

DPIA uitgevoerd door	Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A. (SIVON) www.sivon.nl info@sivon.nl
Betrokkenen bij uitvoering DPIA	*Schrijvers van de DPIA:* Sander van de Molen (jurist en adviseur IBP) Susan Ashworth (adviseur IBP) Pascal Marcelis (adviseur IBP) *Betrokken bij de uitvoering van de DPIA:* Ashley Hoogendoorn (DPIA-projectmanager) Reza Razai (ISO en adviseur IBP) Randy Baerts (adviseur IBP)
Met dank aan	Team van Malmberg: Donovan Prins (Privacy Officer Sanoma Learning BeNe-regio) Ilja Förster (Manager Market Enablement Sanoma Learning BeNe-regio) André Schouten (Methode Ontwikkelaar Digitaal 12+ Sanoma) Marianum Scholengemeenschap (Carmel College): I. Kamphuis, B. Siebers en D. Visschedijk
Auteurs model DPIA	Hans-Peter Ligthart (portfoliomanager IBP SIVON) Job Vos (jurist en adviseur IBP SIVON) Ferdy IJsselmuiden (DPIA-projectmanager)

Versiebeheer

Datum	Versie	Wijziging
Maart 2022	*0.0*	*Model Concept (HL)*
Mei 2022	*1.0*	*Model Basisversie (JV)*
Februari 2023	*1.1*	*Model Wijzigen risico-tabel (FI)*
Juni 2023	*1.2*	*Model Algemene verbeteringen, opnemen proces toetsen verwerkersovereenkomst, diverse technische vragen ondergebracht in bijlagen*
Februari 2024	*1.3*	*Model Aanpassingen en actualisatie (nieuw Rijksmodel 3.0)*
Maart 2024	*2.0*	*Model Nieuwe publieke versie sjabloon DPIA model SIVON*
December 2024	0.1	Uitschrijven DPIA MAX
Augustus 2025	0.91	Afstemmen Malmberg
September 2025	0.92	Afstemmen Malmberg
29 september 2025	1.0	Publicatie DPIA MAX

Inhoudsopgave

1. Leeswijzer

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

Hoofdstuk 1 betreft deze leeswijzer.

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

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

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

De uitvoering van de DPIA bestaat uit de volgende onderdelen:

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

Bijlage 1 bevat veelgebruikte termen en definities.

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

2. Samenvatting

Deze DPIA heeft betrekking op de digitale leeromgeving MAX voor het Voortgezet Onderwijs (VO), die door Uitgeverij L.C.G. Malmberg B.V. (hierna ook: Malmberg), onderdeel van Sanoma Learning, wordt geleverd aan scholen voor het VO. MAX omvat een compleet pakket: boeken, een online leeromgeving, uitgebreid docentenmateriaal en aanvullend lesmateriaal. Voor deze DPIA staat de online leeromgeving centraal.

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

Via MAX hebben leerlingen en docenten van de onderwijsinstelling toegang tot al het door de school beschikbaar gestelde lesmateriaal. Dit omvat *Exacte vakken, Mens & Maatschappij en Talen*.

Samenwerking
De samenwerking tijdens het DPIA-proces met Malmberg als leverancier van MAX was ronduit positief te noemen. De open werkwijze, goede gesprekken en gemotiveerde houding om verbetervoorstellen door te voeren hebben bijgedragen aan het onderzoek en identificatie van de risico's. Tijdens de uitvoering van de DPIA zijn er door Malmberg al bepaalde bevindingen opgelost of aangepast, zoals het bewaren van loggegevens (loggegevens m.b.t. 'wijzigen' van 4 weken naar 13 maanden), een gebruikte Google Font API en (web)teksten met betrekking tot de adaptiviteit binnen MAX.

Bovendien heeft de deelnemende school belangrijke praktijkinzichten gebracht die wezenlijk waren voor het begrip van de werking en het gebruik van MAX.

Conclusie
Malmberg als leverancier van MAX heeft de in deze DPIA geconstateerde risico's ofwel gedurende de uitvoering van de DPIA opgelost, dan wel voor bepaalde risico's een oplossing voorgesteld die binnen afzienbare termijn wordt toegepast. Ook heeft Malmberg aangegeven een aantal verbeteringen nog te zullen doorvoeren, die het met name voor de onderwijsinstelling eenvoudiger maken om haar rol als verwerkingsverantwoordelijke goed uit te kunnen oefenen, zoals het uitbreiden van de loggingfunctionaliteit met inzicht in welke gebruikers exports/downloads hebben uitgevoerd.

Wanneer scholen en Malmberg zich houden aan de voorgestelde maatregelen kan het gebruik van MAX op een veilige manier plaatsvinden. Het schoolbestuur zal zelf de centrale DPIA nog specifiek moeten maken en eventuele restrisico's accepteren.

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

1. De verwerking van persoonsgegevens rechtmatig kan plaatsvinden en ook noodzakelijk is om het doel te bereiken;
2. De inbreuk op de persoonlijke levenssfeer in verhouding staat tot het doel en er geen minder belastende manier is om hetzelfde doel te bereiken;
3. Er adequate maatregelen zijn en worden getroffen om de verwerking te beschermen.

Risico's en maatregelen

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

1. Risico:
Exportfunctionaliteit is standaard beschikbaar zonder beperkingen (exporteren/downloaden by default aan).

Maatregel:
Malmberg: Gaat exporteren/downloaden zichtbaar maken in logging (zie ook bij 2).
Onderwijsinstelling: moet afspraken maken over het genereren en gebruiken van exports en hier controle op uitoefenen.

2. Risico:
Er worden onvoldoende beveiligingsmaatregelen toegepast (loggingfunctionaliteit).

Maatregel:
Malmberg: Gaat loggingfunctionaliteit uitbreiden met inzicht in welke gebruikers exports/downloads hebben uitgevoerd, alsmede wie mutaties in cijfers heeft uitgevoerd.

3. Risico:
Er worden onvoldoende beveiligingsmaatregelen toegepast (toegang tot loggingfunctionaliteit).

Maatregel:
Malmberg: Gaat aan onderwijsinstellingen zelf toegang geven tot logging, zodat men zelfstandig kan monitoren.
Onderwijsinstelling: Moet afspraken maken over controle op de logging.

4.Risico:
Geen grondslag, onvoldoende transparantie, onvoldoende beveiligingsmaatregelen toegepast (YouTube-filmpjes).

Maatregel:
Malmberg: Gaat alternatieve oplossing implementeren voor gebruik filmpjes, waar mogelijk.

5.Risico:
Er worden onvoldoende beveiligingsmaatregelen toegepast (hashing).

Maatregel:
Malmberg: Gaat alternatieve hashing-methode implementeren.

6. Risico:
Er worden onvoldoende beveiligingsmaatregelen toegepast (audits).

Maatregel:
Malmberg: Gaat periodieke uitvoering van audits op het interne ISMS van MAX, of certificering ISO 27001, aantoonbaar maken.

7. Risico:
Ontoereikende afspraken in de verwerkersovereenkomst over de verwerking van de persoonsgegevens.

Maatregel:
Malmberg: Zodra een nieuwe versie van de model verwerkersovereenkomst inclusief model bijlagen beschikbaar is, wordt deze nieuwe versie gehanteerd en aan de daarbij behorende vereisten voldaan.
Onderwijsinstelling: Moet deze nieuwe versie doorvoeren zodra deze beschikbaar is.

8. Risico:
Achterhaalde informatie in de verwerkersovereenkomst over de verwerking van de persoonsgegevens (bewaartermijn logfiles).

Maatregel:
Malmberg: Gaat dit aanpassen in nieuwe versie verwerkersovereenkomst.

9. Risico:
Er worden onvoldoende beveiligingsmaatregelen toegepast (transport en fysieke opslag).

Maatregel:
Malmberg: Gaat de vereiste maatregel hieromtrent uit ROSA certificeringsschema implementeren.

10.Risico:
Gebrek aan transparantie (informatie over adaptiviteitsfunctionaliteit).

Maatregel:
Onderwijsinstelling: Moet betrokkenen hierover adequaat informeren.

3. Uitleg en achtergrond DPIA

1. Informatiebeveiliging en privacy (IBP)

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

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

2. Privacyconvenant en toetsing verwerkersovereenkomsten

Volgens de Europese privacywet Algemene Verordening Gegevensbescherming (AVG) is een schoolbestuur eindverantwoordelijk voor de bescherming van de privacy en persoonsgegevens van leerlingen, hun ouders, en medewerkers. Het schoolbestuur wordt **verwerkingsverantwoordelijke** genoemd. Het schoolbestuur moet de controle houden over het gebruik van deze persoonsgegevens en zij bepaalt dus voor welke doelen deze gegevens mogen worden gebruikt. Een leverancier van software waarin al deze persoonsgegevens zijn opgenomen, wordt in de AVG **verwerker** genoemd. Deze mag die persoonsgegevens niet zomaar voor eigen doeleinden gebruiken. In een **verwerkersovereenkomst** legt het schoolbestuur afspraken vast met deze leverancier. In het onderwijs wordt hiervoor gebruik gemaakt van de model-verwerkersovereenkomst van het Privacyconvenant onderwijs[1].

Scholen kunnen gemakkelijk verwerkersovereenkomsten goedkeuren en digitaal ondertekenen met behulp van de Dienst Verwerkersovereenkomsten van Kennisnet[2]. SIVON toetst voor het primair en voortgezet onderwijs vooraf of de verwerkersovereenkomsten van leveranciers van de meest-gebruikte applicaties voldoen aan de eisen van het Privacyconvenant[3]. Deze rapportages zijn onder andere beschikbaar in de Dienst Verwerkersovereenkomsten.

[1] https://www.privacyconvenant.nl/
[2] https://www.kennisnet.nl/dienst-verwerkersovereenkomsten/
[3] https://sivon.nl/toetsen-verwerkersovereenkomsten/

3. DPIA

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

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

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

4. Verplichte uitvoering DPIA

Deze privacytoets is verplicht als de verwerking van persoonsgegevens - gelet op de aard, de omvang, de context en de doeleinden van die verwerking - waarschijnlijk een hoog risico inhoudt voor de 'rechten en vrijheden’ (privacy) van leerlingen en medewerkers. Ook is het mogelijk dat het uitvoeren van een DPIA verplicht is volgens de regels van de privacy toezichthouder Autoriteit Persoonsgegevens (AP) die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van aan DPIA verplicht is[4]. Voor het onderwijs betekent dit dat een DPIA altijd verplicht is op tenminste het leerlingvolg- en/of -administratiesysteem (LVS/LAS), personeelsadministratiesysteem en breed ingezette applicaties met digitaal leermateriaal. Dit is ook de bedoeling van de EDPB[5]: ‘*Een gegevensbeschermingseffectbeoordeling kan ook nuttig zijn om het gegevensbeschermingseffect van een technologisch product te beoordelen, bijvoorbeeld*

[4] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf
[5] EDPB: European Data Protection Board (de Europese privacy toezichthouder): https://www.edpb.europa.eu/edpb_en.

hardware of software, indien dit waarschijnlijk door verschillende verwerkingsverantwoordelijken zal worden gebruikt om verschillende verwerkingen uit te voeren. Natuurlijk blijft de verwerkingsverantwoordelijke die het product lanceert verplicht om zijn eigen gegevensbeschermingseffectbeoordeling uit te voeren met betrekking tot de specifieke implementatie, al kan hij zich hiervoor baseren op een door de productaanbieder uitgevoerde gegevensbeschermingseffectbeoordeling, in voorkomend geval.'

Voor MAX geldt dat het gaat om verwerking van persoonsgegevens op grote schaal van kwetsbare personen (leerlingen). Dit betekent dat er een DPIA-plicht is.

5. Centrale en lokale DPIA

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

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

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

6. Methodiek DPIA

SIVON volgt bij de uitvoering van de centrale DPIA het model van de Rijksoverheid[6], aangevuld met onderwijsspecifieke informatie uit de *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*[7]. Het model is daarnaast aangepast aan specifieke informatie over de applicatie en aangevuld met een model lokale DPIA voor schoolbesturen. Er wordt rekening gehouden met Europese richtlijnen van de gezamenlijke Europese toezichthouders (EDPB) waaronder de “Richtsnoeren voor gegevensbeschermingseffectbeoordelingen (2016/679, 4 april 2017)".

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

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

7. Funderend onderwijs referentie architectuur (FORA)

Gebruik FORA: Funderend Onderwijs Referentie Architectuur

Applicatie landschap

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

[6] Model DPIA Rijksdienst v3.0.pdf (kcbr.nl)
[7] https://aanpakibp.kennisnet.nl/app/uploads/Handreiking-DPIA-v1.0-1.pdf

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

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

De FORA biedt inzicht in wat de bedrijfsfuncties zijn van een po en vo school. Het hoofdbedrijfsfunctiemodel beschrijft op hoofdlijnen wat een onderwijsorganisatie doet. Verdieping daarvan vindt plaats in het bedrijfsfunctiemodel dat in meer detail weergeeft op welke manier een invulling gegeven wordt aan het 'wat'. Hiermee is het mogelijk om ‘referentiecomponenten’ toe te voegen. Referentiecomponenten zijn typen systemen - zoals een LAS, een toetssysteem, of een ELO - met bijbehorende functionaliteiten ('applicatiefuncties').

In deze DPIA gebruiken we FORA om een applicatie te kunnen plaatsen in het applicatie-landschap (welke plaats neemt de applicatie in, in het totaal aan applicaties die een school gebruikt).

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

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

4. Motivering DPIA MAX

1. Verplichting uitvoeren DPIA

Bij het onderzoek naar de online omgeving van MAX van leverancier L.C.G. Malmberg B.V., is gebleken dat het uitvoeren van een DPIA verplicht is om de volgende redenen.

Volgens het overzicht van de European Data Protection Board[8] wordt aan verschillende criteria voldaan. Hierdoor spreken we van een 'hoog risicoverwerking'. Er is namelijk sprake van een verwerking 'op grote schaal' (verwerking van persoonsgegevens van leerlingen in het VO met een verspreidingsgebied over geheel Nederland). Daarnaast heeft deze verwerking van persoonsgegevens deels betrekking op kinderen onder de 16 jaar. Deze vorm van gegevensverwerking vereist een extra bescherming omdat het hier kwetsbare personen betreft. Dit betreft een tweede criterium. Een derde criterium betreft de verwerking van 'gevoelige gegevens' die kunnen leiden tot 'evaluatie of scoretoekenning', omdat er binnen MAX leer- en testresultaten worden verwerkt over een langere periode en deze resultaten zichtbaar zijn voor gebruikers (leerkrachten en leerlingen). Hieruit volgt dat er sprake is van ten minste twee criteria uit de lijst van de WP29 op basis waarvan een DPIA verplicht is om uit te voeren door de verwerkingsverantwoordelijke bij gebruikmaking van deze applicatie.

Volgens de lijst van de Autoriteit Persoonsgegevens[9] is er tevens sprake van '15. Profilering'. Dit gaat om een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op automatische verwerking, zoals bijvoorbeeld prestaties van leerlingen. Ook het voldoen aan dit criterium stelt het uitvoeren van een DPIA verplicht. Bij MAX gaat het hier specifiek om het vastleggen van resultaten van leerlingen ('leerprestaties') van methodetoetsen over een langere periode, waarin door middel van een dashboard de prestaties van leerlingen ten opzichte van andere leerlingen inzichtelijk zijn. Docenten kunnen hieruit afleiden dat een leerling bijvoorbeeld extra ondersteuning nodig heeft. Het vastleggen van leerprestaties is uiteraard een wezenlijk onderdeel van het onderwijs, aangezien beoordelingen en voortgangsregistratie onmisbaar zijn voor het leerproces en het verantwoorden van onderwijskwaliteit. In deze zin is 'profileren' een bijkomend logisch onderdeel van het onderwijs.

2. Scope van deze DPIA

Deze DPIA heeft betrekking op de online omgeving van MAX, een blended leeromgeving die door L.C.G. Malmberg B.V. als leverancier wordt geleverd aan scholen voor het voorgezet onderwijs. Kinderen, leerlingen in het voortgezet onderwijs, maken gebruik van deze

[8] De 'WP29 werkgroep' (vanaf mei 2018: European Data Protection Board – EDPB): zie de WP29-richtlijn voor DPIA's (WP 248 rev.01 zoals vastgesteld op 4 april 2017, en laatstelijk gewijzigd op 4 oktober 2017).
[9] Zie Staatscourant 2019, nummer 64418 van 27 november 2019.

leermethode. De risico's die het gebruik van de online leeromgeving van dit digitale leermiddel met zich meebrengen worden in deze DPIA geïnventariseerd. Op basis van de risico's wordt nagegaan of de juiste maatregelen worden toegepast om deze risico's te minimaliseren, zodat een veilig gebruik van MAX mogelijk is.

MAX is een blended leerplatform voor het aanleren van vooraf bepaalde leerdoelen voor diverse vakken in het voortgezet onderwijs, zoals bijvoorbeeld biologie, Nederlands, Engels, wiskunde en geschiedenis.

De online omgeving van dit oefen- en toetsplatform gebruiken leerlingen om (individueel) opdrachten en aanvullend digitaal lesmateriaal te gebruiken, inclusief adaptieve oefeningen en summatieve[10] en formatieve[11] toetsen en zelftoetsen.

MAX ondersteunt leerlingen bij het leren, verwerken en oefenen van de leerstof. Het stelt docenten in staat het onderwijs af te stemmen op individuele behoeften en stimuleert leerlingen om zelfstandig en op hun eigen niveau te leren.

Doel hiervan is om bij te dragen aan de verbetering van de studieresultaten en het bevorderen van zelfstandig leren van de leerlingen. Leerlingen kunnen behaalde resultaten direct inzien. De leraar heeft inzicht in de voortgang en resultaten van leerlingen. Op basis van de resultaten van het gebruik van digitale leermiddelen kan de onderwijsinstelling zelf conclusies trekken over de leerontwikkeling van leerlingen.

Link naar uitgever en/of productpagina: https://www.malmberg.nl/voortgezet-onderwijs/over-max.htm

Doelgroep: Voortgezet onderwijs (VO).

Gebruikers: leerlingen, leraren en beheerder(s).

De scope van deze DPIA beperkt zich tot de verwerking van persoonsgegevens in het kader van het gebruik van de online omgeving van MAX.

3. Buiten scope

Buiten scope van deze DPIA valt:

- Het uitwisselen van leer- en testresultaten met het Leerling Administratie Systeem van de onderwijsinstelling.

[10] Een summatieve toets is een vorm van toetsen die gericht is op het vaststellen van wat een leerling heeft geleerd aan het einde van een leerperiode of leertraject. Het doel van een summatieve toets is om de *leerprestaties te beoordelen*, vaak met een cijfer, en om te beslissen of een leerling een bepaald leerdoel heeft behaald.

[11] Een formatieve toets is een toets die wordt gebruikt om het leerproces te bevorderen en niet om leerprestaties te beoordelen. De nadruk ligt op feedback en het identificeren van punten die verfijnd moeten worden, in plaats van op een cijfer of een eindconclusie.

- Het uitwisselen van leer- en testresultaten met dashboards die de onderwijsinstelling in gebruik heeft.
- De inlogsystematiek via Entree Federatie, omdat dit buiten het interne landschap valt (zie DPIA Entree Federatie).

Indien koppelingen wenselijk zijn, wordt voor het beoordelen van deze specifieke risico's verwezen naar de DPIA's die gaan over de beoordeling van een Leerling Administratie Systeem (LAS) van bijvoorbeeld Magister of Somtoday, en andere digitale diensten die specifiek ingaan op het vastleggen van leerresultaten en het verder uitwisselen van persoonsgegevens via koppelingen.

5. Deel A: Gegevensverwerkingsanalyse

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

1. Beschrijving van het gegevensverwerkende proces

MAX is een leerplatform voor het aanleren van vooraf bepaalde leerdoelen voor diverse vakken in het voortgezet onderwijs, zoals biologie, Nederlands, Engels, wiskunde en geschiedenis.

De online omgeving van dit oefen- en toetsplatform gebruiken leerlingen om (individueel) opdrachten en aanvullend digitaal lesmateriaal te gebruiken, inclusief adaptieve oefeningen en summatieve en formatieve toetsen en zelftoetsen.

Leerlingen kunnen behaalde resultaten direct zelf inzien. De leraar heeft inzicht in de voortgang en resultaten van leerlingen en kan op basis hiervan sturing geven en eventueel rapportages opstellen.

Middels een inlog via Entree kunnen leerlingen en docenten met een combinatie van inlognaam en wachtwoord (eventueel via Single Sign On/2FA/MFA) de digitale leeromgeving van MAX bereiken. Hierbij worden persoonsgegevens verwerkt, zoals in deze DPIA weergegeven.

2. Persoonsgegevens

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

Betrokkenen

In MAX worden persoonsgegevens verwerkt van leerlingen van de onderwijsinstelling en van medewerkers (docenten en beheerders) van de onderwijsinstelling.

Persoonsgegevens

De volgende typen persoonsgegevens worden in de MAX verwerkt.

Tabel 2.1 Persoonsgegevens

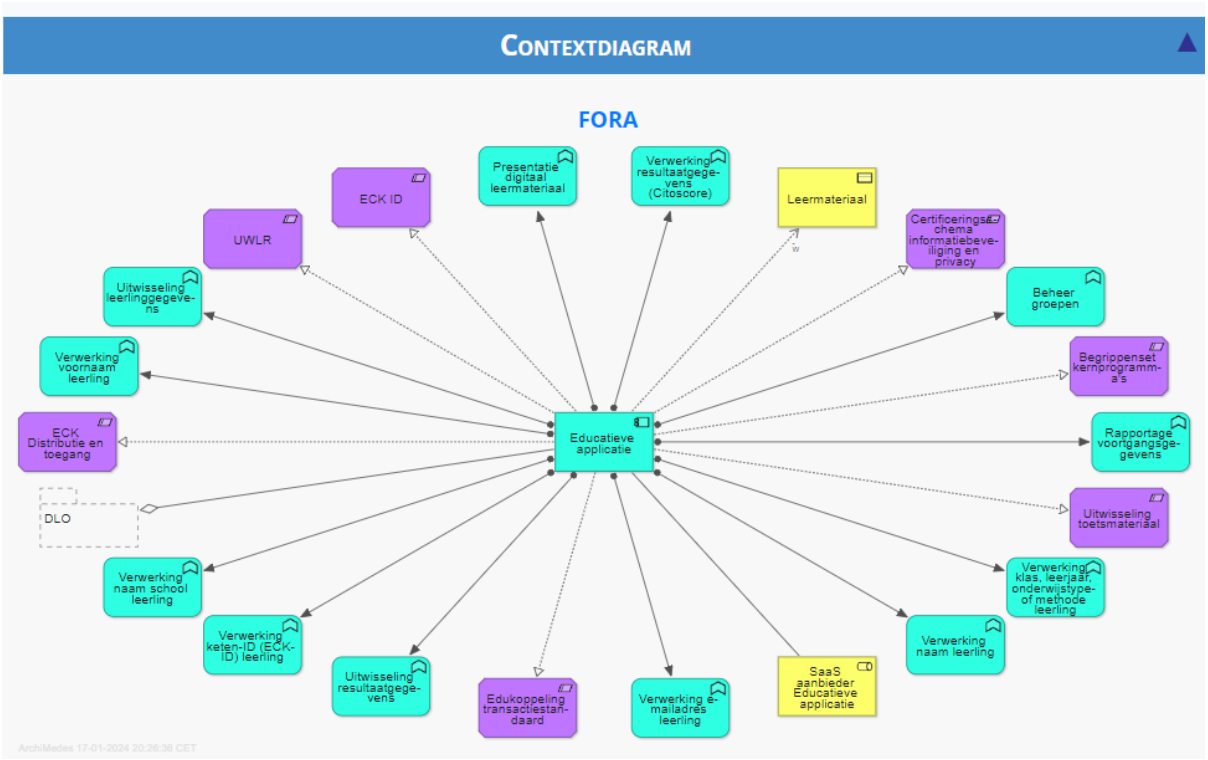
Categorie persoonsgegevens	Categorie betrokkene	Persoonsgegeven	Bron/verkrijging persoonsgegeven
Algemene contactgegevens	(Minderjarige) leerlingen	- Voornaam - Tussenvoegsel - Achternaam	SSO-dienst Entree Federatie, of eigen invoer
Overige contactgegevens		- Schoolnaam - Brincode	SSO-dienst Entree Federatie, of eigen invoer
Overige gegevens		- MalmbergID - Rol (leerling) - Niveau - Naam van de klas - ECK-iD - nlEduPersonRealId - nlEduPersonProfileId - uid - Oefenopgaven - Toetsopgaven - Leer- en testresultaten)	SSO-dienst Entree Federatie, of eigen invoer
Algemene contactgegevens	Medewerker	- Voornaam - Tussenvoegsel - Achternaam	SSO-dienst Entree Federatie, of eigen invoer
Overige contactgegevens		- Schoolnaam - Brincode	SSO-dienst Entree Federatie, of eigen invoer
Overige gegevens		- MalmbergID - Rol (docent) - Sectornaam - Klassencode	SSO-dienst Entree Federatie, of eigen invoer

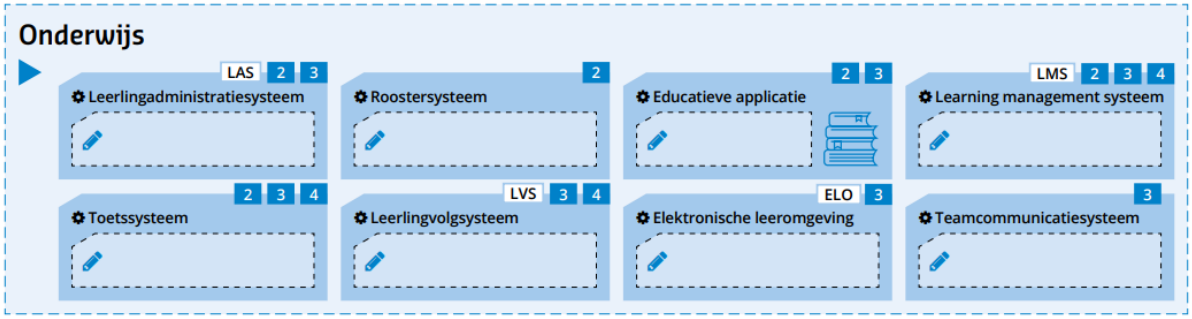
Algemene Contactgegevens en Overige (contact) gegevens (conform medewerker)	Beheerders (niet een aparte functionaliteit)	- Voornaam - Tussenvoegsel - Achternaam - Schoolnaam - Brincode - MalmbergID - Sectornaam - Rol (docent)	SSO-dienst Entree Federatie, of eigen invoer
Overige	Allen	Uitwisseling van andere attributen wordt vastgelegd in een verzoek uitbreiding attributen. - E-mailadres docent - Gebruikersafbeelding Chat en/of FAQ-ondersteuning: - E-mailadres docent - Sessie-informatie (tijd, browsergegevens, IP-adres) - Chatberichten - Paginabezoeken - Opt-in systeemberichten In-app feedback: - MalmbergID - Naam - Nummer Onderwijsinstelling - Besturingssysteem (incl. Useragent) - Browserinformatie - Datum melding	SSO-dienst Entree Federatie, of eigen invoer
Overige	Allen	Loggegevens - inlogactiviteit gebruikers - wijziging van (persoons)gegevens)	MAX / applicatie

3. Gegevensverwerkingen

De verwerkingen binnen MAX vinden primair plaats om onderwijsinstellingen in staat te stellen om met gebruikmaking van de digitale leermiddelen onderwijs te geven en leerlingen te volgen en te begeleiden.

MAX wordt in termen van FORA geduid als ‘Educatieve applicatie’.





Voor de beschrijving van de verwerkingen die binnen MAX plaatsvinden is aansluiting gezocht bij de verwerkersovereenkomst en de FORA.

In de verwerkersovereenkomst staan de verwerkingen opgesomd. Deze staat ook aan de basis van de scope bepaling van deze DPIA, zie hoofdstuk 2 van deze DPIA. Raadpleging van de FORA (zie hierboven weergegeven afbeelding ‘Contextdiagram[12]’) heeft geen aanleiding

[12] https://fora.wikixl.nl/index.php/FORA/id-3476eb2d-278a-4ecf-8931-f5d510a71b1b.

gegeven tot het verder uitbreiden van de scope. De binnen de FORA vastgelegde elementen omvatten de elementen zoals deze in de scope van de DPIA zijn meegenomen.

Bij het gebruik van de digitale leermiddelen voor het voortgezet onderwijs vinden altijd de volgende verwerkingen plaats, in lijn met artikel 5 van het Convenant Digitale Onderwijsmiddelen en Privacy:

- De opslag, analyse en interpretatie van leer- en testresultaten;
- Het terugontvangen door de onderwijsinstelling van leer- en testresultaten;
- De beoordeling van leer- en testresultaten om leerstof en toetsmateriaal te verkrijgen of aan te bieden, dat is afgestemd op de specifieke leerbehoefte van een leerling;
- Het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
- Het verkrijgen van toegang tot de aangeboden digitale leermiddelen, waaronder de identificatie, authenticatie en autorisatie;
- De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik, en het voorkomen van inconsistentie en onbetrouwbaarheid in de verwerkte persoonsgegevens;
- De continuïteit en goede werking van het digitale leermiddel, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning.

Adaptiviteit

Binnen MAX wordt gewerkt met een beperkte vorm van adaptiviteit in de methode zelf als ook in het onderdeel Versterk Jezelf. Het betreft geen geavanceerde algoritmes of inzet van een AI-model. De uitleg van Malmberg hierover is als volgt:

*“De ruggengraat van de Versterk Jezelf is **het concept**. In het concept staat wat je gaat doen als leerling. Bijvoorbeeld 'Future gebruiken (will/won't)' (Engels) of 'Feit of mening? (moderne tijd)' (Geschiedenis). In de **content** verbinden we de concepten (optioneel) aan elkaar door zogenaamde prerequisites/voorwaardelijkheden. Je kan bijvoorbeeld zeggen het concept 'Present simple' is voorwaardelijk voor het concept 'Present continuous'. Wanneer de leerling het concept 'Present continuous' dan niet goed maakt, wordt de leerling doorgestuurd naar het concept 'Present simple'. Didactisch gezien betekent het zoveel als 'je hebt kennis van de Present simple nodig, voordat je de Present continuous kan beheersen'. Een leerling wordt alleen doorgestuurd als een concept fout wordt gemaakt. Als de leerling een concept goed maakt, wordt het concept afgerond wanneer alle opdrachten van dat concept zijn gemaakt. De leerling wordt niet meer dan twee keer doorgestuurd. Dus niet dieper dan een voorwaardelijke concept van een voorwaardelijk concept van het originele concept.*
Naast deze verbinding door voorwaardelijkheden, leggen we in de content optioneel de verbinding tussen bepaalde opdrachtschermen in MAX met bepaalde concepten van de

Versterk Jezelf. Het gaat vaak om een verbinding tussen grammatica opdrachten en de daarbijhorende Versterk Jezelf concepten. Als de leerling dan een aantal opdrachtschermen fout heeft, krijgt de leerling een pop-up met de suggestie naar het gelinkte Versterk Jezelf concept te gaan. Als de leerling naar de Versterk Jezelf gaat, is de werking zoals hierboven beschreven."

Er vindt binnen de adaptiviteit geen verwerking plaats met het oog op de beoordeling van de leer- en testresultaten van één leerling ten opzichte van de resultaten van een normgroep, om inzicht te krijgen hoe een leerling presteert ten opzichte van deze groep.

Adaptiviteit binnen MAX wordt gebruikt om leerlingen te ondersteunen in het leerproces. Door leerlingen niet te vermoeien met opdrachten die zij al goed kunnen maar juist extra oefeningen aan te bieden van de leerdoelen die zij nog niet (volledig) beheersen.

De conclusie is dat er slechts een beperkte functionaliteit is met betrekking tot de adaptiviteit in de leermethode. Op basis van de vragen goed/fout, worden alleen makkelijke of juist moeilijker vragen gesteld. Het betreft een niet-zelflerend[13] algoritme en er vindt binnen dit regelgebaseerd algoritme geen profilering plaats. De aanbevelingen komen tot stand in een geïsoleerde situatie die niet gekoppeld is aan andere (voortgangs)resultaten, zoals methodetoetsen en cijfers. Dit betekent dat bij het niet of niet optimaal behalen van de beheersingsniveaus binnen de adaptiviteitsmodule dit geen invloed heeft op het uiteindelijke cijfer van de leerling. Ook vindt er geen (leer en/of onderwijs) niveau-inschatting van de leerling plaats op basis van de gebruikte adaptiviteit.

Hierdoor is er geen sprake van een AI-Systeem[14] in de zin van de AI-Verordening, dat wordt gebruikt voor het bepalen van toegang of toelating, noch het 'evalueren van leerresultaten', het beoordelen van het passende onderwijsniveau, dan wel het monitoren of detecteren van ongeoorloofd gedrag.

In het kader van de transparantieverplichting heeft Malmberg gedurende het DPIA-traject de teksten op de website over adaptiviteit binnen MAX aangepast. Deze suggereerden een meer geavanceerdere werking waardoor betrokkenen andere conclusies zouden kunnen trekken over de verwerking van hun gegevens.

Onderwijsinstellingen zijn zelf, als verwerkingsverantwoordelijken, ook verplicht hierover transparant te zijn en dienen dit derhalve op te nemen in hun verantwoording over verwerking van persoonsgegevens.

[13] De mens specificeert de regels die de computer moet volgen (regelgebaseerde algoritmes met een specifiek vooraf ontworpen stappenplan).
[14] Zie Bijlage III bij de AI-Verordening: een uitwerking van de in artikel 6 lid 2 van de AI-Verordening bedoelde AI-Systemen met een hoog risico.

Optionele verwerkingen

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

Onderwijsinstellingen hebben voor deze verwerkingen een actieve keuzeoptie en gaan in de verwerkersovereenkomst, of opdracht voor het inzetten van digitale leermiddelen voor het voortgezet onderwijs of anderszins, expliciet akkoord met de verwerkingen voordat deze plaatsvinden.

Het betreft de volgende verwerkingen, welke *buiten* de scope van deze DPIA vallen (zie hoofdstuk 2, Scope):

- Het kunnen uitwisselen van leer- en testresultaten met leerling administratiesystemen van de onderwijsinstelling;
- Het kunnen uitwisselen van leer- en testresultaten met dashboards die de onderwijsinstelling in gebruik heeft;
- Het beschikbaar stellen van gegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan digitale onderwijsmiddelen;
- Het door de onderwijsinstelling beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek.

Applicatielandschap

In deze DPIA ligt de focus op de leeromgeving (applicatie) MAX. In het applicatielandschap van een schoolbestuur kunnen vanuit de applicatie koppelingen worden gelegd met andere applicaties. De andere applicaties vallen niet binnen de scope van deze DPIA.

[School: geef hier het applicatielandschap aan. etc.].

Koppelingen

Entree Federatie geeft gebruikers in het vo en mbo toegang tot een groot aantal educatieve diensten met slechts één login (ook wel bekend als Single Sign On of SSO). De federatie wordt gevormd door aanbieders van een educatieve dienst of content (Service Providers), beheerders van identiteiten (Identity Providers) en de applicatie van Kennisnet (Entree Federatie).

Een Identity Provider is de applicatie die voor de school de communicatie met Entree Federatie verzorgt. Voorbeelden van Identity Providers zijn:

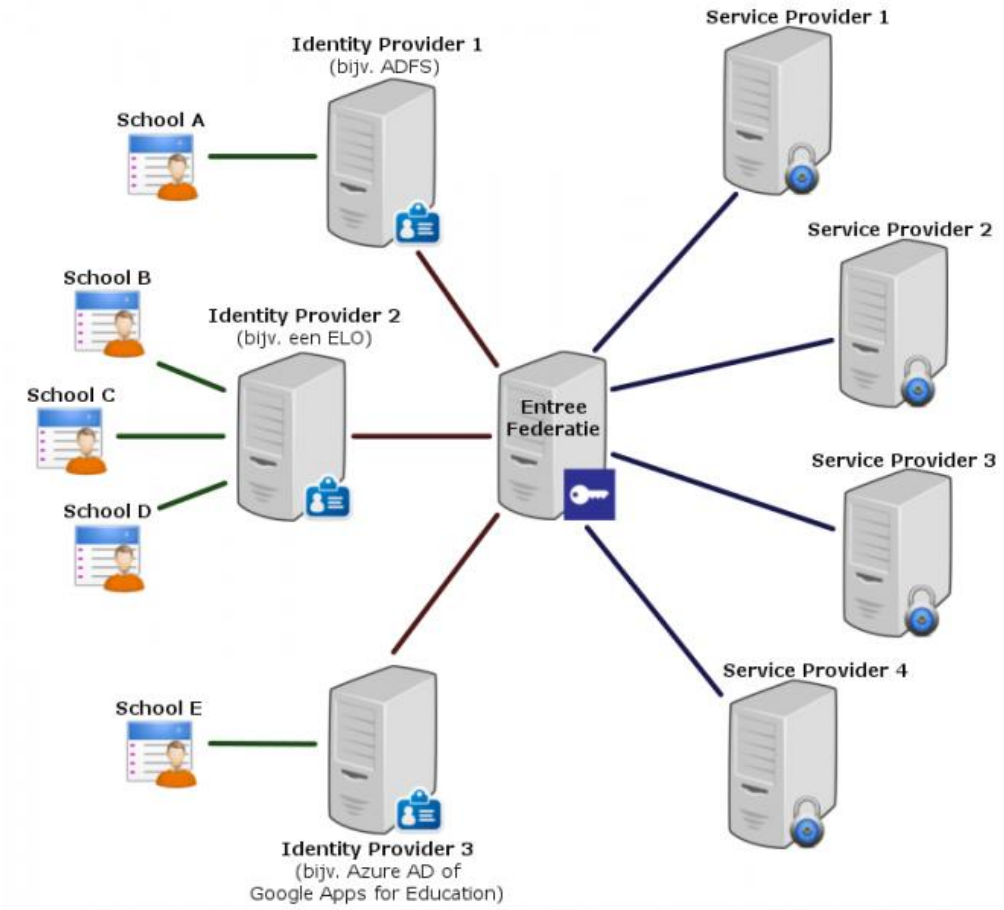
- Elektronische Leeromgevingen (een centrale digitale omgeving die meestal door meerdere scholen wordt gebruikt);

- Active Directory Federation Service (ADFS), zoals Microsoft;
- Google Apps for Education;
- Azure AD.

De applicatie van Entree Federatie fungeert als een federatieve intermediair (of hub) in het authenticatieproces. Het is dus het centrale knooppunt waarlangs alle federatieve authenticatie berichten worden afgehandeld.

MAX van Malmberg is een educatieve dienst en wordt daarom beschouwd als een 'Service Provider'.

Voor de koppeling met Entree is onderstaande overzichtsplaat van toepassing*



* [Entree Federatie - Funderend Onderwijs Referentie Architectuur (wikixl.nl)]

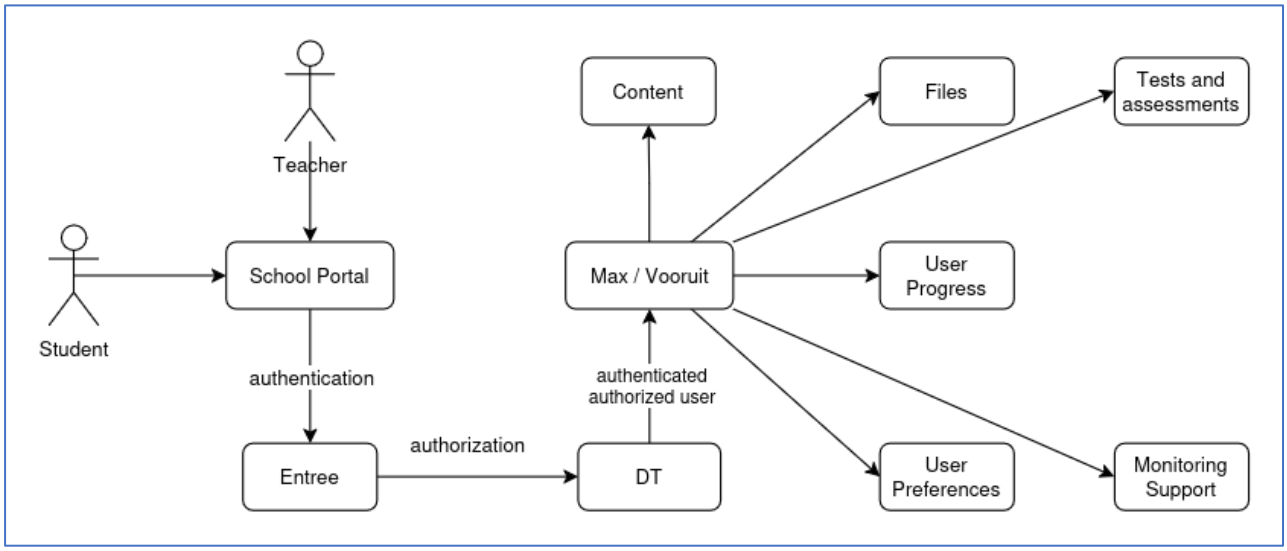
Bovenstaande visualisatie laat zien hoe Entree Federatie (SSO t.b.v. vo en mbo) zich verhoudt tot MAX als service provider ten aanzien van het tot stand komen van toegang tot digitaal lesmateriaal.

De toegang tot MAX kan alleen gerealiseerd worden via een koppeling met Entree, waarbij 2FA/MFA wordt afgedwongen. De toegang via 2FA/MFA wordt in deze DPIA als een

belangrijke beheersmaatregel gezien, omdat MAX veel (gevoelige) persoonsgegevens bevat, waaronder leerresultaten over een langere periode. Deze worden door de Autoriteit Persoonsgegevens[15] gezien als 'profilering', waardoor onder andere extra technische waarborgen nodig zijn. Deze vorm van toegangsbeveiliging is daar een onderdeel van.

Gegevensstromen/stroomschema

Hieronder wordt in een vereenvoudigde weergave aangegeven hoe de gegevensstromen binnen MAX plaatsvinden.



Bron: Malmberg

Details over alle betrokken partijen zijn beschreven in hoofdstuk 5.

4. Verwerkingsdoeleinden

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

[15] Zie: https://www.autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia; Staatscourant 2019, nr. 64418, 27 november 2019, onderdeel 15. Profilering: Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering), zoals bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.

De FORA[16] is gebruikt om de verwerkingsdoeleinden te bepalen.

Voor MAX is, zoals eerder aangegeven, het referentiecomponent 'Educatieve applicatie'. De relatie tussen referentiecomponent en bedrijfsfuncties wordt gebruikt als definitie van het doel van de verwerking, zijnde: "Verzamelbegrip van applicaties, ingezet voor of ontwikkeld met een educatief doel, dat onderwijsdeelnemers ondersteunt bij het uitvoeren van leertaken."

De verwerkingsdoeleinden sluiten aan bij de in het Privacyconvenant[17] opgenomen verwerkingsdoeleinden.

De verwerkingsdoeleinden zijn schematisch weergegeven en gekoppeld aan de verwerking.

Tabel 4.1 Verwerkingsdoeleinden en verwerking

Doeleinde verwerking	Gegevensverwerking	Toelichting
Onderwijsevaluatie	De opslag van leer- en toetsresultaten.	Resultatenregistratie. Beoordeling.
Onderwijsevaluatie	Het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten.	Resultatenregistratie.
Leerlingbegeleiding	De beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer.	Monitoring en begeleiding voortgang leerroute en leerproces. Onderwijsbegeleiding. Voortgang- en resultatenweergave.
Leerlingbegeleiding	Analyse en interpretatie van leer- en toetsresultaten.	Monitoring en begeleiding voortgang leerroute en leerproces.
Inkoop en contractbeheer Ict-ondersteuning Onderwijsuitvoering	Het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier.	Inkoop Beheer ict-middelen. (Toegang tot) aanbod leermateriaal.
Onderwijsuitvoering Ict-ondersteuning	Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen,	(Toegang tot) aanbod leermateriaal. Beheer identiteiten.

[16] https://fora.wikixl.nl/index.php/Hoofdpagina en https://fora.wikixl.nl/index.php/DPIA
[17] https://www.privacyconvenant.nl/downloads

	waaronder de identificatie, authenticatie en autorisatie.	Authenticatie en autorisatie.
Informatiebeveiliging en privacy	De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens.	
Ict-ondersteuning (Inkoop en contractbeheer)	De continuïteit, verbetering en goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning.	Beheer ict-middelen (Contractbeheer).

5. Betrokken partijen

De hieronder genoemde organisaties zijn betrokken bij de volgende gegevensverwerkingen.

Tabel 5.1 Betrokken partijen en gegevensverwerking

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens	Verstrekker of ontvanger
Onderwijs-instelling	Verwerkings-verantwoordelijke	Beheer en toepassing van het digitaal leermateriaal	Alle genoemde persoonsgegevens	Verstrekker
L.C.G. Malmberg B.V.	Verwerker	Aanbieder digitaal leermateriaal	Alle genoemde persoonsgegevens	Ontvanger
Aknostic	Subverwerker	Serviceprovider	Alle genoemde persoonsgegevens	Ontvanger
Amazon Webservices	Subverwerker	Hostingprovider, cloudservices	Alle genoemde persoonsgegevens	Ontvanger
Datadog, Inc.	Subverwerker	Opslag logging	Gepseudonimiseerde gegevens (voor Datadog anoniem)	Ontvanger
Zendesk	Subverwerker	Chat- en FAQ-ondersteuning voor docenten	E-mailadres docent Sessie-informatie (tijd, browsergegevens, IP-adres)* Inhoud chatberichten Paginabezoeken Opt-in systeemberichten	Ontvanger
Sanoma – Group IT	Subverwerker	Inrichting AWS security maatregelen	Alle genoemde persoonsgegevens	Ontvanger
Sanoma – analytics	Subverwerker	Voorwerk voor productanalyse	Gepseudonimiseerde gegevens (voor Sanoma analytics anoniem)	Ontvanger
Sanoma – analytics	Subverwerker	Het analyseren van de effectiviteit van de content met het doel deze te verbeteren ten behoeve van de kwaliteit van het onderwijs	Geanonimiseerde persoonsgegevens	Ontvanger

Uit de verwerkersovereenkomst: “Naast bovengenoemde subverwerkers maken enkele methodes in de applicaties gebruik van YouTube filmpjes. Malmberg biedt deze aan in

‘privacy enhanced mode’. Na het aanklikken van het filmpje worden er cookies van YouTube geplaatst.’’

Dit kan leiden tot onrechtmatige verwerking van persoonsgegevens. Immers, als de school de aanvullende services van Google niet aan heeft staan, worden er via het gebruik van YouTube binnen MAX alsnog door Google persoonsgegevens verwerkt. Zie ook hoofdstuk 19, Risico’s.

6. Belangen bij de gegevensverwerking

De Onderwijsinstelling heeft belang bij een goed werkend en betrouwbaar digitaal leermiddel waarmee zij optimaal kan lesgeven en de leerling zich maximaal kan ontwikkelen.

De belangen die Malmberg heeft, zijn het leveren van een goed werkende digitale omgeving waarin leermiddelen en toetsen worden aangeboden. Hierbij heeft Malmberg ook een commercieel belang; een goed werkend product levert financieel voordeel op en het ondersteunt een goede reputatie en marktpositie van Malmberg.

De belangen van de geïdentificeerde subverwerkers is ondersteunend aan het hierboven genoemde hoofddoel: een goed werkende digitale leer-en toetsapplicatie. Daarnaast geldt ook voor hen het commerciële belang.

7. Verwerkingslocaties

Hieronder is beschreven in welke landen de gegevensverwerkingen plaatsvinden.

Tabel 7.1 Verwerkingslocaties

Naam partij	Statutaire vestigings-plaats (sub-) verwerker	Beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt verwerkt door deze subverwerker	Plaats/land van opslag en verwerking persoonsgegevens en doorgifte mechanisme indien buiten de EER
L.C.G. Malmberg B.V.	’s-Hertogenbosch	Zie hoofdstuk 5, kolom Functie/taak	Nederland
Aknostic	Utrecht	Idem	Nederland
Amazon Webservices (AWS)	Seattle, VS	Idem	Ierland (EU)
Datadog, Inc.	New York City, VS	Idem	Ierland (EU) of Duitsland
Zendesk	Amsterdam	Idem	Ierland (EU)
Sanoma – Group IT	Helsinki, Finland	Idem	Nederland
Sanoma – analytics	Helsinki, Finland	Idem	Nederland

Met AWS zijn volgens de verwerkersovereenkomst aanvullende afspraken (Standard Contractual Clauses) gemaakt, net als met Datadog Inc. Ook zijn aanvullende maatregelen genomen, zoals het niet-standaard gebruiken van services die ondersteund worden vanuit de VS, en het aanleveren van gepseudonimiseerde gegevens waar mogelijk.

Binnen Sanoma, waar Malmberg onderdeel van uitmaakt, hebben alle bedrijven een intracompany verwerkersovereenkomst getekend.

8. Data Transfer Impact Assessment (DTIA)

Voor de (sub)verwerkers die betrokken zijn bij MAX zijn waar nodig de EU-Standard Contractual Clauses (SCC) afgesloten, zoals hierboven aangegeven. Zowel AWS als Datadog Inc. zijn tevens onderdeel van het Data Transfer Framework. Er zijn daarom geen DTIA's uitgevoerd.

9. Technieken en methoden van gegevensverwerking

Artikel 32 van de AVG schrijft voor dat er passende technische en organisatorische maatregelen genomen moeten worden om een op het risico afgestemd beveiligingsniveau te waarborgen. Om inzicht te krijgen in welke mate er vorm wordt gegeven aan deze abstracte formulering is gebruik gemaakt van de voor de verwerkers opgestelde standaard DPIA-vragenlijst. Deze vragenlijst is door Malmberg ingevuld en geeft voor een belangrijk deel inzicht geven in o.a. de bestaande technische beheersmaatregelen en informatiebeveiliging. Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende risico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, AI/algoritmes, cloud, nieuwe technologie, profilering en big dataverwerkingen.

De antwoorden gegeven door Malmberg op de vragenlijst zijn besproken tussen SIVON (CISO) en Malmberg en waar nodig verder uitgediept, om volledig inzicht te krijgen in het gevraagde.

Status van informatiebeveiliging

Er is onderzoek verricht naar de status van informatiebeveiliging van MAX[18]. Dit onderzoek is uitgevoerd door de informatie van Malmberg te analyseren, door in een demo-omgeving

[18] Er is geen diepgaand technisch- of verificatieonderzoek uitgevoerd naar het implementatieniveau van de beveiliging.

van MAX onderzoek te doen en door een compliance check op het ROSA certificeringsschema uit te voeren.

Hieruit is het volgende vastgesteld:

- Er wordt door Malmberg in het ROSA certificeringsschema een BIV classificatie[19] toegepast voor de applicatie MAX op het niveau Hoog-Midden-Midden. Dit betekent dat Malmberg de 'Vertrouwelijkheid' van de persoonsgegevens beoordeelt als 'Midden'. Vanuit SIVON is aangegeven dat er sprake is van een Vertrouwelijkheidsscore 'Hoog'. Dit vanwege het feit dat in de applicatie sprake is van '*profilering*' conform de omschrijving van de Autoriteit Persoonsgegevens[20]:

  15. Profilering
  Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering), zoals bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.

  De Autoriteit Persoonsgegevens gaat duidelijk in op het verwerken van persoonsgegevens van *kwetsbare jongeren* in een geautomatiseerd systeem dat toetsresultaten en andere persoonsgegevens verwerkt. Dit wordt vervolgens *profilering* genoemd en gelabeld als een '*hoog risico verwerking' (corresponderend met classificatie 'Hoog' qua Vertrouwelijkheid in het ROSA schema)*, waarbij de juiste technische en organisatorische maatregelen moeten worden toegepast.

  Hierdoor is er een discrepantie in de beoordeling van de maatregelen op het niveau van Vertrouwelijkheid 'Hoog' ten opzichte van de scoring door Malmberg toegekend op basis van de ROSA, waarbij Malmberg uitkomt op 'Midden'. Aangezien de huidige voorwaarden bij het ROSA certificeringssysteem nog niet zijn aangepast op de uitleg door de AP, zal deze selfassessment op 'Midden' in deze DPIA niet als een risico opgenomen worden.

  Het ROSA certificeringssysteem wordt momenteel doorontwikkeld waarbij het verwerken van cijfers/prestaties van leerlingen opnieuw wordt beoordeeld, en mogelijk in de toekomst de classificatie voor een onderwijsapplicatie van het niveau 'Midden' naar 'Hoog' wordt aangepast inzake de BIV-classificatie op Vertrouwelijkheid.

  SIVON adviseert om de volgende maatregelen toe te passen ter bevordering van een optimale beveiliging van persoonsgegevens, welke in lijn zijn met de classificatie 'Hoog' van de ROSA:

  - Dubbele encryptie van de database.
  - Uitgebreide loggingfunctionaliteit.

[19] BIV staat voor 'Beschikbaarheid, Integriteit en Vertrouwelijkheid. Deze drie categorieën 'B, I en V' worden op basis van de ROSA certificering ingedeeld in drie niveaus: 'laag', 'midden' of 'hoog'.
[20] Zie: https://www.autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia; Staatscourant 2019, nr. 64418, 27 november 2019, onderdeel 15. Profilering

Malmberg werkt met verschillende databases, waarbij er scheiding is van diverse verwerkingen. De identificerende gegevens zijn gescheiden van de databases, welke alle encrypted zijn op 1 laag. Hierdoor is het risico op ernstige incidenten al aanzienlijk beperkt.

- Autorisaties zijn instelbaar op een '*need to know'*, zodanig dat alleen de docent toegang heeft tot de gegevens van zijn klas/leerlingen.
- Malmberg conformeert zich aan de ISO 27001 normering. Hiervan is echter geen certificering beschikbaar voor MAX. Dit wordt als een risico gezien, wat door een aantoonbare jaarlijkse onafhankelijke toetsing kan worden gemitigeerd.
- Jaarlijks wordt de omgeving van MAX aan een security/pentest onderworpen door een externe partij, die hier een uitgebreide rapportage van uitbrengt. Ook worden maandelijks externe vulnerability scans uitgevoerd. De prioritering en opvolging is binnen Malmberg in een procedure vastgelegd en door SIVON als adequaat beoordeeld.
- Malmberg heeft een adequaat back-up beleid. Het back-up beleid voldoet aan alle vereisten zoals benoemd in het ROSA model.
- Malmberg past voor MAX logging toe, die (uitsluitend) door de onderwijsinstelling is op te vragen via de servicedesk van Malmberg. Het Normenkader IBP schrijft voor dat de onderwijsinstelling de logging zelfstandig moet kunnen monitoren. Daarnaast gaat ook de ISO 27001-norm ervan uit dat de verwerkingsverantwoordelijke zelf verantwoordelijk is voor de monitoring van loggegevens. Het is daarom van belang om functionaliteit te implementeren die het mogelijk maakt voor de onderwijsinstellingen om zelf over de loggegevens beschikken.
- De exportfunctionaliteit binnen MAX is *by default* voor gebruikers beschikbaar, daar zitten geen beperkingen op. Ook heeft de onderwijsinstelling zelf geen loginformatie over het gebruik van deze exportfunctionaliteit. Hierdoor ontbreekt inzicht in welke gebruiker, welke exports heeft uitgevoerd en is er geen monitoring op afwijkend gedrag met betrekking tot deze functionaliteit. Het is daarom in lijn met de vereisten van Privacy by Default uit de AVG, om tenminste de logging van de exports uit te breiden.
- Op één onderdeel binnen MAX wordt nog gebruik gemaakt van een verouderde hashing methode. Deze wordt vervangen door Malmberg.
- Docenten kunnen via een chatfunctie intern berichten sturen naar de helpdesk van Malmberg. Dit is geen externe mailfunctionaliteit en bevat derhalve geen risico's voor het onderzochte in deze DPIA.
- Binnen MAX wordt gebruik gemaakt van YouTube video's. Dit houdt een risico in omdat er dan via MAX persoonsgegevens gedeeld worden met Google. Voor scholen die de Google additionele services uit hebben staan, betekent dit dat via MAX toch, zij het beperkt, gegevens worden uitgewisseld met Google.

- MAX maakt in slechts beperkte mate gebruik van (deels gemaskeerde) metadata, die voor functionele toepassingen worden gebruikt en die afdoende zijn beschreven in de verwerkersovereenkomst.

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

Organisatorische maatregelen

Binnen Malmberg/Sanoma wordt organisatiebreed gebruik gemaakt van gedocumenteerde beveiligings- en incidentprotocollen en is een register van verwerkingen geïmplementeerd wat in OneTrust wordt bijgehouden.

IAMA: mensenrechten in beeld bij algoritmes

Er wordt volgens opgave van Malmberg binnen MAX geen gebruik gemaakt van geavanceerde algoritmes of AI technologie. Zie hiervoor de analyse in hoofdstuk 3.

Hierdoor is er geen sprake van een AI-systeem[21] met een hoog risico dat wordt gebruikt voor het bepalen van toegang of toelating, noch het 'evalueren van leerresultaten', het beoordelen van het passende onderwijsniveau, dan wel het monitoren of detecteren van ongeoorloofd gedrag.

Op basis van deze conclusie is het uitvoeren van een Impact Assessment Mensenrechten en Algoritmes (IAMA) geen verplichting.

10. Juridisch en beleidsmatig kader

Onderstaande tabel geeft vorm aan de juridische en beleidsmatige fundamenten ten aanzien van het gebruik van MAX binnen het onderwijs. De hieruit voortkomende verwerking van persoonsgegevens is inherent aan het doel van de verwerking, namelijk het aanbieden van digitale leer- en toetsapplicatie.

Het Normenkader[24] wordt op termijn een verplichting voor schoolbesturen om aan te voldoen. De relevante waarborgen die MAX raken zijn daarom ook opgenomen in dit overzicht.

Tabel 10.1 Juridisch en beleidsmatig kader

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
Leermiddelen (inzet van) t.b.v. onderwijsevaluatie en leerlingbegeleiding	Algemeen belang o.b.v. onderwijswetgeving. Wet op het Voorgezet onderwijs (WVO 2020)	2.89 WVO 2020 2.91 sub a WVO 2020 en *8.17 lid 10 WVO 2020*

[21] Zie Bijlage III bij de AI-Verordening: een uitwerking van de in artikel 6 lid 2 van de AI-Verordening bedoelde AI-Systemen met een hoog risico.

Digitaal afnemen van toetsen t.b.v. onderwijsevaluatie	Algemeen belang o.b.v. onderwijswetgeving. Wet op het Voortgezet onderwijs (WVO 2020)	2.89 WVO 2020 2.91 sub a WVO 2020 en *8.17 lid 10 WVO 2020*
Inzet van leermiddelen en het digitaal afnemen van toetsen via een externe leverancier (als ketenpartner) t.b.v. onderwijsevaluatie	Normenkader IBP	Domein 15, Ketenbeheer

11. Bewaartermijnen

De verwerkte persoonsgegevens binnen MAX worden na verloop van tijd gewist. In de tabel hieronder zijn de bewaartermijnen weergegeven.

Tabel 11.1 Bewaartermijnen

Gegevensverwerking	Bewaartermijn	Motivatie bewaartermijn
Onderwijsevaluatie	2 jaar na laatste geslaagde inlogpoging	Conform landelijk vastgestelde sectoraal beleid
Leerlingbegeleiding	2 jaar na laatste geslaagde inlogpoging	Conform landelijk vastgestelde sectoraal beleid
Ict-ondersteuning/ Informatiebeveiliging en privacy	Logging inlogactiviteit, wijzigingen en inzien: 13 maanden	Conform vereisten ROSA-certificeringsschema
Ict-ondersteuning/ Informatiebeveiliging en privacy	Back-up: 1 jaar	Conform vereisten ROSA-certificeringsschema

Het verwijderen van de persoonsgegevens binnen MAX die verband houden van lesuitvoering en toetsafnames worden door de verwerker verwijderd twee (2) jaar na de laatste geslaagde inlogpoging, conform het landelijk vastgestelde sectoraal beleid[22].

Deze bewaartermijnen zijn ‘hard’ in het systeem ingevoerd en kunnen niet worden aangepast door de school zelf. De onderwijsinstelling kan zelf wel aan de servicedesk van Malmberg aangeven dat er persoonsgegevens geschoond moeten worden.

1. Onderwijs	Onderwijsuitvoering	Lesuitvoering	Gemaakt en ingeleverd huiswerk, ingevuld digitaal les- en leermateriaal	2 jaar	Na einde schooljaar
1. Onderwijs	Onderwijsuitvoering	Toetsafname	Gemaakt schoolwerk, toetsen, opdrachten	Zodra niet meer relevant, maar uiterlijk 2 jaar na uitschrijving leerling	Na uitschrijving van de leerling

[22] https://aanpakibp.kennisnet.nl/bewaartermijnen/

In de handreiking bewaartermijnen van Kennisnet[23] worden op de persoonsgegevens die binnen MAX worden verwerkt dezelfde bewaartermijnen aangegeven, waardoor ook hieraan voldaan wordt:

6. Digitaal leermateriaal	Persoonsgegevens: niet langer bewaren dan noodzakelijk	Po Onderbouw vo	Gegevens huidige schooljaar, plus gegevens voorgaande schooljaar bewaren
		Bovenbouw vo	Gegevens huidige schooljaar, plus de twee voorgaande schooljaren bewaren

NB: SIVON adviseert hierbij *aan de onderwijsinstellingen* om de cijfers op te nemen in het LAS en niet verder langdurig te verwerken in de leeromgeving, zoals die van MAX. Dit betekent dat de bewaartermijn beperkt kan worden tot het (jaarlijkse) moment waarop de relevante leerresultaten in het LAS zijn opgenomen. Hierdoor wordt het risico voor de rechten en vrijheden van betrokkenen, doordat mogelijk iemand onbevoegd toegang krijgt tot deze gegevens, verder geminimaliseerd. Voor de (kortere) bewaartermijnen in MAX kan dit worden gerealiseerd door een verzoek om schoning van de betreffende persoonsgegevens in te dienen bij de servicedesk van Malmberg.

[23] Zie Kennisnet: Tijdelijke handreiking bewaartermijnen po/vo 1.2 (december 2020).

6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen

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

12. Rechtsgrond

Artikel 6 van de AVG geeft een zestal verwerkingsgrondslagen die het verwerken van persoonsgegevens kunnen rechtvaardigen:

a) Toestemming van de betrokkene (art.6. eerste lid, sub a, AVG)
b) Uitvoering van een overeenkomst (art.6, eerste lid, sub b, AVG)
c) Wettelijke verplichting[24] (art.6, eerste lid, sub c, AVG)
d) Vitaal belang van de betrokkene (art.6, eerste lid, sub d, AVG)
e) Taak van algemeen belang[25] (of openbaar gezag) (art.6, eerste lid, sub e, AVG)
f) Gerechtvaardigd belang (art. 6. eerste lid, sub f, AVG)

Schoolbesturen maken in de uitoefening van de onderwijstaken zoals in deze DPIA beschreven gebruik van de bij formele wet voorgeschreven Wet op het voortgezet onderwijs (WVO 2020). Hierdoor kunnen schoolbesturen de verwerkingen baseren op artikel 6, eerste lid onder e van de AVG. De verwerkingen zijn noodzakelijk voor de vervulling van een taak van algemeen belang welke aan de verwerkingsverantwoordelijke is opgedragen. Namelijk het uitvoeren van onderwijstaken.

Deze verwerkingsgrondslag is niet uitsluitend bedoeld voor overheidsinstellingen en bestuursorganen, maar kan ook worden gebruikt door organisaties die persoonsgegevens verwerken ten behoeve van een publieke taak. De AVG eist dat de rechtsgronden voor het verwerken van persoonsgegevens bij lidstatelijk recht zijn vastgelegd. Met andere woorden, de door de Nederlandse overheid opgelegde taak waarvoor het verwerken van persoonsgegevens onvermijdelijk is, moet specifiek zijn vastgelegd in een wet. De verwerkingsverantwoordelijke (de onderwijsinstelling) is als zodanig in de WVO 2020 aangewezen om deze taak uit te voeren.

[24] De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn.
[25] Met betrekking tot rechtsgrond taak van algemeen belang geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak persoonsgegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak ook worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

AVG

Artikel 6
Lid 1: De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:
Sub e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Wet voortgezet onderwijs 2020

In de sectorspecifieke wetgeving die op de schoolbesturen van toepassing is bij het uitvoeren van de processen die in deze DPIA centraal staan, zijn de hoofdlijnen van de hierbij gepaard gaande verwerkingen van persoonsgegevens voldoende kenbaar. Zo behoort het tot de verantwoordelijkheid van de school om er voor zorg te dragen dat de leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen.[26]

Het staat het schoolbestuur vrij welke (leer)middelen zij daarvoor inzet, deze kunnen zowel digitaal, fysiek als hybride zijn. Uit Artikel 8.17 lid 10 Gebruik persoonsgebonden nummer door bevoegd gezag, WVO 2020 volgt impliciet dat een onderwijsinstelling in het kader van haar taken digitale leermiddelen mag inzetten.

De AVG schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. Er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen voor de vervulling van een taak van algemeen belang. De relevante wetgeving in de WVO 2020 sluit aan op de verwerkingen die plaatsvinden binnen MAX omdat dit een digitaal leermiddel en toetssysteem betreft, dat de noodzakelijke ondersteuning biedt voor de uitvoering van leertaken.

Artikel 2.89 van de WVO 2020 *'Onderwijskundig beleid'* biedt daarmee een solide basis voor de gegevensverwerkingen die binnen het gebruik van MAX plaatsvinden. De gegevensverwerkingen zijn op basis van de genoemde wetgeving dan ook rechtmatig. Hierbij moet bedacht worden dat de uitvoering van de wettelijke taken het doel is, terwijl de inzet van de applicatie MAX een 'middel' is.

Wet op het voortgezet onderwijs 2020

Artikel 2.91 sub a WVO 2020

Schoolplan: Stelsel van kwaliteitszorg

Sub a. *Het bewaken dat leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen en dat het onderwijs wordt afgestemd op de voortgang in de ontwikkeling van leerlingen, bedoeld in artikel 1.4 lid 2.*

Sub b. Het vaststellen van welke maatregelen ter verbetering nodig zijn.

Artikel 8.17 lid 10 WVO 2020

[26] Zie artikel 1.4 lid 2 WVO 2020: *Het onderwijs wordt zodanig ingericht dat de leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen. Het wordt afgestemd op de voortgang in de ontwikkeling van de leerlingen.*

Het bevoegd gezag kan het pseudoniem gebruiken voor het genereren van een ander pseudoniem voor een leerling in het kader van de toegang tot en het gebruik van digitale leermiddelen of het digitaal afnemen van toetsen en examens, waarbij het bevoegd gezag er zorg voor draagt dat dit andere pseudoniem wordt bewaard in de systemen waarin de leerlingen zijn geregistreerd. Dit andere pseudoniem wordt uitsluitend verstrekt aan een leverancier die een digitaal product of een digitale dienst aanbiedt bestaande uit leerstof of toetsen en de daarmee samenhangende digitale diensten.

Er is dus een grondslag '*algemeen belang o.b.v. onderwijswetgeving'* om digitale leermiddelen in te zetten. Deze kan gevonden worden in artikel 6, eerste lid, sub e, van de AVG jo artikel 8.17 lid 10 WVO 2020.

De conclusie is dat de verwerking van persoonsgegevens bij het inzetten van de leermethode MAX kan plaatsvinden op grond van artikel 6 lid 1 sub e AVG (*algemeen belang, o.b.v. onderwijswetgeving*, zoals in deze paragraaf beschreven).

Tabel 12.1 Rechtsgrond

Verwerking/doeleinde	Grondslag AVG	Toelichting
De opslag van leer- en toetsresultaten. Het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten. De beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer. Analyse en interpretatie van leer- en toetsresultaten. Het geleverd krijgen/ in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier. Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8.17 lid 10 WVO 2020. Taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leermethode zoals MAX is toegestaan op grond van artikel 6 lid 1 sub e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).

identificatie, authenticatie en autorisatie. De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens. De continuïteit, verbetering en goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning. Het beschikbaar stellen van gegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan digitale onderwijsmiddelen.		

13. Bijzondere persoonsgegevens

In het kader van de verwerking van persoonsgegevens via MAX worden er geen bijzondere of strafrechtelijke persoonsgegevens verwerkt.

In het kader van deze DPIA wordt gewezen op het risico van open tekstvelden. In MAX kan de leerkracht in een open tekstveld feedback aan de leerling geven op de gemaakte opdracht. Ook kan een leerkracht via de chat-functie (open tekstveld) feedback aan Malmberg geven over de applicatie. Het vraagt om een gedragsregel vanuit de onderwijsinstelling om de medewerker van de onderwijsinstelling erop te wijzen dat in deze tekstvelden geen gevoelige en/of bijzondere persoonsgegevens mogen worden verwerkt.

In het kader van gepersonaliseerde instellingen kan de onderwijsdeelnemer (leerling) in MAX eigen instellingen doorvoeren, die het leren en zich eigen maken van de doelstellingen vergemakkelijken. Zo beschikt MAX bijvoorbeeld over een leeslineaal waarbij de tekst ‘geschaduwd’ wordt. Tevens kunnen teksten voorgelezen worden en kunnen tekstdelen in

een apart tekstvak worden geplaatst, waarbij voorkeuren kunnen worden ingesteld, zoals kleur van de tekst, grootte en lettertype ('fonts'). Eén van de mogelijkheden is het kiezen van het lettertype 'Open Dyslexic'. Dit is echter alleen de naam van een font, en betekent niet dat indien een leerling voor dit type kiest, dat MAX persoonsgegevens verwerkt als zijnde bijzondere persoonsgegevens. De instellingen blijven opgeslagen, zodat deze manier van gepersonaliseerde instellingen behouden blijven. Dit dient het gebruiksgemak.

14. Doelbinding

In het kader van de verwerking van persoonsgegevens via MAX worden er geen persoonsgegevens verwerkt voor een ander doel dan waarvoor deze oorspronkelijk zijn verzameld.

15. Kinderrechten-afweging (Best Interests Assessment Children)

Artikel 3 van het Verdrag inzake de rechten van het kind, schrijft voor dat bij alle maatregelen betreffende kinderen - ongeacht of deze worden genomen door openbare of particuliere instellingen, rechterlijke instanties, bestuurlijke autoriteiten of wetgevende lichamen - de belangen van het kind de eerste overweging (moeten) vormen. Deze belangenafweging gaat verder dan een veilige gegevensverwerking maar ziet ook op de mogelijke gevolgen van de verwerking. Met schoolbesturen als leden van SIVON in het primair en voortgezet onderwijs, betekent dit dat SIVON in haar DPIA's rekening houdt met o.a. gebruikers (betrokkenen) in de leeftijd van 4 tot 18 jaar (of ouder). Kinderen hebben recht op specifieke bescherming van hun persoonsgegevens. Dit volgt uit het feit dat zij zich minder bewust zijn van de risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van hun persoonsgegevens. SIVON geeft hier in deze DPIA invulling aan door af te wegen of het gebruik van MAX en/of de gegevensverwerking(en) die daarmee samenhangen, in het belang zijn van de betrokkenen (kind/leerling als betrokkene). SIVON maakt hierbij gebruik van de systematiek van de best interests assessment children van de Britse ICO[27]. De afweging bestaat uit 4 stappen:

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

Hieronder wordt beschreven welke rechten[28] van en voor kinderen relevant zijn in het kader van deze DPIA. Van belang is de leeftijd van de kinderen (leeftijdsadequaat). Hierbij wordt nagegaan of de gegevensverwerking (negatieve) gevolgen heeft voor de ondersteuning en van de behoeften van het kind op het gebied van veiligheid, gezondheid, welzijn, familierelaties, fysieke, psychologische en emotionele ontwikkeling, identiteit, vrijwaring

[27] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/best-interests-self-assessment/
[28] https://wetten.overheid.nl/BWBV0002508/2002-11-18#Verdrag_2

van economische commerciële en/of fysieke uitbuiting, vrijheid van meningsuiting, privacy en de mogelijkheid om een eigen mening te vormen en deze te laten horen, het belang van toegang tot informatie, omgang met anderen en spel (buiten spelen) om de ontwikkeling van het kind te ondersteunen. Het gaat erom dat het kind in overeenstemming met zijn of haar ontwikkelende capaciteiten, een stem heeft (kan hebben) in zaken die hem of haar aangaan.

MAX wordt gebruikt door kinderen en jongvolwassenen. Ten gevolge hiervan wordt overwogen of het gebruik van de applicatie leeftijdsadequaat is en past bij de leeftijd van de leerlingen. De leeftijdscategorie en de verschillende behoeften van kinderen van verschillende leeftijden en ontwikkelingsstadia moeten centraal staan bij het ontwerpen van MAX en de daarmee samenhangende gegevensverwerkingen. Dit wordt hieronder verder afgewogen.

2. Identificatie het effect van de gegevensverwerking en gebruik van MAX op deze rechten

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

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

De toepassing van MAX lijkt geen (negatieve) gevolgen te hebben voor de ondersteuning en van de behoeften van het kind op het gebied van veiligheid, gezondheid, welzijn, familierelaties, fysieke, psychologische en emotionele ontwikkeling, identiteit, vrijwaring van economische commerciële en/of fysieke uitbuiting, vrijheid van meningsuiting, privacy en de mogelijkheid om een eigen mening te vormen en deze te laten horen, het belang van toegang tot informatie, omgang met anderen en spel (buiten spelen) om de ontwikkeling van het kind te ondersteunen.

Reden hiervoor is dat MAX als oefen- en toetsplatform wordt toegepast op een ‘vak’, bijvoorbeeld Biologie, of Natuurkunde dat op de leeftijd en leerbehoeften van de leerling is afgestemd. MAX geeft hierbij juist mede invulling aan artikel 28 van het Verdrag, namelijk het recht van het kind op onderwijs, teneinde gelijke kansen te creëren.

De MAX beschikt wel over een zogenaamde ‘*inkijkfunctie*’. Deze functie betreft een functie om vanuit de docentrol te kijken wat een leerling precies heeft gedaan om een vraag op te lossen. Het is een manier om het door de leerling gemaakte werk te kunnen bekijken. Dit betreft een voor onderwijskundige doeleinden belangrijke functie. De docent kan hiermee

bijvoorbeeld inzicht krijgen in hoe de leerling tot een antwoord komt. Hiervoor is binnen MAX in het geval van open vragen een veld beschikbaar waarin de leerling uitschrijft hoe deze tot een conclusie komt. Door inzage in dit veld kan de docent de leerling helpen tot verbeterde inzichten te komen. Het betreft geen meekijkfunctie in de zin van het 'live' meekijken of een andersoortige 'proctoring' functie. De conclusie is dat deze inkijkfunctie geen inbreuk maakt op wezenlijke rechten van het kind. Deze digitale inkijkfunctie verschilt niet van bijvoorbeeld het in een schrift bekijken hoe de leerling tot een bepaalde conclusie komt. Het is hierdoor niet noodzakelijk de leerling er via een 'privacyverklaring' op te wijzen dat het werk kan worden ingezien: er wordt niet 'live' meegekeken worden.

3. Beoordeling of dit effect wenselijk is

Zoals onder punt 2 vermeld, lijken er geen negatieve gevolgen te zijn voor het gebruik van MAX. MAX wordt altijd ingezet via het onderwijskundige proces van de onderwijsinstelling, waarbij de onderwijsinstelling bepaalt wie verantwoordelijk is en er dus geen sprake is van willekeurigheid of onrechtmatigheid.

De mogelijkheden binnen MAX om gepersonaliseerde instellingen toe te passen en het eenvoudige algoritme dat makkelijker, dan wel moeilijker vragen voorstelt en aldus inspeelt op de individuele leerbehoefte van de leerling lijkt alleszins in het voordeel van de leerling.

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

Er is geen noodzaak om aanvullende maatregelen te nemen om de rechten van het kind te beschermen. De effecten die de gegevensverwerkingen binnen MAX hebben op de kinderrechten zijn over een brede linie tegen het licht gehouden en lijken hier niet een niet te rechtvaardigen inbreuk op te maken.

16 a. Noodzakelijkheid

Verwerking van persoonsgegevens met behulp van digitale onderwijsmiddelen door onderwijsinstellingen vindt plaats ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces) en het begeleiden en volgen van onderwijsdeelnemers (in hun leerproces).

Uit de analyse van de gegevensverwerking, zie deel A: de gegevensverwerkingsanalyse, blijkt dat de door MAX te verwerken persoonsgegevens noodzakelijk zijn in relatie tot het doel van de gegevensverwerking, te weten het via het inzetten van leermiddelen en toetsapplicatie kunnen waarborgen van een ononderbroken ontwikkelingsproces voor de leerling.

De verwerkingen door de onderwijsinstelling via MAX vinden plaats om door middel van digitale les- en oefenopdrachten de vaardigheden van leerlingen in verschillende vakken te oefenen, verbeteren en begeleiden. Het afleggen van (digitale) toetsen is daarnaast noodzakelijk in het kader van goed onderwijs en het beoordelen van de prestatie van leerlingen.

De opsomming van verwerkingen en soorten persoonsgegevens zijn hierbij noodzakelijk om het leerplatform op de gewenste manier te kunnen gebruiken.

16. b. Proportionaliteit en subsidiariteit

De onderwijsinstelling is verantwoordelijk voor de uitvoering van goed onderwijs volgens de bepalingen van de Wet op het voortgezet onderwijs 2020. Hierbij staat de inbreuk op de persoonlijke levenssfeer in evenredige verhouding tot de verwerkingsdoelen, namelijk het waarborgen van een ononderbroken ontwikkelingsproces met behulp van (digitale) leermiddelen. Vanwege het feit dat via een autorisatiebeheer alleen medewerkers van de onderwijsinstelling (en de leverancier) op een '*need to know*' basis bij de gegevens van leerlingen van hun groep kunnen, is de 'inbreuk' beperkt tot professionals die leerlingen ondersteunen in hun ontwikkelingsproces. De minimale gegevens zijn noodzakelijk om de vakken en toetsen binnen MAX aan leerlingen aan te kunnen bieden.

Het gebruik van potlood/papier is een alternatief, maar deze optie is niet per definitie makkelijker en veiliger. Het gebruik van een digitaal leerplatform is niet meer belastend om hetzelfde doel te behalen.

17. Rechten van de betrokkenen

'Art. 15, lid 1, van de AVG beschrijft dat iedere betrokkene het recht heeft om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens.'

De onderwijsinstelling die gebruik maakt van MAX dient op haar website een duidelijke privacyverklaring en een privacyreglement opgenomen te hebben. Hierin staat beschreven welke rechten betrokkenen hebben betreffende de verwerking van hun Persoonsgegevens en hoe men hun rechten kan uitoefenen.

Malmberg ondersteunt de onderwijsinstelling bij het voldoen aan de verplichtingen van de verwerkingsverantwoordelijke om te voldoen aan de rechten van betrokkenen[29]. Verzoeken van de onderwijsinstelling worden via privacy@malmberg.nl in behandeling genomen. Daar wordt geverifieerd of de vragende instelling een accounthouder is bij Malmberg. Indien dit het geval is en de verwerkingsverantwoordelijke is geverifieerd worden persoonsgegevens verstrekt.

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

[29] Zie Hoofdstuk III van de AVG 'Rechten van de betrokkene', artikel 12 – 23 AVG.

Tabel 17.1: rechten van betrokkenen

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking*
Het recht op informatie	De onderwijsinstelling dient als verwerkingsverantwoordelijke te zorgen voor een: • Openbaar gepubliceerde privacyverklaring op de website.	n.v.t.
Het recht van inzage	Malmberg kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht op rectificatie	Malmberg kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht op gegevenswissing	Malmberg kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht op beperking van de verwerking	Malmberg kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	Malmberg kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht op overdraagbaarheid van gegevens	Malmberg kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht van bezwaar	Malmberg kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit	Dit is niet aan de orde. De onderwijsinstelling neemt de uitkomsten van de leer- en toetsresultaten mee in de eigen beoordeling van de leerling.	n.v.t.

18. Beoordeling verwerkersovereenkomst

Voor leveranciers die deelnemer (of medestander) zijn van het Convenant digitale onderwijsmiddelen en privacy 4.0 (ook wel: Privacyconvenant Onderwijs, hierna: Convenant) of de opvolger daarvan, zijnde het keurmerk Edu-V, en gebruik maken van het daarbij horende model verwerkersovereenkomst, vindt een toetsing plaats welke wordt afgezet tegen de vereisten van het convenant/Edu-V. Dit wordt de theoretische toets genoemd. Aanvullend hierop vindt ook, mede aan de hand van de inzichten die deze DPIA heeft gebracht, een praktische toets plaats. Hierbij is een vergelijk gemaakt tussen de in de

theorie genoemde afspraken en de verwerkingen die in de praktijk plaatsvinden. De hiervoor gebruikte toetsingskaders zijn via https://sivon.nl/toetsen-verwerkersovereenkomsten-2/ terug te vinden.

Na de bespreking van het Toetsformulier en het doorvoeren van verbeteringen en/of het maken van eventuele afspraken, wordt uiteindelijk een verwerkersovereenkomst Toetsrapport met de bevindingen opgeleverd die via de Dienst Verwerkersovereenkomsten (van Kennisnet) of op de website van de leverancier ontsloten voor schoolbesturen.

Tabel 18.1 Bevindingen toets verwerkersovereenkomst

Toets - Verwerkersovereenkomst	**Opgenomen (volledig en juist)?**	**Vragen of opmerkingen**
Verwerkersovereenkomst conform Edu-V Model verwerkersovereenkomst 4.1	Nee, want	Hoewel wel Edu-V model verwerkersovereenkomst 4.1 is gebruikt, staat in de koptekst en in de ondertitel een verwijzing naar het Privacyconvenant en dat klopt niet. Ook in de bijlagen klopt de koptekst niet. Het Privacyconvenant kent geen model 4.1.
Naam/Versie/Datum aangeboden verwerkersovereenkomst	Ja, want	Versiedatum ontbreekt. Versienummer is gelijk aan versie van Edu-V Model verwerkersovereenkomst. Dat kan, maar kan ook verwarrend zijn, zeker wanneer Leverancier tussen 2 versies van Edu-V aanpassingen zou doen.
Overwegen het volgende: verwijzing onderliggende overeenkomst (naam en datum) en benoeming product/dienst	Ja, want	De tekst 'op <datum>' zou mogen vervallen omdat de onderliggende overeenkomst mogelijk/waarschijnlijk niet per schoolbestuur maar per school wordt ondertekend.
Verschillen geconstateerd tov Edu-V Model verwerkersovereenkomst 4.1?	Ja, want	Er zijn bij 'Partijen', 'Overwegen het volgende' en in de 'Artikelen' geen verschillen geconstateerd.
Zo ja, opgenomen in Bijlage 3: Wijzigingenbijlage	Nee, maar	Verplichte Bijlage 3 ontbreekt. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
Toets - Bijlage 1: Privacybijsluiter	**Opgenomen (volledig en juist)?**	**Vragen of opmerkingen**

A. Contactgegevens Verwerker en Onderwijsinstelling		Gebruiken Model MEVW voor bijlagen.
• Functie contactpersonen	Ja, maar	De functie van de contactpersoon is niet opgenomen. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
• Contactgegevens (e-mailadres, telefoonnummer)	Nee, maar	Er is geen ruimte voor Onderwijsinstellingen om contactgegevens op te nemen. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
Het meest recente versienummer van de Privacybijsluiter en de datum daarvan worden hier vastgelegd.	Nee, maar	Nieuwe datum is opgenomen. Versienummer ontbreekt. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
• Naam Verwerker en vestigingsgegevens	Nee, maar	Volledige vestigingsgegevens ontbreken. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
• Link naar Leverancier (website/URL)	Nee, maar	Er is geen link opgenomen naar de webpagina van de leverancier. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
• Link naar productpagina (website/URL)	Ja, want	Link naar productpagina's is netjes opgenomen.
a. omschrijving van producten en/of diensten en bijbehorende Verwerkingen die een onlosmakelijk onderdeel vormen van het aangeboden product en/of de aangeboden dienst, inclusief de koppelingen en uitwisseling met derde partijen;	Nee, maar	Er wordt geen onderscheid gemaakt tussen onlosmakelijk verbonden producten/diensten en optionele, en er wordt ook geen melding gemaakt van koppelingen. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
b. omschrijving van aanvullende optionele producten en/of diensten en bijbehorende Verwerkingen die de Verwerker	Nee, maar	Er wordt geen onderscheid gemaakt tussen

aanbiedt, inclusief de koppelingen en uitwisseling met derde partijen.		onlosmakelijk verbonden producten/diensten en optionele, en er wordt ook geen melding gemaakt van koppelingen. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
In dit onderdeel wordt vastgelegd welke doeleinden, zoals vastgelegd in artikel 5 van het Convenant, van toepassing zijn op de Verwerking van Persoonsgegevens met behulp van de specifieke producten en/of diensten.	Ja, want	Doeleinden zijn in overeenstemming gebracht met doeleinden Privacy Convenant. Juiste Doeleinden zijn van toepassing.
1. een omschrijving van de categorieën Betrokkenen (o.a. Onderwijsdeelnemers, ouders/verzorgers, medewerkers) over wie Persoonsgegevens worden verwerkt, en de te verwerken categorieën Persoonsgegevens van deze Betrokkenen, en	Nee, maar	Betrokkene-categorieën worden niet vermeld. Sessie-informatie staat bij optioneel verwerkte persoonsgegevens, terwijl deze verplicht zijn om vast te leggen (bij gebruik) i.h.k.v ROSA-certificeringsschema. Vermelding van licentie-/activeringscode ontbreekt als Persoonsgegeven. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
2. door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen).	Nee, maar	Suggesties voor de bewaartermijnen vanuit de Leverancier zijn opgenomen. Het is echter niet duidelijk hoe de Onderwijsinstelling hiervan af kan wijken. Het is ook niet helemaal duidelijk welke bewaartermijn er geldt bij einde contract. En de bewaartermijn van logging (wijziging en inzien persoonsgegevens) dient conform ROSA-certificeringsschema 13 maanden te zijn. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
Onder G. wordt vastgelegd wat de plaats(en)/land(en) van opslag en Verwerking van de Persoonsgegevens zijn.	Nee, maar	Aangezien er Subverwerkers zijn waarbij Vestigingsplaats Holding (Moedermaatschappij)

		buiten de EER is gevestigd en meer specifiek de VS en daardoor toch sprake kan zijn van verwerking buiten de EER dient dit duidelijker vermeld te worden. Er zijn wel extra waarborgen getroffen in de vorm van SCC's voor 2 Subverwerkers. Het is onduidelijk of Salesforce ook een Subverwerker is, aangezien deze wel in 'Malmberg External Integrations' genoemd wordt. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
Verwerker legt hier vast van welke Subverwerkers hij ten tijde van het afsluiten van de Verwerkersovereenkomst gebruikmaakt.	Nee, maar	Het is onduidelijk welke persoonsgegevens door welke Subverwerker worden verwerkt. Er is een nette opmerking opgenomen over de inzet van YouTube voor filmpjes. Onderwijsinstelling kan hier rekening mee houden. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
Toets - Bijlage 2: Beveiligingsbijlage	**Opgenomen (volledig en juist)?**	**Vragen of opmerkingen**
Het meest recente versienummer van deze bijlage en de datum daarvan worden hier vastgelegd.	Nee, maar	Nieuwe datum is opgenomen. Versienummer ontbreekt. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
Inlogpagina	Ja, want	Vermelding van de inlogpagina's ontbreekt. Voor VO zou dat moeten zijn: inloggenvo.malmberg.nl. Voor MBO: startmalmbergmbo.nl.
Beschikbaarheid (alleen opnemen, indien niet voldaan of bij vragen/opmerkingen over de uitleg)	Ja, want	Maatregel 'Herstel' wordt niet aan voldaan. > Leverancier geeft transparant aan dat alleen het onderdeel recovery test

		niet 2x per jaar wordt uitgevoerd.
Integriteit (alleen opnemen, indien niet voldaan of bij vragen/opmerkingen over de uitleg)	Ja	Alles voldaan.
Vertrouwelijkheid (alleen opnemen, indien niet voldaan of bij vragen/opmerkingen over de uitleg)	Nee, maar	Maatregel 'Transport en fysieke opslag' wordt niet aan voldaan. > Leverancier verwacht dat hieraan wordt voldaan eind 2025.
Verwerker (naam, functie, e-mail en telefoonnummer)	Nee, maar	Telefoonnummer ontbreekt. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
Onderwijsinstelling (naam, functie, e-mail en telefoonnummer)	Nee, maar	Er is geen ruimte voor Onderwijsinstellingen om contactgegevens op te nemen. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.
Toets - Bijlage 3: Wijzigingenbijlage	**Opgenomen (volledig en juist)?**	**Vragen of opmerkingen**
Het meest recente versienummer van deze bijlage en de datum daarvan worden hier vastgelegd.	Nee, maar	Verplichte bijlage 3 ontbreekt. > Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de reguliere bijlagen.

Malmberg wijkt af van sommige toetsingscriteria omdat zij de goedgekeurde bijlagen van het branchemodel van de MEVW gebruiken. Ze zijn in afwachting van het nieuwe model verwerkersovereenkomst.

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

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

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

Beoordelingskader risico's

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

De methodiek die wordt gevolgd, is beschreven door de Britse toezichthouder[30] om risico's te classificeren. Hierbij wordt een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade).

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

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

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

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

1. risico's identificeren;
2. risico's inschatten/analyseren;

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

3. risico’s beoordelen/evalueren.

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

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

Zie bijlage 2 voor nadere uitleg over de risico’s.

19. Risico’s

In onderstaande risicotabel worden de risico’s beschreven. Per risico worden de mogelijke oorzaken en gevolgen aangegeven met daarbij de kans dat het zich voordoet en de impact. Tevens is aangegeven of het risico betrekking heeft op een proces waarbij MAX wordt ingezet of dat het risico het systeem zelf betreft (de applicatie). Hierbij wordt ook gebruik gemaakt van de MAPGOOD-methode.

Toelichting MAPGOOD-methode

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

- **M**ens – de mensen die nodig zijn om het informatiesysteem te beheren en gebruiken, denk aan: directe en indirecte gebruikers, en functioneel en technisch applicatiebeheer.
- **A**pparatuur – de apparatuur die nodig is om het informatiesysteem te laten functioneren, denk aan: webserver, applicatieserver, beheer van werkplekken en werkplekken van gebruikers.
- **P**rogrammatuur – de programmatuur waaruit het informatiesysteem bestaat, denk aan: de diverse applicaties die gebruikt worden.
- **G**egevens – de gegevens die door het systeem worden verwerkt, denk aan: basisregistraties, financiële verantwoording en vergunningen.
- **O**rganisatie – de organisatie die nodig is om het informatiesysteem te laten functioneren, denk aan: beheer-, gebruikers- en ontwikkelorganisatie.
- **O**mgeving – de omgeving waarbinnen het informatiesysteem functioneert, denk aan: locatie, serverruimte en werkplekken.
- **D**iensten – de externe diensten die nodig zijn om het systeem te laten functioneren, denk aan: technisch systeembeheer, netwerkinfrastructuur en onderhoudscontracten met externe dienstverleners.

Tabel 19.1 Risico's

Risico nr.	Map-good	Risico-omschrijving	Oorzaak	Gevolg	Kans	Impact	Risico	Proces en/of systeem-risico+ verantwoordelijke
1	P O	Exportfunctionaliteit is standaard beschikbaar zonder beperkingen, waardoor onbedoeld persoonsgegevens kunnen worden geëxporteerd (geen '*privacy by design*'). Het risico is dat er door het gebruik van de export en/of download functie mogelijk (gevoelige) persoonsgegevens buiten de applicatie terecht komen wat verlies van controle over deze data tot gevolg heeft.	De beperking op downloads en exports is ontoereikend, deze kunnen leiden tot onrechtmatige verdere verwerkingen.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen	2	3	6	Systeem en proces Malmberg en onderwijsinstelling
2	P	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregelen toegepast.	De loggingfunctionaliteit is ontoereikend. In de logfiles is o.a. niet te zien wie exports/downloads heeft uitgevoerd.	Dit kan leiden tot een beperking van uitoefening van rechten en vrijheden van het individu en is een risico voor de rechten en vrijheden van betrokkenen	2	3	6	Systeem Malmberg
3	P	Er worden onvoldoende beveiligingsmaatregelen toegepast.	De logfiles van wijzigingen zijn niet door de onderwijsinstelling zelf in te zien.	Dit kan leiden tot een beperking van uitoefening van rechten en vrijheden van het individu en is een risico voor de rechten en vrijheden van betrokkenen	2	3	6	Systeem Malmberg

4	P D	Data-uitwisseling met subverwerker buiten de EU/EEA, omdat er gebruikt wordt gemaakt van YouTube - filmpjes. Geen grondslag voor verwerking, gebrek aan transparantie en er worden onvoldoende beveiligingsmaatregelen toegepast.	Niet juist geïmplementeerde instellingen, waardoor de YouTube filmpjes niet in de 'privacy enhanced'(no-cookie) modus worden gebruikt.	Dit kan leiden tot ongewenst evalueren van persoonlijke aspecten (profilering), mogelijk misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen	3	2	6	Systeem Malmberg
5	P	Er worden onvoldoende beveiligingsmaatregelen toegepast.	Er wordt (in beperkte mate) gebruik gemaakt van verouderde hashing-methode.	Dit kan leiden tot ongedaanmaking van versleuteling, misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen	3	3	9	Systeem Malmberg
6	O	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregelen toegepast	Er wordt geconformeerd aan de ISO27001 standaard, echter deze technische maatregelen dienen op effectiviteit te worden getoetst door een onafhankelijke partij en aantoonbaar te zijn.	Dit kan leiden tot verlies van vertrouwelijkheid, misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen	1	3	3	Proces Malmberg

7	O	Ontoereikende afspraken in de verwerkersovereenkomst over de verwerking van de persoonsgegevens.	Verwerkersovereenkomst wijkt af van de vereisten die het Privacyconvenant Onderwijs, de AVG en/of Edu-V daaraan stellen. Informatie is op punten onjuist of er ontbreekt informatie.	Onderwijsinstelling kan de rechten van betrokkenen niet waarborgen, meer specifiek het recht op informatie (AVG artikel 13 en 14). Verwerkingsverantwoordelijke kan verwerkingsregister niet naar volledigheid en juistheid vullen (AVG artikel 30 lid 1). Bij een inbreuk op persoonsgegevens (datalek) kunnen risico's en maatregelen niet goed beoordeeld en ingeschat worden (AVG artikel 33 lid 3, artikel 32 lid 2).	3	3	9	Proces Malmberg en onderwijsinstelling

8	O	Achterhaalde informatie in de verwerkersovereenkomst over de verwerking van de persoonsgegevens.	Informatie over bewaartermijn van logging is niet actueel (bewaartermijn van logging wijziging en inzien persoonsgegevens), de technische aanpassingen zijn gemaakt.	Verwerkingsverantwoordelijke kan de rechten van betrokkenen niet waarborgen, meer specifiek het recht op informatie (AVG artikel 13 en 14). Verwerkingsverantwoordelijke kan verwerkingsregister niet naar volledigheid en juistheid vullen (AVG artikel 30 lid 1). Bij een inbreuk op persoonsgegevens (datalek) kunnen risico's en maatregelen niet goed beoordeeld en ingeschat worden (AVG artikel 33 lid 3, artikel 32 lid 2).	2	3	6	Proces Malmberg

9	P	Er worden onvoldoende beveiligingsmaatregelen toegepast.	Aan de maatregel 'Transport en fysieke opslag' in het ROSA certificeringsschema wordt niet voldaan.	Onderwijsinstelling kan de rechten van betrokkenen niet waarborgen, meer specifiek het recht op informatie (AVG artikel 13 en 14). Verwerkingsverantwoordelijke kan verwerkingsregister niet naar volledigheid en juistheid vullen (AVG artikel 30 lid 1). Bij een inbreuk op persoonsgegevens (datalek) kunnen risico's en maatregelen niet goed beoordeeld en ingeschat worden (AVG artikel 33 lid 3, artikel 32 lid 2).	2	3	6	Systeem Malmberg
10	O	Gebrek aan transparantie	Informatievoorziening over adaptieve functionaliteit kan vragen oproepen bij betrokkenen vanwege summiere inhoudelijke informatie(web)teksten. Verwerkingsverantwoordelijke dient hierin te voorzien.	Dit kan leiden tot verkeerde verwachtingen bij gebruikers over de mate van personalisatie, profilering en dataverwerking	2	2	4	Proces Onderwijsinstelling

8. Deel D: Beschrijving voorgenomen maatregelen

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

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

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

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

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

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

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

- *Fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;*
- *Opslag van gegevens in een kluis;*
- *Project-, risico- en incidentenmanagement;*

- *Data opsplitsen;*
- *Dataminimalisatie;*
- *Back-ups;*
- *Integriteitscontroles;*
- *2FA/MFA;*
- *Monitoring en logging;*
- *Controle van toegekende bevoegdheden;*
- *Privacybewustzijn- en beveiligingstrainingen;*
- *Managementrapportages over risicobeheer;*
- *Beperken inzageniveau;*
- *Periodiek een audit of hack- of penetratietest uitvoeren;*
- *Richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;*
- *Resonsible-disclosurebeleid;*
- *Geheimhoudingsverklaringen;*
- *Service level agreements (met boeteclausules);*
- *Verwerkersovereenkomsten.*
- *Screening personeel en VOG-verklaring.*

20. Maatregelen

20.1 Maatregelentabel

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (Leverancier / school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum) maatregel geïmplementeerd?
1	Exportfunctionaliteit is standaard beschikbaar zonder beperkingen (exporteren/downloaden by default aan)	6	Exporteren/downloaden zichtbaar maken in logging (zie ook bij 2). (technisch) Onderwijsinstelling moet afspraken maken over het maken en gebruiken van exports en hier controle op uitoefenen. (organisatorisch)	Malmberg Onderwijsinstelling	2	Na implementatie wordt het risico verminderd, maar het kan niet geheel weggenomen worden.	Op de ontwikkelagenda geplaatst. Uiterste datum gereed eind december 2026.
2	Er worden onvoldoende	6	Uitbreiden loggingfunctiona	Malmberg	0	Er is na het doorvoeren	Op de ontwikkelag

	beveiligingsmaatregelen toegepast. (loggingfunctionaliteit)		liteit met inzicht in welke gebruikers exports/downloads hebben uitgevoerd, alsmede wie mutaties in cijfers heeft uitgevoerd. (technisch)			van de maatregelen geen restrisico	enda geplaatst. Uiterste datum gereed eind december 2026.
3	Er worden onvoldoende beveiligingsmaatregelen toegepast. (Toegang tot loggingfunctionaliteit)	9	Onderwijsinstellingen zelf toegang geven tot logging, zodat men zelfstandig kan monitoren. (technisch) Onderwijsinstelling moet afspraken maken over controle op de login. (organisatorisch)	Malmberg Onderwijsinstelling	0	Er is na het doorvoeren van de maatregelen geen restrisico	Op de ontwikkelag enda geplaatst. Uiterste datum gereed eind december 2026.
4	Geen grondslag, onvoldoende transparantie, onvoldoende beveiligingsmaatregelen toegepast. (YouTube-filmpjes)	6	Alternatieve oplossing implementeren (stoppen met gebruik YouTube) voor gebruik filmpjes. Indien dit niet mogelijk is, i.v.m. externe filmpjes, dan de meest privacy vriendelijke instellingen (aantoonbaar) doorvoeren. (technisch)	Malmberg	2	Malmberg is bereid om zoveel mogelijk filmpjes op eigen platform te realiseren. Daar waar dit niet mogelijk is, zal Malmberg de instellingen doorvoeren conform de *'privacy enhanced' (no-cookies)* modus. Er is na het doorvoeren van de maatregelen een minimaal en	Op de ontwikkelag enda geplaatst. Uiterste datum gereed eind december 2026.

						aanvaardbaar restrisico.	
5	Er worden onvoldoende beveiligingsmaatregelen toegepast. (hashing)	9	Implementeren van alternatieve hashing-methode.	Malmberg	0	Er is na het doorvoeren van de maatregelen geen restrisico	Hashing op basis van SHA-256 wordt geïmplementeerd. Uiterste datum gereed eind december 2025.
6	Er worden onvoldoende beveiligingsmaatregelen toegepast. (audits)	3	Aantoonbare uitvoering van audits op het interne ISMS van MAX, of certificering ISO 27001 (technisch)	Malmberg	0	Er is na het doorvoeren van de maatregelen geen restrisico	Periodieke interne controles bij Malmberg zijn reeds ingeregeld; aantoonbaarheid blijft aandachtspunt.
7	Ontoereikende afspraken in de verwerkersovereenkomst over de verwerking van de persoonsgegevens	9	Leverancier zal, zodra een nieuwe versie van de model verwerkersovereenkomst inclusief model bijlagen beschikbaar zijn, deze nieuwe versie hanteren en aan de daarbij behorende vereisten voldoen.	Malmberg + onderwijsinstelling	0	Er is na het doorvoeren van de maatregelen geen restrisico	Naar verwachting eind 2025 (afhankelijk van vaststellen nieuw model door Edu-V).
8	Achterhaalde informatie in de verwerkersovereenkomst over de verwerking van de persoonsgegevens. (bewaartermijn logfiles)	6	Aanpassen in nieuwe versie verwerkersovereenkomst	Malmberg + onderwijsinstelling	0	Er is na het doorvoeren van de maatregelen geen restrisico	Naar verwachting eind 2025 (afhankelijk van vaststellen nieuw model door Edu-V).
9	Er worden onvoldoende beveiligingsmaatregelen toegepast. (transport en fysieke opslag)	6	Voldoen aan de ROSA-vereisten m.b.t. Transport en fysieke opslag	Malmberg	0	Er is na het doorvoeren van de maatregelen geen restrisico	Uiterste datum gereed eind december 2025

10	Gebrek aan transparantie (adaptiviteitsinformatie)	4	Onderwijsinstelling moet betrokkenen hierover informeren	Onderwijsinstelling	0	Er is na het doorvoeren van de maatregelen geen restrisico	Uiterste datum gereed …

9. Deel E: MODEL lokale DPIA

Dit hoofdstuk bevat de afweging die iedere individueel schoolbestuur zelf moet maken. Het gaat om de rechtmatigheid van de voorgenomen verwerkingen, geconstateerde risico's en genomen en nog te nemen maatregelen om de gevolgen van die risico's te beperken. Daarnaast benoemt het schoolbestuur – indien van toepassing – extra risico's en aanvullende maatregelen die van toepassing zijn binnen het eigen schoolbestuur.

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

A. Uitvoering lokale DPIA

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

Bij de beoordeling in deze lokale DPIA zijn betrokken:

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

B. Overwegingen over centrale DPIA

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

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

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

C. Organisatiespecifieke- en algemene applicatierisico's

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

Risicotabel 1. Organisatie-specifieke risico's

Veilige gegevensverwerking omvat meer dan alleen de verwerkingsomgeving van de applicatie/ het systeem. Het vergt ook

dat de basis op orde is voor o.a. het besturingssysteem waarop het draait, de kennis en kunde van de gebruiker en het hebben en toepassen van relevant beleid.

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	Het bestuur heeft een eigen privacycoördinator of privacy officer.		
2	Binnen de organisatie zijn de volgende formele structuren geïmplementeerd: een autorisatiebeleid, toegangsbeheer, toewijzing van verantwoordelijkheden en eigenaarschap betreffende gegevensverwerking.		
3	Het gedetailleerde autorisatiebeleid specificeert welke toegangsniveaus en rechten per medewerker of rol vereist zijn om hun taken uit te voeren. Het autorisatiebeleid wordt regelmatig geëvalueerd en bijgewerkt om te blijven voldoen aan de veranderende behoeften en veiligheidsvereisten van de school.		
4	Het bestuur heeft een (externe) Functionaris Gegevensbescherming.		
5	Het bestuur heeft een datalekprotocol/beleid en past dit actief toe.		
6	Het bestuur heeft een IBP beleid en deze vastgesteld.		
7	Er is een PDCA m.b.t. de AVG waarbij er periodiek wordt gekeken of men compliant is en wat er verbeterd kan worden.		
8	Het bestuur heeft een gedragscode waarin diverse maatregelen voor gedrag en ICT beveiliging is opgenomen.		
9	Het bestuur heeft op elke schoolwebsite een pagina, dan wel een link naar de juiste pagina, over de AVG waarop informatie wordt verstrekt met betrekking tot de verwerking van persoonsgegevens, waaronder het gebruik van digitale leermiddelen (Privacyverklaring).		
10	Er is een actueel proces voor de rechten van betrokkenen.		
11	Ouders en medewerkers kunnen altijd en met succes de rechten van betrokkenen inroepen.		
12	Het bestuur heeft op elke schoolwebsite een pagina, dan wel een link naar de juiste pagina, over de wijze waarop de ouders (of leerlingen > 16 jaar) hun rechten kunnen uitoefenen (Privacyreglement).		

Risicotabel 2. Algemene applicatiespecifieke risico's

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

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	De verwerkersovereenkomst met verwerker is getekend.		

2	De verwerking is opgenomen in het register van verwerkingen.		
3	Het bestuur zal de DPIA over MAX minimaal eens per drie jaar herbeoordelen.		
4	Er zijn duidelijke afspraken over de invoer bij open velden. Dit kan bijvoorbeeld aan de hand van vastgesteld beleid of protocollen zijn geïmplementeerd. Hierin is vastgesteld of het gebruik van vrije invulvelden noodzakelijk is en zo ja voor welke informatie. Over deze uitgangspunten is duidelijk gecommuniceerd met alle medewerkers die gebruik maken van de applicatie.		
5	Het bestuur houdt rekening met dataminimalisatie voor verwerken van persoonsgegevens in de applicatie.		
6	Het bestuur hanteert de wettelijke bewaartermijnen. De bewaartermijnen zijn vastgesteld en beschreven.		
7	Het bestuur zorgt ervoor dat persoonsgegevens na afloop van de bewaartermijn daadwerkelijk worden geschoond en heeft een procedure hiervoor. De logbestanden (m.n. exports) worden periodiek gecontroleerd en de downloadmap wordt periodiek geleegd.		
8	Het bestuur voldoet aan het transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over de toepassing van MAX.		
9	Het bestuur heeft autorisaties ingericht op basis van 'need to know' (role based access).		
10	Afstemming met betrokkenen. Het bestuur heeft bij het uitvoeren van de lokale DPIA de betrokkenen om hun mening gevraagd over de verwerking en deze meegenomen in de DPIA (artikel 35 lid 9 AVG). Dit kan bijvoorbeeld via de medezeggenschapsraad.		
11	Gebruikers van de applicatie zijn/worden afdoende geschoold in het gebruik ervan.		
12	Persoonsgegevens worden niet op verkeerde plekken opgeslagen omdat regels en/of bekendheid met MAX dit voorkomt. Er is daarom geen sprake van een schaduwadministratie op verschillende schijven en mappen van medewerkers.		
13	Er is een functioneel beheerder aangewezen voor MAX.		
14	De onderwijsinstelling neemt verantwoordelijkheid voor het veilig koppelen van de applicatie met een ander systeem zoals een leerlingadministratiesysteem. *NB: MAX koppelt niet met andere systemen.*		

15	Kennis over applicatiebeheer is belegd bij meerdere personen en is gedocumenteerd.		
16	De onderwijsinstelling neemt verantwoordelijkheid om bij het beëindigen van de softwarelicentie de verwerkte persoonsgegevens terug te vorderen van de verwerker, samen met een schriftelijke bevestiging dat de vernietiging heeft plaatsgevonden.		

Risicotabel 3. Uit de centrale DPIA op schoolniveau te mitigeren risico's.

Risico	Te nemen maatregel	Uitgevoerd?	Opmerking/toelichting
In de open tekstvelden kunnen gevoelige/bijzondere persoonsgegevens worden ingevuld	Gedragsregel/instructie opstellen waarin is opgenomen dat dit niet toegestaan is.		
Exports/downloads onbeperkt beschikbaar	Gedragsregel/instructies opstellen over het maken en gebruiken van exports en hier controle op uitoefenen.		
Ontoereikende afspraken in de verwerkersovereenkomst over de verwerking van de persoonsgegevens	Doorvoeren nieuwe versie verwerkersovereenkomst zodra deze beschikbaar is.		
Onvoldoende informatie over adaptiviteitsfunctionaliteit	Betrokkenen hierover informeren (bijv. in privacyverklaring).		

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

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

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

- onvermogen om rechten uit te oefenen (inclusief maar niet beperkt tot privacyrechten);
- onvermogen om toegang te krijgen tot diensten of kansen;
- verlies van controle over het gebruik van persoonsgegevens;
- discriminatie;
- identiteitsdiefstal of fraude;
- financieel verlies;
- reputatieschade;
- verlies van vertrouwelijkheid;

- heridentificatie van gepseudonimiseerde gegevens; of
- elk ander significant economisch of sociaal nadeel
- gevolgen en risico's voor de beveiliging van MAX.

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

kans (waarschijnlijkheid) X impact (ernst) = risico

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

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

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

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

[kans (waarschijnlijkheid) X impact (ernst)] -/- [de risico-mitigerende maatregelen] = restrisico

De in de lokale DPIA geconstateerde risico's betreffen:

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

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

E. Verklaring en advies functionaris voor gegevensbescherming (fg)

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

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

Het advies van de fg is […].

F. Visie betrokkenen

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

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

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

G. Conclusie

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

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

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

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

H. Risico-mitigerende maatregelen schoolbestuur

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

Het schoolbestuur moet daarom zorgen voor:

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

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

I. Aanbevelingen

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

A. …

B. …

J. Verklaring schoolbestuur

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

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

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

Naam bestuurder(s):

Plaats:

Datum:

Ondertekening:

Bijlage 1: Gebruikte termen en definities

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

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

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

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

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

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

Gevoelige persoonsgegevens gaan over gegevens die volgens de Autoriteit Persoonsgegevens (AP) snel inbreuk (kunnen) maken op de persoonlijke levenssfeer. Het gaat bijvoorbeeld om leerresultaten van kinderen, omdat daar conclusies aan kunnen worden verbonden met gevolgen voor het latere maatschappelijke leven. Of het gaat om grote verzamelingen van informatie van (zeer) jonge kinderen, gegevens over (problematische) gezinssituatie of[31] zwaardere eisen gesteld aan de beveiliging van de gegevens.

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

[31] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf

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

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

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

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

Hieronder staan voorbeelden van categorieën persoonsgegevens en type persoonsgegevens die binnen die categorie vallen:
• Naam (voornaam, achternaam, voorvoegsel, initialen)
• Contactgegevens (huisadres, telefoonnummer, e-mailadres)
• Demografische gegevens (leeftijd, geboortedatum en -plaats, geslacht, nationaliteit, opleiding, IQ)
• Apparaat- en internetgegevens (IP-adres, MAC-adres, metadata, locatie-informatie en geografische informatie)
• Financiële gegevens (bankrekeningnummer en -saldo, inkomens- en vermogensgegevens, loonschaal, kredietwaardigheid, winst eenmanszaak)
• Werk gerelateerde gegevens (KvK-nummer, verslag van een functioneringsgesprek, documentatie over negatief gedrag op de werkvloer)
• Overige persoonsgegevens (voertuigidentificatienummer, persoonlijke voorkeuren)

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

Pseudonieme persoonsgegevens Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eisen verbonden dat de sleutels apart worden bewaard en dat maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.
Of pseudonieme gegevens door de ontvanger (verwerker) als persoonsgegevens aangemerkt moeten worden hangt af van de omstandigheden van het geval. Het uitvoeren van een toets zal kunnen uitwijzen in hoeverre deze door de leverancier te herleiden zijn tot persoonsgegevens[32].

[32] Het Gerecht EU 23 april 2023, T557/20, ECLI:EU:T:2023:219

Bijlage 2: Uitleg risico's

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

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

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

Hulpmiddel beoordelen score laag, midden en hoog

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