CENTRALE DPIA Vodix

Versie 2.0.1 (April 2026)

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:* Dyra Tensen (Jurist & adviseur IBP) *Betrokken bij de uitvoering van de DPIA:* Ashley Hoogendoorn (Jurist & project manager DPIA's) Soufyan El Oumaoui (TISO)
Met dank aan	*Vodix:* Robin van Rootseler
Auteurs model DPIA	Hans-Peter Ligthart (portfoliomanager IBP SIVON) Job Vos (jurist en adviseur IBP SIVON) Ferdy IJsselmuiden (DPIA-projectmanager)

Versie beheer

Datum	Versie	Wijziging
Maart 2022	0.0	Concept (HL)
Mei 2022	1.0	Basisversie (JV)
Februari 2023	1.1	Wijzigen risico-tabel (FI)
Juni 2023	1.2	Algemene verbeteringen Opnemen proces toetsen verwerkersovereenkomst Diverse technische vragen ondergebracht in bijlagen
Februari 2024	1.3	Aanpassingen en actualisatie (nieuw Rijksmodel 3.0)
Maart 2024	2.0	Nieuwe publieke versie
April 2026	2.0.1	Kleine (redactionele) wijzigingen

Inhoudsopgave

1. Leeswijzer 4

2. Samenvatting 5

3. Uitleg en achtergrond DPIA 8

1. Informatiebeveiliging en privacy (IBP) 9
2. Privacyconvenant en toetsing verwerkersovereenkomsten 9
3. DPIA 9
4. Verplichte uitvoering DPIA 10
5. Centrale en lokale DPIA 11
6. Methodiek DPIA 11
7. Funderend onderwijs referentie architectuur (FORA) 12

4. Motivering DPIA Vodix 13

1. Verplichting uitvoeren DPIA 13
2. Scope van deze DPIA 14
3. Buiten scope 14

5. Deel A: Gegevensverwerkingsanalyse 15

1. Beschrijving van het gegevensverwerkende proces 15
2. Persoonsgegevens 16
3. Gegevensverwerkingen 17
4. Verwerkingsdoeleinden 22
5. Betrokken partijen 24
6. Belangen bij de gegevensverwerking 25
7. Verwerkingslocaties 25
8. Data Transfer Impact Assessment (DTIA) 26
9. Technieken en methoden van gegevensverwerking 26
10. Juridisch en beleidsmatig kader 30
11. Bewaartermijnen 31

6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen 32

12. Rechtsgrond 32
13. Bijzondere persoonsgegevens 36
14. Doelbinding 37
15. Kinderrechten-afweging (Best Interests Assessment Children) 37
16 a. Noodzakelijkheid 40
16. b. Proportionaliteit en subsidiariteit 40

17. Rechten van de betrokkenen 40
18. Beoordeling verwerkersovereenkomst 42
7. Deel C: Beschrijving en beoordeling risico's voor de betrokkenen 42
Beoordelingskader risico's 42
19. Risico's 44
8. Deel D: Beschrijving voorgenomen maatregelen 46
20. Maatregelen 48
9. Deel E: MODEL lokale DPIA 52
A. Uitvoering lokale DPIA 52
B. Overwegingen over centrale DPIA 53
C. Organisatiespecifieke- en algemene applicatierisico's 53
D. Overwegingen implementatie en lokale DPIA: aanvullende risico's en maatregelen 56
E. Verklaring en advies functionaris voor gegevensbescherming (fg) 58
F. Visie betrokkenen 58
G. Conclusie 58
H. Risico-mitigerende maatregelen schoolbestuur 59
I. Aanbevelingen 59
J. Verklaring schoolbestuur 60
Bijlage 1: Gebruikte termen en definities 60
Bijlage 2: Uitleg risico's 63
Bijlage 3: Toetsrapport Verwerkersovereenkomst Vodix 65

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).

<u>De uitvoering van de DPIA bestaat uit de volgende onderdelen:</u>

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

Bijlage 1 bevat veelgebruikte termen en definities.

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

Bijlage 3 bevat het Toetsrapport Verwerkersovereenkomst Vodix.

2. Samenvatting

Deze DPIA heeft betrekking op de digitale leer- en toetsomgeving Vodix, die door Vodix wordt aangeboden aan onderwijsinstellingen in het voortgezet onderwijs. Vodix omvat verschillende lesmethodes: Tijd voor Geschiedenis, BeatsNbits, Backstage, iSociety, Paspoort 21, en CKV-lab. Binnen deze DPIA staat het gebruik van de online leeromgeving van deze methodes (applicatie) centraal.

Leerlingen en leraren in het voortgezet onderwijs maken gebruik van Vodix voor het oefenen, toetsen en begeleiden van leerprocessen. Daarbij worden persoonsgegevens van leerlingen en leraren verwerkt, waaronder identificerende gegevens, leer- en toetsresultaten en gebruiksgegevens. Omdat het hier grotendeels gaat om minderjarige betrokkenen en om structurele verwerking van leerresultaten (waaronder profilering in de zin van de AVG), is het uitvoeren van een DPIA verplicht.

In deze DPIA zijn de mogelijke risico's voor de rechten en vrijheden van betrokkenen geïnventariseerd en beoordeeld. Op basis daarvan is vastgesteld welke maatregelen noodzakelijk zijn om deze risico's te beperken en een veilig gebruik van Vodix mogelijk te maken. Ieder schoolbestuur dient deze centrale DPIA nog te vertalen naar een lokale DPIA, waarin eventuele organisatie-specifieke risico's en restrisico's worden afgewogen. Met deze centrale DPIA kan het schoolbestuur als verwerkingsverantwoordelijke aantoonbaar maken dat is voldaan aan de verplichtingen uit artikel 35 AVG.

Samenwerking

De samenwerking met Vodix tijdens het DPIA-proces is constructief en transparant verlopen. Vodix heeft actief meegedacht, relevante documentatie aangeleverd en inhoudelijk toelichting gegeven op onder andere de werking van de applicatie, de beveiligingsmaatregelen. Tijdens de uitvoering van de DPIA zijn reeds verschillende risico's onderkend en (gedeeltelijk) opgelost of op de ontwikkelagenda geplaatst, waaronder verbeteringen op het gebied van logging, bewaartermijnen, exportfunctionaliteiten en documentatie over rechten van betrokkenen.

Conclusie

Vodix heeft de in deze DPIA geïdentificeerde risico's deels reeds opgelost en voor de overige risico's concrete maatregelen voorgesteld die binnen afzienbare termijnen worden geïmplementeerd. In onderstaande tabel staan de risico's en maatregelen:

Risico nr.	Risico	Maatregel(en)
1.	Er zijn ontoereikende afspraken in de verwerkersovereenkomst over de verwerking van de persoonsgegevens. (verwerkersovereenkomst)	1.1 Het toevoegen van de verwerkingen en categorieën persoonsgegevens die onder het leerlingvolgsysteem vallen. 1.2 Het aanpassen van de bewaartermijnen, na uitvoering van maatregel. (organisatorisch)

Risico nr.	Risico	Maatregel(en)
		1.3 Het tekenen van, zodra er een nieuwe versie beschikbaar is, de laatste versie van de verwerkersovereenkomst door de scholen.
2.	Door onbedoeld gebruik van de export en/of download functie komen er mogelijk (gevoelige) persoonsgegevens buiten de applicatie terecht, met verlies van controle over deze data als gevolg. (exporteren/downloaden by default aan)	2.1 Het implementeren van een deactivatie-knop voor exporteren, waar bij de standaardinstelling op 'uit' staat. 2.2 Het implementeren van een waarschuwingsvenster voor het exporteren van data 2.3 Het inventariseren van de behoefte aan exports op leerlingniveau. Indien deze aanwezig is, dit mogelijk maken. (technisch) 2.4 Het door de scholen maken van afspraken over het maken en gebruiken van exports en hier controle op uitoefenen. (organisatorisch)
3.	Er worden onvoldoende beveiligingsmaatregelen toegepast, waardoor incidenten met persoonsgegevens niet adequaat/tijdig kunnen worden onderzocht en opgevolgd. (loggingfunctionaliteit)	3. Het uitbreiden van de loggingfunctionaliteit met inzicht in welke gebruikers exports/downloads hebben uitgevoerd, alsmede wie mutaties in cijfers heeft uitgevoerd. (technisch)
4.	Er worden onvoldoende beveiligingsmaatregelen toegepast, wat het tijdig signaleren van ongeautoriseerde of onbedoelde wijzigingen bemoeilijkt, evenals het snel onderzoeken van mogelijke incidenten. (toegang tot loggingfunctionaliteit	4.1 Scholen zelf toegang geven tot logging, zodat men zelfstandig kan monitoren. (technisch) 4.2 Het door de scholen maken van afspraken over controle op de logging. (organisatorisch)
5.	Persoonsgegevens worden langer bewaard dan noodzakelijk, waardoor het risico op ongeoorloofde toegang, datalekken, misbruik of onrechtmatige verwerking toeneemt. (bewaartermijnen)	5.1 Het aanpassen van de bewaartermijnen in lijn met sectoraal beleid en de handreiking van Kennisnet. 5.2 Het inkorten van bewaartermijnen na einde overeenkomst (2 á 3 maanden). (technisch) 5.3 Het, op initiatief van de onderwijsinstelling, inkorten van bewaartermijnen zodat deze aansluiten op de praktijk.
6.	Er worden onvoldoende beveiligingsmaatregelen toegepast. (audits)	6. Het uitvoeren van aantoonbare audits op het interne ISMS van Vodix, of certificering ISO 27001. (technisch)

Risico nr.	Risico	Maatregel(en)
7.	Er worden onvoldoende beveiligingsmaatregelen toegepast, waardoor wachtwoorden gemakkelijk zijn te kraken. (wachtwoordbeleid)	7.1 Het aanpassen van het wachtwoordbeleid in lijn met de vereisten in de NIST SP 800-63B Digital Identity Guidelines. (technisch) 7.2 Het door de scholen inregelen van een proces in voor het veilig beheren en bewaren van hun wachtwoorden (organisatorisch)
8.	Onvoldoende documentatie over de afhandeling van verzoeken van betrokkenen. (beleid rechten van betrokkenen)	8. Het ontwikkelen van beleid/werkinstructie omtrent de rechten van betrokkenen. (organisatorisch)
9.	Er worden onvoldoende beveiligingsmaatregelen toegepast, doordat vooraf gedefinieerde maatregelen tijdens het ontwerpen van de software, niet volledig of correct in het eindproduct worden geconfigureerd. (configuratie beveiligingsmaatregelen)	9. Het treffen van aanvullende beveiligingsmaatregelen ter voorkoming van 'Insecure Design'. (technisch)
10.	Er worden onvoldoende beveiligingsmaatregelen toegepast, door gebruik te maken van YouTube-video's waarbij er gegevens doorgegeven aan een partij buiten de EU/EEA. (YouTube-video's)	Geen aanvullende maatregelen vereist. De verwerking vindt plaats binnen de door YouTube aangeboden privacy-enhanced modus, waarmee tracking en profilering worden voorkomen en het resterende risico als laag wordt aangemerkt.
11.	Er worden onvoldoende beveiligingsmaatregelen toegepast. (toelichting ROSA-schema)	11. Het toevoegen van een toelichting bij de geïmplementeerde maatregelen in het ROSA-schema. (organisatorisch)

Wanneer de voorgestelde maatregelen door Vodix en de onderwijsinstellingen worden uitgevoerd, kan het gebruik van Vodix op een veilige wijze plaatsvinden. Het schoolbestuur blijft verantwoordelijk voor het uitvoeren van een lokale DPIA, het implementeren van organisatie-specifieke maatregelen en het expliciet aanvaarden van eventuele restrisico's.

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 de **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 de **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] of direct bij de verwerker. SIVON toetst voor het primair en voortgezet onderwijs vooraf of de verwerkersovereenkomsten van leveranciers van de meestgebruikte applicaties voldoen[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, applicatie of verwerking van persoonsgegevens. Meestal gaat het om een applicatie van een leverancier (verwerker). De DPIA wordt uitgevoerd volgens de eisen van artikel 35 van de AVG.

Met een DPIA wordt beoordeeld wat de risico's en (mogelijke) gevolgen zijn van het gebruik van de applicatie voor de bescherming van de persoonsgegevens van de leerlingen, hun ouders en medewerkers. Er wordt vastgesteld of het gebruik van persoonsgegevens (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 betreft een 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 uiteindelijke de DPIA vast, hiermee wordt bepaald 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 heeft gepubliceerd van de verwerkingen waarvoor 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.

Ook de EDPB benadrukt dit[5]: ‘*Een gegevensbeschermingseffectbeoordeling kan ook nuttig zijn om het gegevensbeschermingseffect van een technologisch product te beoordelen, bijvoorbeeld hardware of software, indien dit waarschijnlijk door verschillende verwerkingsverantwoordelijken zal worden gebruikt om verschillende verwerkingen uit te voeren. Natuurlijk blijft de verwerkingsverantwoordelijke die het product lanceert verplicht*

[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.

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.'

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 leerling-administratiesysteem. 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, worden 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. Bovendien leidt deze centrale aanpak tot een kostenbesparing voor de onderwijsinstellingen.

Schoolbesturen moeten volgens de AVG zelf als verwerkingsverantwoordelijke een DPIA uitvoeren en zelf de risico's afwegen. Dat kan SIVON niet doen. Na de uitvoering van de centrale DPIA moet daarom ieder schoolbestuur de uitkomsten uit de centrale DPIA op hun 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 onderwijs-specifieke 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)".

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

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

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

7. Funderend onderwijs referentie architectuur (FORA)

Bij de uitvoering van de DPIA wordt gebruik gemaakt van FORA[8]: Funderend Onderwijs Referentie Architectuur. FORA is een gestandaardiseerde methodiek die inzicht geeft in de verplichte processen en onderwijsactiviteiten in het primair en voortgezet onderwijs.

Applicatielandschap

Het hebben van een architectuur helpt bij het tijdig en goed reageren op zakelijke of juridische (AVG) eisen en/of (externe) dreigingen die een (mogelijke) aanpassing in de informatiehuishouding vragen.[9]

De FORA biedt inzicht in wat de bedrijfsfuncties zijn van een school in het primair of voortgezet onderwijs. Het hoofdbedrijfsfunctiemodel beschrijft op hoofdlijnen wat een onderwijsorganisatie doet. De 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.

[8] https://fora.wikixl.nl/index.php/Hoofdpagina
[9] Norm 1.4 architectuur van het Normenkader IBP https://aanpakibp.kennisnet.nl/normenkader/

Referentiecomponenten[10] 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, oftewel: hoe de applicatie zich verhoudt tot de overige applicaties die de school gebruikt.

SIVON voert centrale DPIA's uit op een applicatie. Een applicatie kan in de FORA vertaald worden naar een of meerdere referentiecomponenten[11]. Een referentiecomponent is een functionele afbakening van een modulair, zelfstandig inzetbaar en vervangbaar (deel van een) systeem.

4. Motivering DPIA Vodix

1. Verplichting uitvoeren DPIA

Bij het onderzoek naar het product Vodix, is gebleken dat het uitvoeren van een DPIA verplicht is om de volgende redenen. Volgens het overzicht van de European Data Protection Board[12] wordt er aan verschillende criteria voldaan, waardoor er sprake is van een 'hoog risicoverwerking'.

Er is ten eerste sprake van een verwerking 'op grote schaal' doordat er persoonsgegevens van leerlingen in het vo worden verwerkt binnen een verspreidingsgebied dat heel Nederland beslaat. Daarnaast worden er persoonsgegevens verwerkt van kinderen onder de 16 jaar. Deze gegevensverwerking vereist extra bescherming omdat het hier kwetsbare personen betreft. Een derde criterium betreft de verwerking van 'gevoelige gegevens' wat kan leiden tot 'evaluatie of scoretoekenning', omdat er binnen Vodix leer- en testresultaten worden verwerkt over een langere periode en deze resultaten zichtbaar zijn voor gebruikers (leraren en leerlingen). Hieruit volgt dat er sprake is van ten minste twee criteria uit de lijst van de WP29 op basis waarvan het uitvoeren van een DPIA verplicht is voor de verwerkingsverantwoordelijke die gebruikmaakt van Vodix.

Volgens de lijst van de Autoriteit Persoonsgegevens[13] 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 door aan dit criterium te voldoen is het uitvoeren van een DPIA verplicht. Bij Vodix gaat het hier specifiek om het vastleggen van resultaten en RTTI-scores van leerlingen ('leerprestaties') van methodetoetsen over een langere periode, waardoor de prestaties van leerlingen ten opzichte van andere leerlingen inzichtelijk zijn. Leraren kunnen hieruit afleiden dat een leerling bijvoorbeeld extra ondersteuning nodig heeft. Het vastleggen van leerprestaties is vanzelfsprekend een

[10] https://fora.wikixl.nl/index.php/Referentiecomponentenmodel
[11] https://fora.wikixl.nl/index.php/Referentiecomponentenmodel
[12] 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).
[13] Zie Staatscourant 2019, nummer 64418 van 27 november 2019.

wezenlijk onderdeel van het onderwijs, aangezien beoordelingen en voortgangsregistratie onmisbaar zijn voor het leerproces en het verantwoorden van onderwijskwaliteit. In deze context is 'profileren' een bijkomend logisch onderdeel van het onderwijs.

2. Scope van deze DPIA

Deze DPIA heeft betrekking op het gebruik van alle vormen van lesmateriaal die door Vodix via haar eigen applicatie worden aangeboden. Hieronder vallen de producten Tijd voor geschiedenis, BeatsNbits, Backstage, iSociety, Paspoort 21 en CKV-lab. Deze leermiddelen worden gebruikt door leerlingen in het voortgezet onderwijs.

De verwerking van persoonsgegevens binnen deze producten en diensten heeft betrekking op:

- Het toegang krijgen tot producten door middel van een inlogprocedure;
- Het werken met oefenmateriaal, waaronder oefenopgaven en toetsen, waarbij de gegevens worden verwerkt die leerlingen invullen bij gebruik van het leermiddel;
- Het terugkoppelen van resultaten van het gebruik door leerlingen aan een leerkracht, waardoor het bijvoorbeeld mogelijk is om te zien wat ieder van de leerlingen met de lesstof heeft gedaan en wat het resultaat daarvan is.

De scope van deze DPIA is beperkt tot alle verwerkingen van persoonsgegevens in het kader van het gebruik van de online omgeving van Vodix. 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 geïmplementeerd om deze risico's te minimaliseren, zodat Vodix op een veilige manier kan worden gebruikt.

Link naar uitgever en/of productpagina: https://www.vodix.nl.

Doelgroep: Voortgezet Onderwijs (VO), alle leerjaren.

Gebruikers: Leerlingen en leraren.

3. Buiten scope

Buiten deze DPIA vallen alle activiteiten die niet gerelateerd zijn aan het gebruik van Vodix door leerlingen en/of leraren, evenals de lesmethode Generation 24/7.

Verder vallen de volgende optionele verwerkingen buiten de scope van deze DPIA:

- 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.

In deze DPIA ligt de focus op de online leeromgeving (applicatie) van Vodix. In het applicatielandschap van een schoolbestuur kunnen vanuit de applicatie koppelingen worden gelegd met andere applicaties. Deze andere applicaties vallen buiten de scope van deze DPIA. Bij het gebruik van koppelingen 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

Vodix is een leverancier die als uitgeverij actief is binnen het voortgezet onderwijs en leerlingen ondersteunt bij het leren, verwerken en oefenen van de leerstof. Het doel hiervan is om bij te dragen aan het verbeteren van de studieresultaten en het stimuleren van zelfstandig leren bij leerlingen. Vodix levert verschillende modules (Tijd voor Geschiedenis, BeatsNbits, Backstage, iSociety, Paspoort 21 en CKV-lab) die leraren kunnen inzetten als digitaal lesmateriaal voor leerlingen in de volgende vakken:

- Maatschappijleer
- Geschiedenis
- Muziek
- Culturele en Kunstzinnige Vorming (CKV)

Leerlingen en leraren loggen in met een combinatie van inlognaam en wachtwoord of via Entree Federatie (Single Sign On, 2FA of MFA). Hierbij worden persoonsgegevens verwerkt zoals in deze DPIA weergegeven. De leraar kan gebruik maken van vaste modules voor de genoemde vakken of deze samenstelling zelf aanpassen. Een leerling kan binnen de modules uitleg krijgen over een onderwerp, en ook aan de hand hiervan vragen beantwoorden of toetsen maken. De uitkomsten van deze opdrachten kunnen vervolgens ook gekoppeld worden aan het Leerlingvolgsysteem (LVS).

De online omgeving van dit oefen- en toetsplatform gebruiken leerlingen om (individueel) opdrachten en aanvullend digitaal lesmateriaal te gebruiken, inclusief adaptieve oefeningen en zogenaamde Diagnostisch, Adaptief en Formatief (DAF) -toetsen.

Leerlingen kunnen de behaalde resultaten direct zelf inzien. Leraren hebben ook inzicht in de voortgang en resultaten van leerlingen en kan op basis hiervan niveaugericht feedback

en sturing geven. Er kunnen ook gegevens worden geëxporteerd in de vorm van een Excel-CSV- of PDF-bestand.

Leerlingvolgsysteem

Tijdens de les kan de leraar live volgen bij welke opdrachten de leerlingen zijn en de antwoorden per leerling bekijken, ook voordat de antwoorden definitief zijn ingevoerd. Ook wordt bijgehouden hoelang een leerling is ingelogd en hoeveel tijd er aan een opdracht is besteed. Hier wordt in de Kinderrechten-afweging (*zie hoofdstuk 6, 16.*) verder op in gegaan.

Hoewel Vodix de functionaliteit aanduidt als een leerlingvolgsysteem, betreft het hier geen LVS in de gebruikelijke onderwijsbetekenis. De functionaliteit is methode-gebonden en biedt inzicht in voortgang, inzet en resultaten binnen specifieke leermiddelen. De gegevens dienen primair ter didactische ondersteuning en worden waar relevant doorgezet naar een schoolbreed Leerlingvolgsysteem.

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 de digitale leeromgeving van Vodix worden persoonsgegevens verwerkt van leerlingen en leraren in het voortgezet onderwijs. Omdat de meeste leerlingen in het voortgezet onderwijs minderjarig zijn, is deze verwerking gericht op het verwerken van persoonsgegevens van kwetsbare personen (kinderen).

Persoonsgegevens

Tabel 3.1 Persoonsgegevens

Categorie persoonsgegevens	Leerling	Leraren	Bron verkrijging persoonsgegevens
Algemene (contact)gegevens	• Voornaam • Achternaam • Rol • Klas • Leerjaar • ILT-code • E-mailadres (school) • Naam en ID's Onderwijsinstelling • Licenties	• Voornaam • Achternaam • Rol • E-mailadres (school) • Naam en ID's Onderwijsinstelling • Licenties	SSO-dienst Entree Federatie of eigen invoer

Categorie persoonsgegevens	Leerling	Leraren	Bron verkrijging persoonsgegevens
Onderwijsdeelnemer-nummer	• ECK-ID		SSO-dienst Entree Federatie
Feiten en waarderingen over iemand zijn gedragingen, eigenschappen of opmerkingen	• RTTI-scores[14] • Feedback en beoordelingen	• Feedback en beoordelingen	Vodix of eigen invoer
Studievoortgang	• Tijdsbesteding per opdracht • Oefen- en toetsopgaven • Leer- en testresultaten		Vodix of eigen invoer
Inloggegevens	• E-mailadres i.c.m. wachtwoord • Inlogactiviteit	• E-mailadres i.c.m. wachtwoord • Inlogactiviteit	Eigen invoer
Gebruikersgegevens	• Diagnostische gegevens • Loggegevens • Metadata • IP-adres	• Diagnostische gegevens • Loggegevens • Metadata • IP-adres	Vodix
Cookiegegevens (leeromgeving)	• Gegevens over het functioneren en gebruik van het systeem	• Gegevens over het functioneren en gebruik van het systeem	Vodix

Er worden geen bijzondere, gevoelige of strafrechtelijke persoonsgegevens verwerkt.

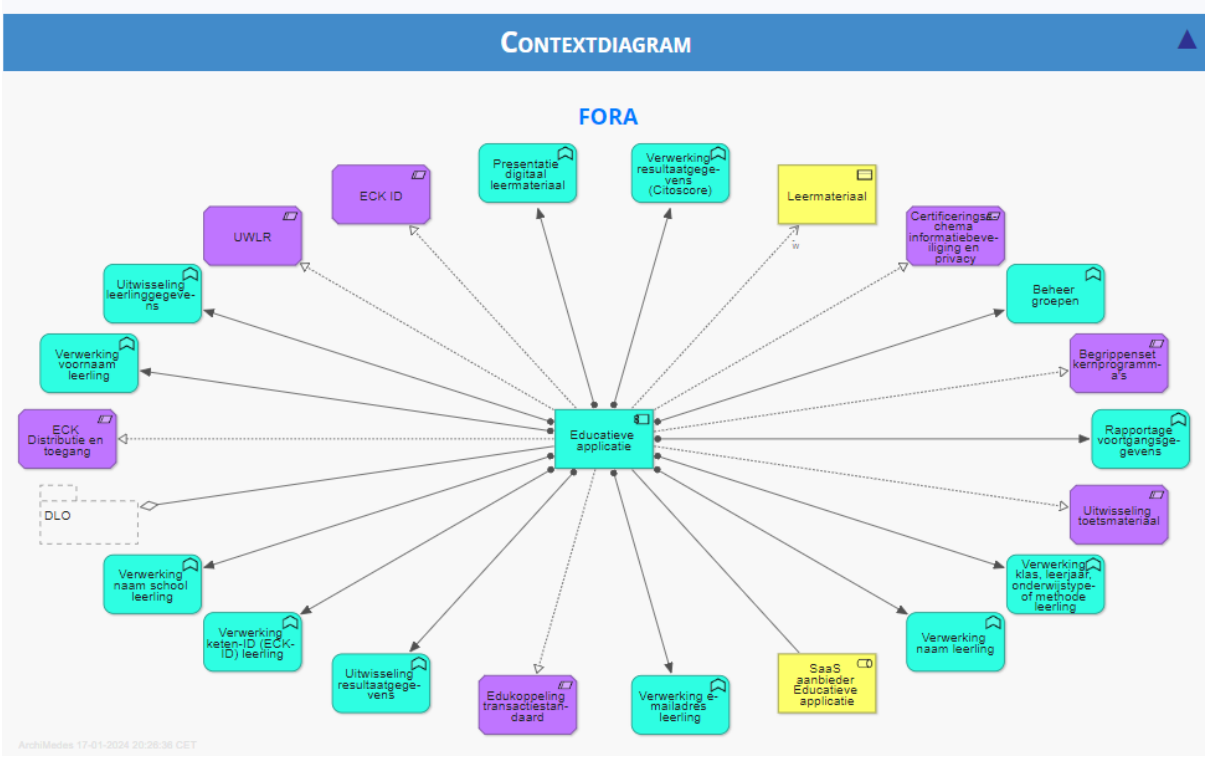
3. Gegevensverwerkingen

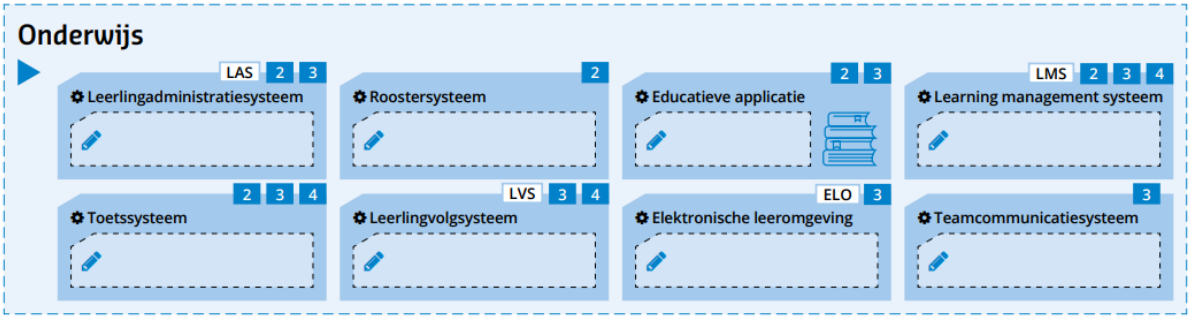
De verwerkingen binnen Vodix vinden primair plaats om onderwijsinstellingen in staat te stellen om door middel van de digitale leermiddelen onderwijs te geven en leerlingen te begeleiden.

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

Applicatielandschap

14 RTTI is een onderwijskundige taxonomie (Reproductie, Toepassing I & II, Inzicht) die toetst op vier cognitieve niveaus om leerresultaten te analyseren en leerprocessen te verbeteren. Het helpt docenten achter het cijfer te kijken, biedt inzicht in leerniveaus en maakt formatieve evaluatie mogelijk.





Voor de beschrijving van de verwerkingen die binnen Vodix 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 scopebepaling van deze DPIA, *zie hoofdstuk 4, 2 en 3*. De FORA (zie hierboven weergegeven afbeelding 'Contextdiagram[15]') heeft geen aanleiding 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 van Vodix vinden altijd de volgende verwerkingen plaats, in lijn met de doeleinden in 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;

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

- 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;
- Het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.

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 4, 3.*):

- 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.

Koppelingen

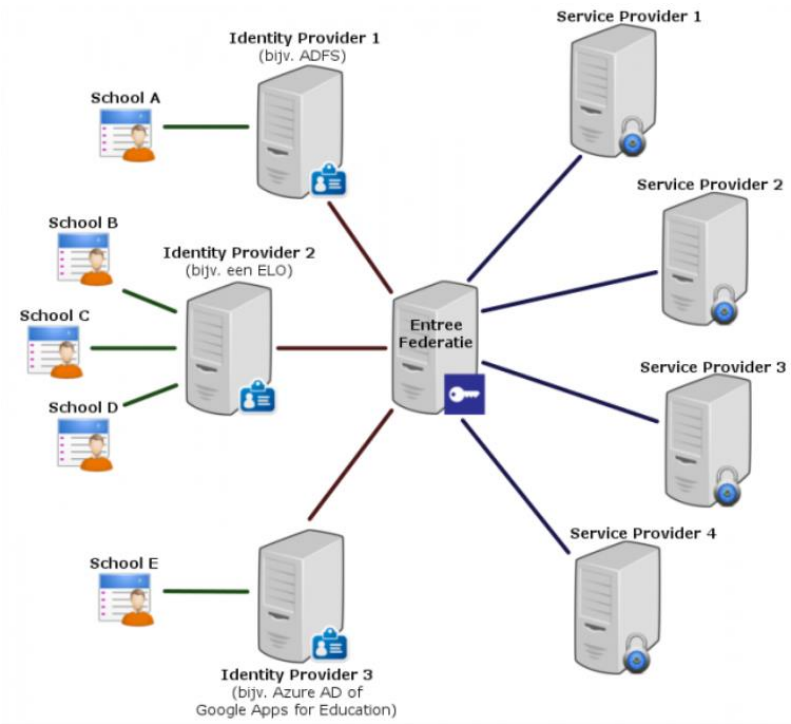
Entree Federatie geeft gebruikers in het vo en mbo-toegang tot een groot aantal educatieve diensten met slechts één login (ook wel bekend als Single Sign On of SSO). De federatie wordt gevormd door aanbieders van een educatieve dienst of content (Service Providers), beheerders van identiteiten (Identity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

Vodix is een educatieve dienst en wordt daarom beschouwd als een 'Service Provider'. Voor de koppeling met Entree is onderstaande overzichtsplaat van toepassing[16].



Bovenstaande visualisatie laat zien hoe Entree Federatie (SSO t.b.v. vo en mbo) zich verhoudt tot Vodix als serviceprovider ten aanzien van de toegang tot digitaal lesmateriaal.

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

Toegang tot Vodix kan onder andere plaatsvinden via een koppeling met Entree, waarbij 2FA/MFA niet wordt afgedwongen. Voor medewerkers van Vodix is MFA wel verplicht. De toegang via 2FA/MFA wordt in deze DPIA als een belangrijke beheersmaatregel gezien omdat Vodix veel (gevoelige) persoonsgegevens bevat, waaronder leerresultaten van leerlingen over een langere periode. Het verwerken van deze persoonsgegevens wordt door de Autoriteit Persoonsgegevens[17] gezien als 'profilering', waardoor onder andere extra technische maatregelen nodig zijn. Deze vorm van toegangsbeveiliging is daar een onderdeel van.

Adaptiviteit

Binnen Vodix wordt gebruik gemaakt van een beperkte vorm van adaptiviteit in de lesmethodes. Het betreft geen geavanceerde algoritmes of inzet van een AI-model. In Vodix wordt adaptiviteit gebruikt om leerlingen te ondersteunen in het leerproces, door extra oefeningen aan te bieden voor de leerdoelen die zij nog niet (volledig) beheersen. Er wordt gebruik gemaakt van DAF-toetsen waarbij DAF staat voor Diagnostisch, Adaptief en Formatief. Elk van die termen zegt iets over hoe de toets werkt en wat het doel ervan is:

- Diagnostisch betekent dat de toets laat zien wat een leerling al weet of kan en waar nog hiaten zitten (een soort nulmeting of voortgangsmeting).
- Adaptief houdt in dat de toets zich aanpast aan het niveau van de leerling: als een leerling veel goede antwoorden geeft, worden de vragen moeilijker; bij foute antwoorden juist iets makkelijker. Hierdoor sluit de toets beter aan bij het eigen niveau van de leerling.
- Formatief betekent dat de toets bedoeld is om te leren, niet om een eindcijfer te geven. Leerlingen krijgen inzicht in hun voortgang en kunnen zichzelf verbeteren.

Na afloop wordt er automatisch een rapport gegenereerd voor zowel de leraar als de leerling, waarin staat hoe goed de leerdoelen beheerst worden.

De conclusie is dat er slechts een beperkte functionaliteit is met betrekking tot de adaptiviteit in de leermethode. Op basis van de antwoorden op vragen, worden alleen makkelijke of juist moeilijkere vragen gesteld. Het betreft een niet-zelflerend[18] algoritme en er vindt binnen dit regelgebaseerd algoritme geen profilering plaats. De inzichten 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

[17] 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.

[18] De mens specificeert de regels die de computer moet volgen (regel gebaseerde algoritmes met een specifiek vooraf ontworpen stappenplan).

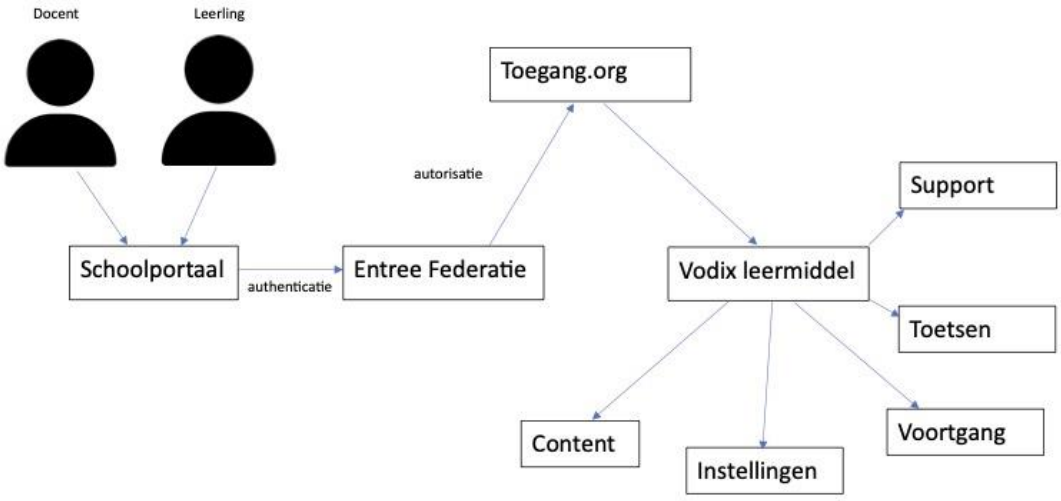
uiteindelijke cijfer van de leerling. Ook vindt er geen (leer en/of onderwijs) niveau-inschatting van de leerling plaats op basis van de gebruikte adaptiviteit.

Hierdoor is er geen sprake van een AI-Systeem[19] 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 Vodix beperkte (maar voldoende) informatie beschikbaar over bovenstaande vorm van adaptiviteit. Onderwijsinstellingen zijn zelf, als verwerkingsverantwoordelijken, verplicht hierover transparant te zijn en dienen dit derhalve op te nemen in hun verantwoording over verwerking van persoonsgegevens.

Gegevensstromen/stroomschema

Hieronder wordt in een vereenvoudigde weergave aangegeven hoe de gegevensstromen binnen Vodix plaatsvinden. Dit schema is op verzoek van SIVON opgesteld.



Bron: Vodix

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 (onderdeel B) en om vast te stellen

[19] 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.

welke maatregelen getroffen dienen te worden om de risico's (onderdeel C) te voorkomen of te verkleinen (onderdeel D).

De FORA[20] is gebruikt om de verwerkingsdoeleinden te bepalen. Voor Vodix 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[21] opgenomen verwerkingsdoeleinden. De verwerkingsdoeleinden zijn in de tabel hieronder schematisch weergegeven en gekoppeld aan de verwerking.

Tabel 4.1 Verwerkingsdoeleinden en verwerking

Doeleinde verwerking	Gegevensverwerking	Toelichting
Onderwijsevaluatie	De opslag, analyse en interpretatie 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.
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, waaronder de identificatie, authenticatie en autorisatie.	(Toegang tot) aanbod leermateriaal. Beheer identiteiten. Authenticatie en autorisatie.

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

Doeleinde verwerking	Gegevensverwerking	Toelichting
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

Tabel 5.1 Betrokken partijen en gegevensverwerking

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens	Verstrekker of ontvanger
Onderwijsinstelling	Zelfstandig verwerkings-verantwoordelijke	Beheer en toepassing van het digitaal leermateriaal	• Alle genoemde persoonsgegevens	V
Vodix	Verwerker	Aanbieder digitaal leermateriaal	• Alle genoemde persoonsgegevens	O
Exonet B.V.	Subverwerker	Hosting	• Alle genoemde persoonsgegevens	O
TransIP	Subverwerker	Hosting	• Alle genoemde persoonsgegevens	O
Do-It	Subverwerker	Helpdesk	• Contactgegevens • Onderwijsdeelnemer nummer • Naam van de Onderwijsinstelling • ID's van de Onderwijsinstelling	O

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens	Verstrekker of ontvanger
			• Licenties	
Topicus	Subverwerker	Toegangsdienstverlener	• Contactgegevens • Onderwijsdeelnemer nummer • ECK-ID • Naam van de Onderwijsinstelling • ID's van de Onderwijsinstelling • Licenties	V

Vodix verwijst vanuit de educatieve applicatie naar meerdere externe websites (waaronder, maar niet beperkt tot YouTube) via hyperlinks en door gebruik te maken van embedding. YouTube wordt niet gebruikt om filmpjes van leerlingen op te laten plaatsen en daarmee is YouTube geen subverwerker maar zelfstandig verwerkingsverantwoordelijke.

Vodix heeft aangegeven dat het gebruik van YouTube noodzakelijk is, aangezien het videomateriaal uitsluitend via dit platform rechtmatig beschikbaar wordt gesteld door de rechthebbenden en het gebruik van alternatieve oplossingen zou leiden tot schending van auteursrechten. Als mitigerende maatregel is wordt gebruik gemaakt van de no-cookie variant, waardoor een geen marketing- of trackingcookies worden geplaatst.

Dit kan leiden tot onrechtmatige verwerking (doorgifte) van persoonsgegevens. Immers, als de school de aanvullende services van Google niet aan heeft staan, worden er via het gebruik van YouTube binnen Vodix alsnog door Google persoonsgegevens verwerkt. *Zie 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 Vodix heeft, zijn het leveren van een goed werkende digitale omgeving waarin leermiddelen en toetsen worden aangeboden. Hierbij heeft Vodix ook een commercieel belang: een goed werkend product levert financieel voordeel op en het ondersteunt een goede reputatie en marktpositie van Vodix.

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

7. Verwerkingslocaties

Er worden via Vodix geen persoonsgegevens doorgegevens aan andere landen buiten de Europese Economische Ruimte (EER). Alle verwerkingen van (de sub-verwerkers van) Vodix vinden uitsluitend plaats binnen de EER.

Tabel 7.1 Verwerkingslocaties

Naam partij	Statutaire vestigings-plaats (sub-) verwerker	Plaats/land van opslag en verwerking persoonsgegevens en doorgifte mechanisme indien buiten de EER
Vodix	Nederland	Nederland
Exonet	Nederland	Nederland
TransIP	Nederland	Nederland
Do-IT	Nederland	Nederland
Topicus	Nederland	Nederland

8. Data Transfer Impact Assessment (DTIA)

De AVG bevat specifieke regels voor de doorgifte van persoonsgegevens naar landen buiten de EER. In beginsel mogen persoonsgegevens alleen worden overgedragen aan landen buiten de EER als het land een 'passend beschermingsniveau' heeft. Dat niveau kan op verschillende manieren worden bepaald: een multinational kan bindende bedrijfsvoorschriften vaststellen (BCR's), de EU-standaardcontractbepalingen (SCC) toepassen of alleen overdragen aan landen waarvoor de Europese Commissie een zogeheten adequaatheidsbesluit[22] heeft genomen. Vodix verwerkt geen persoonsgegevens in landen buiten de EER waardoor aanvullende waarborgen en een Data Transfer Impact Assessment (DTIA) in dit kader niet vereist zijn.

9. Technieken en methoden van gegevensverwerking

Artikel 32 van de AVG schrijft voor dat er passende technische en organisatorische maatregelen genomen moeten worden om een op het risico afgestemd beveiligingsniveau te waarborgen. Om inzicht te krijgen in welke mate er vorm wordt gegeven aan deze abstracte formulering wordt gebruik gemaakt van de voor de verwerkers opgestelde standaard DPIA-vragenlijst. Deze vragenlijst wordt door de verwerker gevuld en zal voor een belangrijk deel inzicht geven in onder andere de genomen technische beheersmaatregelen en informatiebeveiliging. Het gebruik 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 data-verwerkingen.

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

Er is onderzoek verricht naar de status van informatiebeveiliging van Vodix. Dit onderzoek is uitgevoerd door de door Vodix aangeleverde informatie te analyseren, door een Leverancier Security Compliance Check (LSCC) vragenlijst toe te sturen en door een compliance check op het ROSA-certificeringsschema uit te voeren.

Op basis van dit onderzoek is het volgende vastgesteld:

BIV-classificatie
Er wordt door Vodix in het ROSA-certificeringsschema (ROSA-schema) een BIV-classificatie toegepast op het niveau Hoog-Midden-Midden. Dit betekent dat Vodix de 'Vertrouwelijkheid' van de persoonsgegevens beoordeelt als 'Midden'. Vanuit SIVON is aangegeven dat er sprake is van een Vertrouwelijkheidsscore 'Hoog' vanwege het feit dat in de applicatie sprake is van '*profilering*' volgens de omschrijving van de AP[23]:
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 AP gaat duidelijk in op het verwerken van persoonsgegevens van *kwetsbare jongeren* in een geautomatiseerd systeem dat toetsresultaten en andere persoonsgegevens verwerkt. Dit wordt door de AP *profilering* genoemd en gelabeld als een '*hoog risico-verwerking'* (corresponderend met classificatie 'Hoog' voor 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 Vodix toegekend op basis van de ROSA, waarbij Vodix uitkomt op 'Midden'. SIVON adviseert om, voor zover praktisch haalbaar, de maatregelen toe te passen welke in lijn zijn met de classificatie 'Hoog' van de ROSA, ter bevordering van een optimale beveiliging van persoonsgegevens: dubbele encryptie van de database en uitgebreide loggingfunctionaliteit. Aangezien de huidige voorwaarden bij het ROSA-schema nog niet zijn aangepast op de uitleg door de AP, zal deze selfassessment op 'Midden' in deze DPIA niet als een risico opgenomen worden.

Vodix werkt met verschillende databases, waarbij er scheiding is van diverse verwerkingen. Daarnaast zijn de identificerende gegevens gescheiden van de databases, welke alle encrypted zijn.

Leverancier Security Compliance Check
Uit de door de leverancier ingevulde vragenlijst zijn de volgende (technische) bevindingen naar voren gekomen:
Vraagstuk: A6:2025 – Insecure Design: Worden security requirements getraceerd tot implementatie in code?

Bovenstaande vraag is door de leverancier beantwoord met 'Nee'. Dit gaat gepaard met het

[23] Zie: https://www.autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia; Staatscourant 2019, nr. 64418, 27 november 2019, onderdeel 15. Profilering.

risico dat de vooraf gedefinieerde securitymaatregelen tijdens het ontwerpen van de software, niet altijd (volledig of correct) in het eindproduct worden geconfigureerd. Hierdoor zou de applicatie kwetsbaar kunnen worden voor het domein A6:2025 – Insecure Design van de OWASP TOP 10:2025.

Ondanks de bovenstaande bevinding acht SIVON, op basis van alle ontvangen en beoordeelde informatie, de kans dat Vodix kwetsbaar wordt binnen het domein A6:2025 - Insecure Design van de OWASP TOP 10:2025 laag. Om deze reden worden geen aanvullende maatregelen *noodzakelijk* geacht, maar wel geadviseerd ter bevordering van de (technische) informatiebeveiliging:

- Formaliseren van security requirements management
  Zorg ervoor dat security-eisen expliciet worden vastgelegd als onderdeel van de functionele en technische requirements. Deze eisen moeten gedurende de volledige ontwikkelcyclus worden beheerd.
- Traceability tussen security requirements en implementatie
  Richt een proces in waarbij security requirements aantoonbaar worden getraceerd naar ontwerpdocumentatie, code-implementatie en testcases (bijvoorbeeld via requirement management of issue-tracking tooling). Hierdoor kan worden vastgesteld dat alle security-eisen daadwerkelijk zijn geïmplementeerd.
- Secure Software Development Lifecycle (SSDLC) implementeren
  Integreer security structureel in de ontwikkelmethodiek, bijvoorbeeld door het toepassen van een Secure SDLC waarbij security-activiteiten zijn opgenomen in elke ontwikkelfase (ontwerp, ontwikkeling, testen en release).
- Securitydesign reviews uitvoeren
  Voer periodieke securitydesign reviews uit tijdens de ontwerpfase van de applicatie om te controleren of security requirements correct zijn verwerkt in de architectuur en het ontwerp.
- Security testing opnemen in het ontwikkelproces
  Voer aanvullende securitytests uit, zoals:
  - Static Application Security Testing (SAST)
  - Dynamic Application Security Testing (DAST)

  Dit helpt bij het identificeren van kwetsbaarheden die ontstaan door onvolledige implementatie van security requirements.
- Gebruik van secure coding standaarden
  Hanteer erkende secure coding richtlijnen (bijvoorbeeld gebaseerd op OWASP-richtlijnen) en borg dat ontwikkelaars hiermee werken tijdens de implementatie.
- Documentatie en aantoonbaarheid verbeteren
  Documenteer hoe security requirements zijn vertaald naar ontwerp en code. Dit vergroot de aantoonbaarheid richting audits en compliance-controles.

Middels de OWASP Top 10 is door SIVON het volwassenheidsniveau van de (technische) informatiebeveiliging van de applicatie gemeten en geanalyseerd. De leverancier heeft bevestigd dat er passende beveiligingsmaatregelen zijn geïmplementeerd om de meest voorkomende kwetsbaarheden binnen de OWASP-categorieën te mitigeren, met uitzondering van het risicogebied A6:2025 – Insecure Design.

De ingevulde vragenlijst biedt voldoende onderbouwing dat voor de onderwerpen waarbij geen bijzonderheden zijn opgemerkt, de beveiligingsrisico's adequaat zijn beheerst, conform de gangbare beveiligingsprincipes binnen de OWASP-methodiek. Er zijn bij deze onderdelen geen aanvullende risico's of tekortkomingen geconstateerd die impact hebben op de verwerkingsactiviteiten binnen deze DPIA.

Organisatorische maatregelen
Binnen Vodix wordt organisatiebreed gebruik gemaakt van gedocumenteerde beveiligings- en incidentprotocollen en is een register van verwerkingen geïmplementeerd dat wordt bijgehouden.

Overige bevindingen

- Autorisaties zijn instelbaar op een 'need to know'-basis (rolgebaseerd), zodat alleen de leraar toegang heeft tot de gegevens van zijn klas en leerlingen.
- Jaarlijks wordt de omgeving van Vodix intern aan een pentest onderworpen, waar een uitgebreide rapportage aan ten grondslag ligt. De frequentie van externe pentests is afhankelijk van de aard van de ontwikkelingen die hebben plaatsgevonden.
- Vodix heeft een adequaat back-up beleid. Het back-up beleid voldoet aan alle vereisten zoals benoemd in het ROSA model.
- Vodix maakt in slechts beperkte mate gebruik van metadata zoals cookies binnen de applicatie, die voor functionele toepassingen worden gebruikt en die afdoende zijn beschreven in de verwerkersovereenkomst.
- Vodix conformeert zich niet aantoonbaar aan de ISO 27001 normering. Dit vormt een risico op het gebied van informatiebeveiliging, aangezien het ontbreken van een gecertificeerd informatiebeveiligingsmanagementsysteem (ISMS) met zich mee kan brengen dat er onvoldoende technische en organisatorische maatregelen zijn getroffen. Dit risico kan worden gemitigeerd door middel van een aantoonbare, jaarlijkse onafhankelijke toetsing.
- Vodix past logging toe die uitsluitend door de onderwijsinstelling is op te vragen via de servicedesk van Vodix. Het Normenkader IBP schrijft echter voor dat de onderwijsinstelling de logging zelfstandig moet kunnen monitoren. Daarnaast gaat ook de ISO 27001-norm ervan uit dat de verwerkingsverantwoordelijke zelf verantwoordelijk is voor de monitoring van loggegevens. SIVON adviseert daarom om een functionaliteit te implementeren die het mogelijk maakt voor de onderwijsinstellingen om zelf over de loggegevens beschikken.
- De exportfunctionaliteit binnen Vodix is standaard (by default) beschikbaar voor alle gebruikers, zonder functionele of autorisatie-gerichte beperkingen. Daarnaast bevatten de huidige loggegevens geen informatie over het gebruik van deze exportfunctionaliteit. Hierdoor ontbreekt inzicht in welke gebruiker, op welk moment, welke gegevens heeft geëxporteerd.
- Dit vormt een risico voor de bescherming van persoonsgegevens, aangezien ongeautoriseerde of excessieve gegevensverstrekkingen niet kunnen worden gedetecteerd of achteraf getraceerd. Tevens is er geen mogelijkheid tot monitoring of signalering van afwijkend of potentieel misbruik van deze functionaliteit.
- SIVON adviseert om, in lijn met het beginsel van Privacy by Default zoals bedoeld in artikel 25 AVG, de exportfunctionaliteit standaard uit te schakelen. Daarbij moet

worden gewaarborgd dat de school, indien benodigd, gegevens kan exporteren op zowel klasniveau als leerlingniveau. Daarnaast wordt geadviseerd om de logging uit te breiden, zodat ten minste wordt vastgelegd welke gebruiker een export uitvoert, welke gegevens worden geëxporteerd en op welk moment.
- Binnen Vodix wordt gebruikgemaakt van YouTube-video's. Dit houdt een risico in, aangezien bij het gebruik hiervan via Vodix persoonsgegevens worden gedeeld met Google. Voor scholen die de Google additionele services hebben uitgeschakeld, betekent dit dat via Vodix toch, al dan niet in beperkte mate, gegevens worden uitgewisseld met Google.

Zie hoofdstuk 19 en 20 voor de risico's en mitigerende maatregelen.

IAMA: mensenrechten in beeld bij algoritmes

Er wordt door Vodix geen gebruik gemaakt van geavanceerde algoritmes of andere vormen van AI-technologie. Zie hiervoor de analyse in hoofdstuk 3.

Hierdoor is er geen sprake van een AI-systeem[24] 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[25] geen verplichting.

10. Juridisch en beleidsmatig kader

Onderstaande tabel geeft de juridische en beleidsmatige fundamenten ten aanzien van het gebruik van Vodix binnen het onderwijs weer. De hieruit voortvloeiende verwerkingen van persoonsgegevens zijn inherent aan het doel van de verwerking, namelijk het aanbieden van digitale leer- en toetsapplicatie.

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

Tabel 10.1 Juridisch en beleidsmatig kader

[24] 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.
[25] https://www.rijksoverheid.nl/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes

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 8.17 lid 10 WVO 2020
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 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

Binnen het systeem zijn een aantal standaard bewaartermijnen ingeregeld welke zijn weergegeven in de tabel hieronder. Deze gelden ook na beëindiging van het contract tussen Vodix en de onderwijsinstelling.

Tabel 11.1 Bewaartermijnen

Categorieën persoonsgegevens	Bewaartermijn
Naam, klas, gebruikte IP-adressen	Einde schooljaar
E-mailadres/ECK-iD gekoppeld aan oefen- en toetsopgaven en eventuele beoordeling	3 jaar
Unieke ID's en inlogpogingen die gebruikt worden in logbestanden ten behoeve van het bewaken van de integriteit en vertrouwelijkheid	13 maanden
Naam, e-mailadres, ECK-ID, IP-adres in audittrail ten behoeve van de herleidbaarheid en onweerlegbaarheid conform het certificeringsschema	13 maanden
Cookie met session identifier. Dit is een noodzakelijke cookie.	Einde browsersessie
Cookie met gebruikersnaam (op verzoek gebruiker)	1 jaar

De persoonsgegevens binnen Vodix die verband houden met lesuitvoering en toetsafnames worden door Vodix gedurende drie jaar bewaard. De geldende norm uit het landelijk

vastgestelde sectoraal beleid[26] gaat uit van een bewaartermijn van twee jaren na de laatste inlogpoging. De door Vodix gehanteerde bewaartermijn wijkt hiervan af.

In de Handreiking bewaartermijnen van Kennisnet[27] wordt voor deze categorie persoonsgegevens een bewaartermijn van het huidige schooljaar plus een of twee jaar (afhankelijk van of het onder- of bovenbouw betreft) genoemd.

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

SIVON adviseert om bovenstaande bewaartermijnen te hanteren en de termijn na beëindiging van de overeenkomst te verkorten tot drie maanden. Hiermee wordt verondersteld dat de onderwijsinstelling voldoende tijd heeft om de benodigde data te exporteren. *Zie hoofdstuk 19 en 20.*

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 Vodix. 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. Kortere bewaartermijnen in Vodix kunnen worden gerealiseerd door een verzoek in te dienen bij de servicedesk van Vodix.

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 waarop een gegevensverwerking op kan worden gebaseerd:

a) Toestemming van de betrokkene (art. 6, eerste lid, sub a, AVG)
b) Uitvoering van een overeenkomst (art. 6, eerste lid, sub b, AVG)

[26] https://aanpakibp.kennisnet.nl/bewaartermijnen/
[27] Zie Kennisnet: Tijdelijke handreiking bewaartermijnen po/vo 1.2 (december 2020).

c) Wettelijke verplichting[28] (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[29] (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 sub 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.

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 van toepassing is op de schoolbesturen bij de uitvoering van de in deze DPIA beschreven processen, zijn de hoofdlijnen van de daarbij behorende verwerkingen van persoonsgegevens voldoende inzichtelijk vastgelegd. Zo

[28] 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.
[29] 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.

behoort het tot de verantwoordelijkheid van de school om ervoor zorg te dragen dat de leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen.[30]

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 Vodix omdat dit een digitaal leermiddel en toetssysteem betreft, dat de noodzakelijke ondersteuning biedt voor de uitvoering van onderwijstaken.

Artikel 2.89 van de WVO 2020 *'Onderwijskundig beleid'* biedt daarmee een solide basis voor de gegevensverwerkingen die binnen het gebruik van Vodix 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 Vodix 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

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.

[30] 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.*

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 Vodix 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, analyse en interpretatie 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. • Het geleverd krijgen/ in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier. • Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie. • De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8.17 lid 10 WVO 2020. Taak van algemeen belang (of openbaar gezag).	De AVG-grondslag voor het inzetten van een leermethode zoals Vodix is artikel 6 lid 1 sub e AVG (*algemeen belang, o.b.v. onderwijswetgeving)*.

Verwerking/doeleinde	Grondslag AVG	Toelichting
• 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. • Het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.		

Vodix zelf heeft tijdens deze DPIA aangegeven dat de verwerkingen zijn gebaseerd op Art.6, eerste lid, sub b AVG, uitvoering van een overeenkomst (namelijk het contract tussen Vodix en het schoolbestuur). Na het voorleggen van bovenstaande zienswijze van SIVON sluit Vodix aan bij de hierboven toegelichte grondslag, een taak van algemeen belang.

13. Bijzondere persoonsgegevens

Er worden bij het gebruik van Vodix geen bijzondere, gevoelige of strafrechtelijke persoonsgegevens verwerkt of wettelijke identificatienummers.

In het kader van deze DPIA wordt gewezen op het risico van open tekstvelden in Vodix. In Vodix kunnen leraren gedurende en na het maken van de opdrachten feedback geven aan de leerling. 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. Ook kan een leraar via de chat-functie (open tekstveld) feedback aan Vodix geven over de applicatie. Tijdens de uitvoering van deze DPIA is dit risico opgelost doordat de chat-functie is komen te vervallen.

In het kader van gepersonaliseerde instellingen kan de onderwijsdeelnemer (leerling) binnen Vodix eigen voorkeuren instellen die het leerproces en het behalen van de leerdoelen ondersteunen. Zo kunnen teksten worden voorgelezen en kunnen voorkeuren worden ingesteld, zoals tekstkleur, lettergrootte en lettertype ('fonts'). Deze instellingen zijn echter uitsluitend bedoeld als gebruiksvoorkeuren en duiden niet per definitie op zichtbeperkingen of leerstoornissen (zoals dyslexie). De gekozen instellingen worden opgeslagen, zodat de gepersonaliseerde leeromgeving behouden blijft bij volgend gebruik.

14. Doelbinding

In het kader van de verwerking van persoonsgegevens via Vodix worden er geen persoonsgegevens verwerkt voor een ander doel dan waarvoor deze oorspronkelijk zijn verzameld. Alle persoonsgegevens worden verwerkt voor de doeleinden omschreven in Hoofdstuk 4.

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 Vodix 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[31]. De afweging bestaat uit 4 stappen:

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

[31] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/best-interests-self-assessment/

Hieronder wordt beschreven welke rechten[32] van en voor kinderen relevant zijn in het kader van deze DPIA. Van belang is de leeftijd van de kinderen (leeftijdsadequaat). Hierbij wordt nagegaan of de gegevensverwerking (negatieve) gevolgen heeft voor de ondersteuning en van de behoeften van het kind op het gebied van veiligheid, gezondheid, welzijn, familierelaties, fysieke, psychologische en emotionele ontwikkeling, identiteit, vrijwaring van economische commerciële en/of fysieke uitbuiting, vrijheid van meningsuiting, privacy en de mogelijkheid om een eigen mening te vormen en deze te laten horen, het belang van toegang tot informatie, omgang met anderen en spel (buiten spelen) om de ontwikkeling van het kind te ondersteunen. Het gaat erom dat het kind in overeenstemming met zijn of haar ontwikkelende capaciteiten, een stem heeft (kan hebben) in zaken die hem of haar aangaan.

Vodix 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 Vodix en de daarmee samenhangende gegevensverwerkingen. Dit wordt hieronder verder afgewogen.

2. Identificeer het effect van de gegevensverwerking en gebruik van Vodix 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 Vodix:

- 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.

Het gebruik van Vodix 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.

[32] https://wetten.overheid.nl/BWBV0002508/2002-11-18#Verdrag_2

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

Vodix beschikt wel over een zogeheten ‘*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 en betreft een voor onderwijskundige doeleinden belangrijke functie. De leraar kan hiermee bijvoorbeeld inzicht krijgen in hoe de leerling tot een antwoord komt. Hiervoor is binnen Vodix in het geval van open vragen een veld beschikbaar waarin de leerling bijvoorbeeld uitschrijft hoe deze tot een conclusie komt. Door inzage in dit veld kan de leraar de leerling helpen tot verbeterde inzichten te komen.

Ook kan de leraar tijdens de les semi-live meekijken naar met welke opdrachten de leerlingen bezig zijn en daarmee de voortgang in de gaten houden. Zodra een leerling het antwoord op een vraag heeft opgeslagen, is dit ook inzichtelijk voor de leraar. De leraar kan dus niet live meekijken op het device van de leerling en ziet het antwoord pas zodra dit is opgeslagen. Het doel van deze functionaliteit is dat de leraar real-time inzicht krijgt in de voortgang van leerlingen tijdens de les. Zo kan de leraar direct ondersteuning bieden waar nodig en het onderwijs beter afstemmen op de behoeften van de leerlingen.

Bovenstaande functies omvatten 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 meekijken naar hoever de leerling is met een bepaalde opdracht. Het is hierdoor niet noodzakelijk de leerling er via een ‘privacyverklaring’ op te wijzen dat het werk kan worden ingezien: er kan niet ‘live’ meegekeken worden.

3. Beoordeel of dit effect wenselijk is

Zoals onder punt 2 vermeld, lijken er geen negatieve gevolgen te zijn voor het gebruik van Vodix. Vodix 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 Vodix om gepersonaliseerde instellingen toe te passen en het eenvoudige algoritme dat makkelijkere, dan wel moeilijker vragen voorstelt en aldus inspeelt op de individuele leerbehoefte van de leerling lijkt alleszins in het voordeel van de leerling.

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

Er is geen noodzaak om aanvullende maatregelen te nemen om de rechten van het kind te beschermen. De effecten die de gegevensverwerkingen binnen Vodix 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 Vodix 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 Vodix 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.

Door het toepassen van autorisatiebeheer hebben uitsluitend daartoe bevoegde medewerkers van de onderwijsinstelling (en de leverancier) op een ‘*need to know*’-basis toegang tot de gegevens van leerlingen van hun groep, en is de inbreuk beperkt tot professionals die leerlingen ondersteunen in hun ontwikkelingsproces. De minimale gegevens zijn noodzakelijk om de vakken en toetsen binnen Vodix aan leerlingen aan te kunnen bieden.

Het gebruik van potlood en papier vormt in theorie een alternatief, maar is niet per definitie eenvoudiger of veiliger. Het gebruik van een digitaal leerplatform is, gelet op het beoogde doel, niet wezenlijk meer belastend voor de persoonlijke levenssfeer van leerlingen en wordt als proportioneel aangemerkt.

17. Rechten van de betrokkenen

De onderwijsinstelling die gebruik maakt van Vodix dient op haar website een privacyverklaring opgenomen te hebben waarin staat beschreven welke rechten betrokkenen[33] hebben en hoe men hun rechten kan uitoefenen. Voor de afhandeling van verzoeken gericht aan Vodix als verwerkingsverantwoordelijke heeft Vodix tijdens deze DPIA en beleidsdocument 'Afhandeling Privacyverzoeken' opgesteld.

Vodix ondersteunt de onderwijsinstelling bij het voldoen aan de verplichtingen van de verwerkingsverantwoordelijke om te voldoen aan de rechten van betrokkenen. Verzoeken kunnen worden ingediend door een e-mail te sturen naar info@vodix.nl, servicedesk@vodix.nl of privacy@vodix.nl. Ook kan contact worden opgenomen via het contactformulier op de website en op werkdagen telefonisch via +0316820993. Als het verzoek is bedoeld voor de onderwijsinstelling zonder dat daar ondersteuning vanuit Vodix voor nodig is, stuurt Vodix de vraag door naar de onderwijsinstelling.

In de onderstaande tabel wordt aangegeven welke rechten Vodix in behandeling neemt en of er van enige beperking sprake is.

Recht van betrokkene	Toelichting procedure
Het recht op informatie	De onderwijsinstelling dient als verwerkingsverantwoordelijke te zorgen voor een: Openbaar gepubliceerde privacyverklaring op de website.
Het recht van inzage	Als de onderwijsinstelling bij het behandelen van een verzoek ondersteuning nodig heeft van Vodix dan wordt deze verleend.
Het recht op rectificatie	Als de onderwijsinstelling bij het behandelen van een verzoek ondersteuning nodig heeft van Vodix dan wordt deze verleend.
Het recht op gegevenswissing	Als de onderwijsinstelling bij het behandelen van een verzoekondersteuning nodig heeft van Vodix dan wordt deze verleend.
Het recht op beperking van de verwerking	Als de onderwijsinstelling bij het behandelen van een verzoekondersteuning nodig heeft van Vodix dan wordt deze verleend.
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	Als de onderwijsinstelling bij het behandelen van een verzoekondersteuning nodig heeft van Vodix dan wordt deze verleend.
Het recht op overdraagbaarheid van gegevens	Als de onderwijsinstelling bij het behandelen van een verzoekondersteuning nodig heeft van Vodix dan wordt deze verleend.

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

Recht van betrokkene	Toelichting procedure
Het recht van bezwaar	Als de onderwijsinstelling bij het behandelen van een verzoekondersteuning nodig heeft van Vodix dan wordt deze verleend.
Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit	N.v.t, want er is geen sprake van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit.

18. Beoordeling verwerkersovereenkomst

Voor leveranciers die deelnemer of medestander zijn van het Privacyconvenant en daarbij gebruik maken van het daarbij horende model verwerkersovereenkomst vindt een toetsing plaats op basis van de vereisten van het convenant. Dit wordt de theoretische toets genoemd. Aanvullend hierop heeft ook, aan de hand van de inzichten die deze DPIA heeft gebracht, een praktische toets plaatsgevonden. 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 in Bijlage 3 terug te vinden. Na de bespreking van het Toetsformulier en eventuele afspraken wordt uiteindelijk een Toetsrapport met de bevindingen opgeleverd die via de Dienst Verwerkersovereenkomsten (van Kennisnet) of op de website van de leverancier gedeeld wordt (SIVON beoogt deze Toetsrapporten te delen via een afgeschermde omgeving met alle schoolbesturen).

De toetsing van de verwerkersovereenkomst van Vodix is in februari 2025 afgerond. Alle nodige verbeteringen die door SIVON zijn geconstateerd, heeft Vodix in de actuele versie (versie 1.3, 14 februari 2025) doorgevoerd. Daarmee is destijds geconcludeerd dat de verwerkersovereenkomst voldoet aan de vereisten van het Privacyconvenant Onderwijs/Edu-V en de AVG, *zie het Toetsrapport in Bijlage 3.* Tijdens deze DPIA is echter geconstateerd dat de verwerkingen behorende bij het leerlingvolgsysteem van Vodix niet terugkomen in versie 1.3 van de verwerkersovereenkomst. Daarop dient de verwerkersovereenkomst en het Toetsrapport nog aangepast te worden. *Zie hoofdstuk 19 en 20 voor de risico's en mitigerende maatregelen.*

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

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

Beoordelingskader risico's

Alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden hieronder 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 Information Commissioner's Office (ICO)[34] om risico's te classificeren. Hierbij is 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;
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.

[34] How do we do a DPIA? | ICO

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 Vodix wordt ingezet of dat het risico het systeem zelf betreft (de applicatie). De volgorde waarin de risico's worden gepresenteerd impliceert geen prioritering naar belangrijkheid.

Tabel 19.1 Risico's

#	Risico-omschrijving	Oorzaak	Gevolg	Kans	Impact	Risico	Proces en/of systeem-risico+ verantwoordelijk
1	Er zijn ontoereikende afspraken in de verwerkersovereenkomst over de verwerking van de persoonsgegevens.	De 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.	Dit kan ertoe leiden dat persoonsgegevens niet overeenkomstig de geldende wet- en regelgeving of sectorale afspraken worden verwerkt, en vormt een risico voor de rechten en vrijheden van betrokkenen.	3	3	6	Proces Vodix en onderwijsinstelling
2	Door onbedoeld gebruik van de export en/of download functie komen er mogelijk (gevoelige) persoonsgegevens buiten de applicatie terecht, met verlies van controle over deze data als gevolg.	Exportfunctionaliteit is standaard beschikbaar zonder beperkingen en uitsluitend op klasniveau mogelijk, waardoor onbedoeld persoonsgegevens kunnen worden geëxporteerd (geen '*privacy by design*').	Dit kan leiden tot misbruik van gegevens en vormt een risico voor de rechten en vrijheden van betrokkenen.	2	3	6	Systeem en proces Vodix en onderwijsinstelling
3	Er worden onvoldoende beveiligingsmaatregelen toegepast, waardoor incidenten met persoonsgegevens niet adequaat/tijdig kunnen worden onderzocht en opgevolgd.	De loggingfunctionaliteit is ontoereikend: in de logfiles is niet te zien wie exports/downloads heeft uitgevoerd.	Dit kan leiden tot verlies van controle over persoonsgegevens en vormt een risico voor de rechten en vrijheden van betrokkenen.	2	3	6	Systeem Vodix

#	Risico-omschrijving	Oorzaak	Gevolg	Kans	Impact	Risico	Proces en/of systeem-risico+ verantwoordelijk
4	Er worden onvoldoende beveiligingsmaatregelen toegepast, wat het tijdig signaleren van ongeautoriseerde of onbedoelde wijzigingen bemoeilijken, evenals het snel onderzoeken van mogelijke incidenten.	De logfiles van wijzigingen zijn niet door de onderwijsinstelling zelf in te zien, maar uitsluitend op verzoek via Vodix.	Dit kan leiden tot onrechtmatige of ongewenste wijzigingen in persoonsgegevens die langer onopgemerkt blijven en vormt een risico voor de rechten en vrijheden van betrokkenen.	2	3	6	Systeem Vodix
5	Persoonsgegevens worden langer bewaard dan noodzakelijk, waardoor het risico op ongeoorloofde toegang, datalekken, misbruik of onrechtmatige verwerking toeneemt.	Persoonsgegevens worden langer bewaard dan voorgeschreven in sectoraal beleid en de handreiking van Kennisnet. Er zijn geen aangepaste bewaartermijnen na einde overeenkomst.	Dit kan ertoe leiden dat persoonsgegevens langer beschikbaar blijven dan noodzakelijk, waardoor de kans op ongeoorloofde toegang, datalekken of ander onrechtmatig gebruik toeneemt en daarmee een risico vormt voor de rechten en vrijheden van betrokkenen.	2	2	4	Systeem Vodix
6	Er worden onvoldoende beveiligingsmaatregelen toegepast.	Er wordt niet aantoonbaar geconformeerd aan de ISO27001 standaard, waardoor de technische maatregelen niet op effectiviteit zijn getoetst door een onafhankelijke partij.	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 Vodix
7	Er worden onvoldoende beveiligingsmaatregelen toegepast, waardoor wachtwoorden gemakkelijk zijn te kraken.	Het wachtwoordbeleid voldoet niet aan de vereisten in de NIST SP 800-63B Digital Identity Guidelines.	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 Vodix
8	Onvoldoende documentatie over de afhandeling van verzoeken van betrokkenen.	Er ontbreekt beleid en/of een werkinstructie voor het afhandelen van privacyverzoeken.	Dit kan leiden tot onjuiste of vertraagde afhandeling van verzoeken van	2	2	4	Proces Vodix

#	Risico-omschrijving	Oorzaak	Gevolg	Kans	Impact	Risico	Proces en/of systeem-risico+ verantwoordelijk
			betrokkenen en daarmee op schending van AVG-verplichtingen, en vormt een risico voor de rechten en vrijheden van betrokkenen.				
9	Er worden onvoldoende beveiligingsmaatregelen toegepast, doordat vooraf gedefinieerde maatregelen tijdens het ontwerpen van de software, niet volledig of correct in het eindproduct worden geconfigureerd.	Security requirements worden niet (altijd) getraceerd tot implementatie in code.	Dit kan leiden tot verlies van vertrouwelijkheid, misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	1	2	2	Systeem Vodix
10	Er worden onvoldoende beveiligingsmaatregelen toegepast, door gebruik te maken van YouTube-video's waarbij er gegevens doorgegeven aan een partij buiten de EU/EEA.	Er zijn Youtube-video's embed waardoor er persoonsgegevens worden doorgegeven aan Youtube.	Dit kan leiden tot het ongewenst verwerken van persoonsgegevens, mogelijk misbruik van gegevens en vormt een risico voor de rechten en vrijheden van betrokkenen.	2	1	2	Systeem Vodix
11	Er worden onvoldoende beveiligingsmaatregelen toegepast.	Het ingevulde ROSA-schema bevat geen toelichting bij de geïmplementeerde maatregelen.	Dit kan leiden tot verlies van vertrouwelijkheid, misbruik van gegevens en vormt een risico voor de rechten en vrijheden van betrokkenen.	1	2	2	Proces Vodix

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

Beschrijf hierna welke technische en organisatorische maatregelen in redelijkheid (kunnen) worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf daarbij welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Toelichting maatregelentabel:

Eigenaar maatregel: wees hierin specifiek zoals leverancier en/of schoolbestuur, wie moet maatregelen nemen of een product veranderen. Meerdere maatregelen zijn mogelijk, dus ook meerdere eigenaren. Geef toelichting welke impact de toepassing(en) heeft/hebben op het restrisico.

Indien een toelichting nodig is doe dat dan aan de hand van de nummering onder aan de maatregelentabel.

Wees zo volledig mogelijk in de maatregelentabel. Daar waar dit niet werkbaar is kan er aan de hand van de nummers een afzonderlijke toelichting gegeven worden over aspecten die samenhangen met de eigenaar maatregel, datum van implementatie en de toelichting over de aanvaardbaarheid van het restrisico.

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	Er zijn ontoereikende afspraken in de verwerkersovereenkomst over de verwerking van de persoonsgegevens. (verwerkersovereenkomst)	6	1.1 Het toevoegen van de verwerkingen en categorieën persoonsgegevens die onder het leerlingvolgsysteem vallen. 1.2 Het aanpassen van de bewaartermijnen, na uitvoering van maatregel. (organisatorisch)	Vodix en onderwijsinstelling	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Uiterste datum gereed eind september 2026.

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (Leverancier / school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum) maatregel geïmplementeerd?
			Voorgestelde wijzigingen in het Toetsformulier zijn doorgevoerd op 20 februari 2025. 1.3 Het tekenen van, zodra er een nieuwe versie beschikbaar is, de laatste versie van de verwerkersovereenkomst door de scholen.				
2	Door onbedoeld gebruik van de export en/of download functie komen er mogelijk (gevoelige) persoonsgegevens buiten de applicatie terecht, met verlies van controle over deze data als gevolg. (exporteren/downloaden by default aan)	6	2.1 Het implementeren van een deactivatie-knop voor exporteren, waar bij de standaardinstelling op 'uit' staat. 2.2 Het implementeren van een waarschuwingsvenster voor het exporteren van data 2.3 Het inventariseren van de behoefte aan exports op leerlingniveau. Indien deze aanwezig is, dit mogelijk maken. (technisch) 2.4 Het door de scholen maken van afspraken over het maken en gebruiken van exports en hier controle op uitoefenen. (organisatorisch)	Vodix en 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.
3	Er worden onvoldoende beveiligingsmaatregelen toegepast,	6	3. Het uitbreiden van de loggingfunctionaliteit met inzicht in	Vodix	0	Er is na het doorvoeren van de	Op de ontwikkelagenda geplaatst.

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (Leverancier / school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum) maatregel geïmplementeerd?
	waardoor incidenten met persoonsgegevens niet adequaat/tijdig kunnen worden onderzocht en opgevolgd. (loggingfunctionaliteit)		welke gebruikers exports/downloads hebben uitgevoerd, alsmede wie mutaties in cijfers heeft uitgevoerd. (technisch)			maatregelen geen restrisico.	Uiterste datum gereed eind juni 2026.
4	Er worden onvoldoende beveiligingsmaatregelen toegepast, wat het tijdig signaleren van ongeautoriseerde of onbedoelde wijzigingen bemoeilijkt, evenals het snel onderzoeken van mogelijke incidenten. (toegang tot loggingfunctionaliteit)	6	4.1 Scholen zelf toegang geven tot logging, zodat men zelfstandig kan monitoren. (technisch) 4.2 Het door de scholen maken van afspraken over controle op de logging. (organisatorisch)	Vodix en onderwijsinstelling	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Op de ontwikkelagen da geplaatst. Uiterste datum gereed eind maart 2027.
5	Persoonsgegevens worden langer bewaard dan noodzakelijk, waardoor het risico op ongeoorloofde toegang, datalekken, misbruik of onrechtmatige verwerking toeneemt. (bewaartermijnen)		5.1 Het aanpassen van de bewaartermijnen in lijn met sectoraal beleid en de handreiking van Kennisnet. 5.2 Het inkorten van bewaartermijnen na einde overeenkomst (2 á 3 maanden). (technisch) 5.3 Het, op initiatief van de onderwijsinstelling, inkorten van bewaartermijnen zodat deze aansluiten op de praktijk.	Vodix en onderwijsinstelling	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Op de ontwikkelagen da geplaatst. Uiterste datum gereed eind juni 2026.

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (Leverancier / school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum) maatregel geïmplementeerd?
6	Er worden onvoldoende beveiligingsmaatregelen toegepast. (audits)	3	6. Het uitvoeren van aantoonbare audits op het interne ISMS van Vodix, of certificering ISO 27001. (technisch)	Vodix	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Periodieke interne controles bij Vodix zijn reeds ingeregeld. ISO 27001 wordt overwogen.
7	Er worden onvoldoende beveiligingsmaatregelen toegepast, waardoor wachtwoorden gemakkelijk zijn te kraken. (wachtwoordbeleid)	3	7.1 Het aanpassen van het wachtwoordbeleid in lijn met de vereisten in de NIST SP 800-63B Digital Identity Guidelines. (technisch) 7.2 Het door de scholen inregelen van een proces in voor het veilig beheren en bewaren van hun wachtwoorden (organisatorisch)	Vodix en onderwijsinstelling	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Uiterste datum gereed eind juni 2026.
8	Onvoldoende documentatie over de afhandeling van verzoeken van betrokkenen. (beleid rechten van betrokkenen)	4	8. Het ontwikkelen van beleid/werkinstructie omtrent de rechten van betrokkenen. (organisatorisch)	Vodix	1	Er is na het doorvoeren van de maatregelen een minimaal en aanvaardbaar restrisico.	Beleid is opgeleverd op 11 september 2025.
9	Er worden onvoldoende beveiligingsmaatregelen toegepast, doordat vooraf gedefinieerde maatregelen tijdens het ontwerpen van de software, niet volledig of correct in het eindproduct worden geconfigureerd. (configuratie beveiligingsmaatregelen)	2	9. Het treffen van aanvullende beveiligingsmaatregelen ter voorkoming van ‘Insecure Design’. (technisch)	Vodix	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Integreren security requirements tracibility integreren in Software Development Lifecycle (SDLC) gereed eind september 2026. De overige maatregelen worden overwogen.

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (Leverancier / school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum) maatregel geïmplementeerd?
10	Er worden onvoldoende beveiligingsmaatregelen toegepast, door gebruik te maken van YouTube-video's waarbij er gegevens doorgegeven aan een partij buiten de EU/EEA. (YouTube-video's)	2	Geen aanvullende maatregelen vereist. De verwerking vindt plaats binnen de door YouTube aangeboden privacy-enhanced modus, waarmee tracking en profilering worden voorkomen en het resterende risico als laag wordt aangemerkt.	Vodix	2	Er is na het doorvoeren van de maatregelen een minimaal en aanvaardbaar restrisico.	n.v.t.
11	Er worden onvoldoende beveiligingsmaatregelen toegepast. (toelichting ROSA-schema)	2	11. Het toevoegen van een toelichting bij de geïmplementeerde maatregelen in het ROSA-schema. (organisatorisch)	Vodix	0	Er is na het doorvoeren van de maatregelen geen restrisico.	Uiterste datum gereed is gelijk aan periode (+/- 2 maanden) na vaststelling nieuw ROSA-schema.

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 [SYSTEEM] 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.		

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
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.		

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
3	Het bestuur zal de DPIA van Entree Federatie minimaal eens per drie jaar herbeoordelen.		
4	Het bestuur houdt rekening met dataminimalisatie voor verwerken van persoonsgegevens in de applicatie.		
7	Het bestuur zorgt ervoor dat persoonsgegevens na afloop van de bewaartermijn daadwerkelijk worden geschoond en heeft hier een procedure voor.		
8	Het bestuur voldoet aan het transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over de toepassing van Vodix.		
13	Er is een functioneel beheerder aangewezen voor Vodix.		

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

Risico	**Te nemen maatregel**	**Uitgevoerd ja/nee**	**Opmerking/toelichting**
Er zijn ontoereikende afspraken in de verwerkersovereenkomst over de verwerking van de persoonsgegevens.	Het tekenen van de laatste versie van de verwerkersovereenkomst, zodra deze beschikbaar is.		
Informatie van leerlingen wordt buiten systeem om gedeeld door handmatige exports, printjes en via onbeveiligde mails of usb-sticks uitgewisseld.	Het gebruik van de exports van cijfers van leerlingen buiten de applicatie beperken.		
Er worden meer persoonsgegevens vastgelegd dan noodzakelijk.	Het gebruiken van de vrije tekstvelden uitsluitend voor informatie/gegevens die strikt noodzakelijk zijn.		

Risico	Te nemen maatregel	Uitgevoerd ja/nee	Opmerking/toelichting
Verwerkingsverantwoordelijke beschikt niet over een register van verwerkingsactiviteiten.	Het bijhouden van een verwerkingsregister, waarbij indien nodig Vodix wordt geraadpleegd.		
Er worden meer of andere cookies geplaatst dan waarover de betrokkenen zijn geïnformeerd.	De betrokkenen (leerlingen) voldoende informeren over de verwerking van persoonsgegevens, waaronder cookiegegevens.		
Tweefactorauthenti-catie (2FA) wordt ondersteund, maar niet afgedwongen waardoor er ook zonder 2FA kan worden ingelogd.	Het standaard aanzetten van 2FA voor gebruik van de applicatie door leraren en leerlingen.		
Kennis over applicatiebeheer bovenschools is belegd bij één persoon en verder niet vastgelegd.	Het beleggen van het beheer van de applicatie bij meer dan één persoon en het vastleggen van overdrachtsdocument en indien noodzakelijk.		
Er worden onvoldoende beveiligingsmaatregelen toegepast, waardoor wachtwoorden gemakkelijk zijn te kraken.	Het inregelen van een proces over het veilig beheren en bewaren van wachtwoorden.		
Persoonsgegevens worden langer bewaard dan noodzakelijk, waardoor het risico op ongeoorloofde toegang, datalekken, misbruik of onrechtmatige verwerking toeneemt.	Het inkorten van de bewaartermijnen zodat deze aansluiten op de praktijk, door een verzoek bij Vodix in te dienen.		

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 Vodix 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 [Vodix] 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 Vodix.

[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 RESTRISICO	**kans**		**impact**		**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 kennisgenomen 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 leerlingen en medewerkers in Vodix - 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 Vodix 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 [SYSTEEM], 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 [SYSTEEM]. 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 Vodix liggen, terwijl deze aanbevelingen cq. maatregelen in beeld zijn gekomen bij deze DPIA en/of wel bijdragen aan het beperken van risico's:

A. …

B. …

J. Verklaring schoolbestuur

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

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

EN BESLUIT [NA (HER)OVERWEGING] HET GEBRUIK VAN VODIX [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[35] zwaardere eisen gesteld aan de beveiliging van de gegevens.

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

[35] 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[36].

[36] 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.

Laag	Midden	Hoog
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

Bijlage 3: Toetsrapport Verwerkersovereenkomst Vodix

Zie volgende pagina's voor Bijlage 3.

Toetsrapport Verwerkers-overeenkomst

VODIX
DIGITALE LEERMIDDELEN VO [VERSIE 1.3 | 14-02-2025]

19 februari 2025 ☑ THEORETISCHE TOETS | ☐ PRAKTISCHE TOETS

Wat, waarom en hoe

WAT:

Het toetsen van verwerkersovereenkomsten vindt op twee niveaus plaats:

- **Theoretisch:** op verschillen ten opzichte van de huidige Model verwerkersovereenkomst (versie 4.0 van het Privacyconvenant Onderwijs en versie 4.1 van Edu-V) en de AVG (voor leveranciers die niet zijn aangesloten).
- **Praktisch:** op verschillen tussen theorie en praktijk; deze toets is standaard onderdeel van een DPIA. *Voorbeeld: Klopt de opsomming van persoonsgegevens in de verwerkersovereenkomst wel met persoonsgegevens in de applicatie?*

WAAROM:

- Om onderwijsinstellingen te ontlasten en te helpen;
- Om leveranciers te ontlasten en te helpen;
- Voor een gestandaardiseerde werkwijze (iteratief);
- Om (zo nodig) de vereisten bij de Model-bijlagen te verbeteren;
- Voor goede afspraken voor alle betrokkenen.

Kortom: Samen voor Digitaal Veilig Onderwijs!

Het toetsen van verwerkersovereenkomsten maakt deel uit van het programma Digitaal Veilig Onderwijs.

HOE:

LET OP:

Toetsrapporten worden standaard opgesteld op basis van alleen de theoretische toets (Stap 1). Bij een DPIA wordt altijd ook een praktische toets (Stap 2) uitgevoerd, en daarmee wordt een volledig Toetsrapport opgesteld.

LEGENDA:

✗ : Niet conform vereisten, dus inclusief toelichting.
✓ : (Nog) niet geheel conform vereisten, en inclusief toelichting/afspraken.
✓ : Wel conform vereisten, dus zonder toelichting tenzij er wijzigingen zijn tov de vorige versie.

Toets
Verwerkersovereenkomst obv Model 4.1

- **Verwerkersovereenkomst conform Edu-V Model verwerkersovereenkomst 4.1**

- **Naam / Versie / Datum aangeboden verwerkersovereenkomst**

- **Ondergetekende - Verwerker: naam, juridische entiteit, KvK-nummer, tekenbevoegde**

- **Overwegen het volgende: verwijzing onderliggende overeenkomst en benoeming product/dienst**

- **Verschillen geconstateerd tov Edu-V Model verwerkersovereenkomst 4.1?**

  TOELICHTING:

  Er zijn geen verschillen geconstateerd.

- **Zo ja, opgenomen in Bijlage 3: Wijzigingenbijlage**

Toets bijlage 1:
Privacybijsluiter [1.3 | 14-02-2025]

A. Contactgegevens Verwerker en Onderwijsinstelling

- **Functie contactpersonen**
- **Contactgegevens (e-mailadres, telefoonnummer)**

B. Versienummer en versiedatum

- **Het meest recente versienummer van de Privacybijsluiter en de datum daarvan worden hier vastgelegd**

C. Algemene informatie

- **Naam product en/of dienst**
- **Naam Verwerker en vestigingsgegevens**
- **Link naar Leverancier (website/URL)**
- **Link naar productpagina (website/URL)**
  TOELICHTING:
  Links naar de verschillende productpagina's staan netjes bij 1.
- **Beknopte uitleg en werking product en/of dienst**
- **Doelgroep (po/vo/(v)so/mbo)**
- **Gebruikers (Onderwijsdeelnemers/ouders/verzorgers/medewerkers)**

D. Omschrijving specifieke producten en/of diensten

- **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;**
  TOELICHTING:
  Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de vereisten. > In plaats van een onderscheid tussen onlosmakelijke en optionele producten/diensten en verwerkingen is er een onderscheid gemaakt in Doeleinden.
- **b. omschrijving van aanvullende optionele producten en/of diensten en bijbehorende Verwerkingen die de Verwerker aanbiedt, inclusief de koppelingen en uitwisseling met derde partijen.**

TOELICHTING:

Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de vereisten. > In plaats van een onderscheid tussen onlosmakelijke en optionele producten/diensten en verwerkingen is er een onderscheid gemaakt in Doeleinden.

E. Doeleinden voor het verwerken van Persoonsgegevens

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.

TOELICHTING:

Doeleinden zoals vastgelegd in artikel 5 van het Convenant zijn in de nieuwe versie 1-op-1 opgenomen.

F. Categorieën Persoonsgegevens inclusief bewaartermijnen

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

TOELICHTING:

Categorieën betrokkenen en persoonsgegevens ontbraken maar zijn in de nieuwe versie ingevuld.

2. door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen).

TOELICHTING:

Er wordt in de nieuwe versie voldoende rekening gehouden met bewaartermijnen conform artikel 12.1 en 12.2.

G. Locatie van opslag en Verwerking Persoonsgegevens

Onder G. wordt vastgelegd wat de plaats(en)/land(en) van opslag en Verwerking van de Persoonsgegevens zijn.

TOELICHTING:

Leverancier gebruikt het goedgekeurde MEVW-branchemodel, dat afwijkt van de vereisten. > Verbinding met Verwerkingen (ofwel Producten/Diensten) ontbreekt. Er is in plaats daarvan een verbinding met Doeleinden gemaakt.

H. Subverwerkers

Verwerker legt hier vast van welke Subverwerkers hij ten tijde van het afsluiten van de Verwerkersovereenkomst gebruikmaakt.

TOELICHTING:

Er is inzicht gegeven in welke persoonsgegevens worden verwerkt door Subverwerkers.

Toets bijlage 2:
Beveiligingsbijlage [1.3 | 14-02-2025]

Het meest recente versienummer van deze bijlage en de datum daarvan worden hier vastgelegd.

A. Maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking.

- Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast.
- Verwerker neemt maatregelen zodat via een systeem van autorisatie enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.
- Verwerker heeft een coördinator voor informatiebeveiliging om risico's omtrent de verwerking van Persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Verwerker heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.
- Verwerker sluit met medewerkers geheimhoudingsverklaringen af en maakt informatiebeveiligingsafspraken.
- Verwerker stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging.

B. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen.

- Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden. Verwerker gebruikt hiervoor in

beginsel het 'Certificeringsschema informatiebeveiliging en privacy ROSA' (te vinden op www.edustandaard.nl) als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy.

- **Toetsvorm**
- **Uitvoerder toets**
- **Inlogpagina**
  TOELICHTING:
  De inlogpagina's waren in de eerdere versie niet opgenomen. Nu staat er een mooi overzicht per product/dienst. Alle domeinen van deze webapplicaties voldoen aan moderne en veilige internetstandaarden (scoren 100% op Internet.nl)!
- **BIV-classificatie**
- **Categorie**
- **Beschikbaarheid**
- **Integriteit**
- **Vertrouwelijkheid**

C. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

- **Verwerker heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zal Verwerker de Verwerkingsverantwoordelijke de volgende informatie ter hand stellen:**
- **De kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk; samenvatting van de inbreuk, waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (op welk onderdeel van de beveiliging heeft het betrekking, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van Persoonsgegevens).**
- **De oorzaak van de inbreuk;**

- Hoe de inbreuk is ontdekt.
- De maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen.
- Of de bij de inbreuk betrokken Persoonsgegevens versleuteld, gehasht etc. waren.
- De groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep(en) Betrokkenen.
- Wat de mogelijke gevolgen zijn van de inbreuk voor Onderwijsinstelling en de groep(en) Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor groep(en) Betrokkene(n).
- De hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere Persoonsgegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).
- In geval van een (vermoeden van een) beveiligingsincident en/of Datalek, kunnen Onderwijsinstelling en Verwerker, in beginsel per e-mail, contact met elkaar opnemen via onderstaande contactgegevens.
- Verwerker (naam, functie, e-mail en telefoonnummer).
- Onderwijsinstelling (naam, functie, e-mail en telefoonnummer).

Toets bijlage 3:
Wijzigingenbijlage [1.3 | 14-02-2025]

- **Het meest recente versienummer van deze bijlage en de datum daarvan worden hier vastgelegd.**

Beschrijving noodzakelijke afwijkingen Model Verwerkersovereenkomst incl. Bijlagen

- BETREFT ARTIKEL
- WIJZIGING OF AANVULLING?
- HUIDIGE TEKST ARTIKEL
- NIEUWE TEKST ARTIKEL (ONDERSTREEP WIJZIGINGEN EN AANVULLINGEN)
- REDEN VAN WIJZIGING OF AANVULLING (NOODZAAK EN MOTIVERING)

Colofon

UITGEVOERD DOOR:

SIVON (Coöperatie Samen Innoveren/Inkopen/ICT voor Onderwijs Nederland)

www.sivon.nl

ibp@sivon.nl

BETROKKENEN:

ICTRecht

Job Vos | SIVON (Senior adviseur Privacy)

Pascal Marcelis | SIVON (Projectmanager Toetsen verwerkersovereenkomsten)

Dyra Tensen | SIVON (Privacy Officer)

MET DANK AAN:

De vertegenwoordiger(s) van de leverancier VODIX: Robin van Rootseler - CTO.

SIVON