CENTRALE DPIA

ESIS

(Leverancier: Rovict B.V.)

Model versie 2.3 (juli 2026)

Rovict DPIA ESIS versie 1.0

Colofon

DPIA uitgevoerd door	Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A. (SIVON) www.sivon.nl info@sivon.nl
Betrokkenen bij uitvoering DPIA	Sander van de Molen (jurist en adviseur IBP) Susan Ashworth (adviseur IBP) Dyra Tensen (jurist en adviseur IBP) Pascal Marcelis (proj.mgr Toetsen Verwerkersovereenkomsten) Job Vos (jurist en adviseur IBP) Soufyan El Oumaoui (TISO)
Met dank aan	Team van Rovict B.V. / ESIS: Tim Doorduijn (Lead productmanagement & ontwikkeling) Barry van 't Veld (Senior Ontwikkelaar) Jos Bosten (Teamleider ICT, Spaarnesant)
Auteurs model DPIA	Hans-Peter Ligthart (portfoliomanager IBP SIVON) Job Vos (jurist en adviseur IBP SIVON) Ferdy IJsselmuiden (DPIA-projectmanager)

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

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

Versiebeheer

Datum	Versie	Wijziging
Juli 2026	0.1	1e concept DPIA-tekst
Augustus 2026	0.3	2e concept DPIA-tekst na revisie Rovict
Oktober 2026	0.4	3e concept DPIA-tekst na overleg met Rovict
November 2026	1.0	Finale versie

Inhoudsopgave

Inhoudsopgave **4**

1. Leeswijzer **6**

2. Samenvatting **7**

3. Uitleg en achtergrond DPIA **10**

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

4. Motivering DPIA ESIS **13**

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

5. Deel A: Gegevensverwerkingsanalyse **16**

1. Beschrijving van het gegevensverwerkende proces 16
2. Persoonsgegevens 16
3. Gegevensverwerkingen 19
4. Verwerkingsdoeleinden 24
5. Betrokken partijen 28
6. Belangen bij de gegevensverwerking 33
7. Verwerkingslocaties 34
8. Data Transfer Impact Assessment (DTIA) 34
9. Technieken en methoden van gegevensverwerking 34
10. Juridisch en beleidsmatig kader 37
11. Bewaartermijnen 38

6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen **41**

12. Rechtsgrond 41
13. Bijzondere persoonsgegevens 46
14. Doelbinding 47
15. Kinderrechten-afweging (Best Interests Assessment Children) 47

16 a. Noodzakelijkheid 48
16. b. Proportionaliteit en subsidiariteit 49
17. Rechten van de betrokkenen 49
18. Beoordeling verwerkersovereenkomst 51

7. Deel C: Beschrijving en beoordeling risico's voor de betrokkenen 52
Beoordelingskader risico's 52
19. Risico's 53

8. Deel D: Beschrijving voorgenomen maatregelen 55
20. Maatregelen 56

9. Deel E: MODEL lokale DPIA 58
A. Uitvoering lokale DPIA 58
B. Overwegingen over centrale DPIA 58
C. Organisatiespecifieke- en algemene applicatierisico's 58
D. Overwegingen implementatie en lokale DPIA: aanvullende risico's en maatregelen 63
E. Verklaring en advies functionaris voor gegevensbescherming (FG) 64
F. Visie betrokkenen 65
G. Conclusie 65
H. Risico-mitigerende maatregelen **schoolbestuur** 65
I. Aanbevelingen 65
J. Verklaring schoolbestuur 66
Bijlage 1: Gebruikte termen en definities 67
Bijlage 2: Uitleg risico's 69
Bijlage 3: Toetsrapport verwerkersovereenkomst 71

1. Leeswijzer

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

Hoofdstuk 1 betreft deze leeswijzer.

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

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

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

De uitvoering van de DPIA bestaat uit de volgende onderdelen:

- Hoofdstuk 5: deel A bevat de gegevensverwerkingsanalyse (beschrijving van de gegevensverwerkingen).
- Hoofdstuk 6: deel B bevat de beoordeling van de rechtmatigheid van de gegevensverwerkingen.
- Hoofdstuk 7: deel C bevat de beschrijving en beoordeling van de risico's.
- Hoofdstuk 8: deel D bevat de beschrijving van de 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.

2. Samenvatting

Deze DPIA heeft betrekking op het *leerlingadministratie-* en *leerlingvolgsysteem* ESIS. ESIS wordt geleverd door Rovict B.V. (hierna Rovict) en wordt gebruikt door ruim 1.000 scholen, ongeveer 15% van het Nederlandse primaire onderwijs.

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

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

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

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

<u>Samenwerking</u>
De samenwerking tijdens het DPIA-proces met Rovict als leverancier van ESIS was positief en constructief. De open werkwijze, goede besprekingen over de inhoud en gemotiveerde houding om verbetervoorstellen te overwegen hebben bijgedragen aan het onderzoek en identificatie van de risico's. Diverse inhoudelijke besprekingen van met name technische aard, in het kader van het ROSA-schema en bijbehorende beveiligingsmaatregelen, hebben ertoe geleid dat Rovict gedurende het DPIA-traject een groot aantal verbeterpunten heeft doorgevoerd. Dit betrof onder andere het aanpassen van de frequentie van testen (pentesting en recovery-testen) en het opzetten van een aantoonbaar gedocumenteerde procedure voor opvolging van de bevindingen hieruit. Ook wordt het gebruik van de niet-beveiligde mailfunctionaliteit uitgefaseerd. Verder is de frequentie van opschoning verhoogd tot wekelijks en is ook het standaard tonen van het BSN van leerlingen verwijderd, net als optionele velden zoals Gedoopt en Gezindte.

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

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

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

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

Risico's en maatregelen

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

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

1. Risico:
Wijziging van logfiles is mogelijk door root-admins, er wordt geen priviledged access management toegepast.

Maatregel:
Rovict: Voert een alternatief protocol in om melding en vastlegging van wijzigingen te borgen.

2. Risico:
Er is maar één bewaartermijn mogelijk in ESIS, geen mogelijkheid tot splitsing conform wettelijke vereisten.

Maatregel:
Rovict: Voegt de mogelijkheid toe om meerdere bewaartermijnen toe te passen.

3. Risico:
Nog niet alle kolommen in de database zijn versleuteld (encrypted).

Maatregel:
Rovict: Voert de versleuteling door op alle vereiste kolommen in de database.

4. Risico:
Voor bestaande klanten wordt geen 2FA voor beheerders en andere gebruikers by default afgedwongen (bij nieuwe klanten is dat wel het geval).

Maatregel:
Rovict: Wijst bestaande klanten op mogelijkheid van 2FA-gebruik.

Onderwijsinstelling: Interne afspraken maken om 2FA verplicht te gebruiken.

5. Risico:
Gegenereerde exports kunnen zonder beperking als bijlage vanuit ESIS gemaild worden, via een onbeveiligde mailfunctionaliteit.

Maatregel:
Rovict: Verwijdert de gehele mailfunctionaliteit op termijn.

Onderwijsinstelling: Zolang mailen nog mogelijk is, afspraken maken dat er niet gemaild mag worden met bijlages vanuit ESIS.

6. Risico:
Onnodige verplichte uitvraag geboortejaar medewerker.

Maatregel:
Rovict: Het veld wordt automatisch gevuld met fictieve datum 1-1-1990. De hele HR-functionaliteit, waar dit onderdeel van is, wordt op termijn uitgefaseerd.

Onderwijsinstelling: Interne afspraken maken dat het automatisch gegenereerde geboortejaar niet gewijzigd mag worden.

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 zorgvuldig met hun gegevens omgaan en de privacy waarborgen.

Privacy is enerzijds het recht om met rust te worden gelaten en 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 daarmee een randvoorwaarde in een democratische samenleving. Daarom blijft het belangrijk dat scholen privacy goed organiseren. Het beschermen van privacy gaat niet zonder het beschermen van persoonsgegevens: gegevens van betrokkenen mogen immers niet in verkeerde handen vallen. Daarom spreken we vaak over IBP: Informatiebeveiliging en privacy.

2. Privacyconvenant en toetsing verwerkersovereenkomsten

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

Scholen kunnen gemakkelijk verwerkersovereenkomsten goedkeuren en digitaal ondertekenen met behulp van de Dienst Verwerkersovereenkomsten van Kennisnet[2]. SIVON toetst voor het primair en voortgezet onderwijs vooraf of de verwerkersovereenkomsten van leveranciers van de meest gebruikte applicaties voldoen aan de eisen van het Privacyconvenant[3]. Deze rapportages zijn onder andere beschikbaar in de Dienst Verwerkersovereenkomsten. In deze DPIA is een theoretische en praktische toets op de verwerkersovereenkomst opgenomen. Zie hiervoor Hoofdstuk 18.

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 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

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

mitigerende maatregelen genoemd. Als de hoge risico's niet weggenomen kunnen worden, dan mag volgens de AVG deze verwerking (gebruik applicatie) niet worden uitgevoerd of voortgezet.

De uitkomst van de DPIA is onder andere 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 vastgelegd 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, ouders en medewerkers. Ook is het mogelijk dat het uitvoeren van een DPIA verplicht is volgens de regels van de privacytoezichthouder Autoriteit Persoonsgegevens (AP) die een lijst gepubliceerd met verwerkingen waarvoor het uitvoeren van aan DPIA verplicht is[4]. In het onderwijs betekent dit dat een DPIA vrijwel[5] altijd verplicht is op tenminste het leerlingadministratie- en/of -volgsysteem (LAS/LVS) zoals ESIS, personeelsadministratiesysteem en breed ingezette applicaties met digitaal leermateriaal. Ook de EDPB[6] benadrukt dit:

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

5. Centrale en lokale DPIA

Bij applicaties die door veel verwerkingsverantwoordelijken op dezelfde wijze worden gebruikt is het zinvol om deze DPIA samen uit te voeren, denk bijvoorbeeld aan een leerlingadministratiesysteem, zoals ESIS. Dit voorkomt dat ieder schoolbestuur afzonderlijk dezelfde analyse moet uitvoeren. SIVON voert daarom in opdracht van OCW namens het primair en voortgezet onderwijs **centrale DPIA's** uit. Deze DPIA's worden door SIVON uitgevoerd namens een aantal schoolbesturen (leden) als verwerkingsverantwoordelijke(n). Door hierbij samen op te trekken met verschillende schoolbesturen die hun ervaring uit de onderwijspraktijk meebrengen, wordt expertise en ervaring samengebracht. Ook is het makkelijker om afspraken te maken met de leverancier als er aanvullende mitigerende maatregelen moeten worden getroffen, omdat SIVON namens de leden spreekt. Door deze centrale DPIA's uit te voeren op systemen die veel

[4] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf

[5] De Autoriteit Persoonsgegevens heeft op 24 juni 2026 een conceptlijst gepubliceerd waarop verwerkingen zijn opgenomen, waarbij er geen DPIA hoeft te worden uitgevoerd. Het betreft verwerkingen voor (1) 'verwerking van persoonsgegevens van werknemers' en (7) 'verwerkingen door onderwijsinstellingen'. Deze zijn slechts van toepassing voor verwerkingsverantwoordelijken die beroepsbeoefenaar zijn of een andere natuurlijke persoon zonder dienstverband, of werkgever zijn met maximaal 250 werknemers, en die op het grondgebied van het Europese deel van Nederland (hierna: Europees Nederland) hun werkzaamheden uitvoeren. Voor wat betreft het onderwijs is er aanvullend sprake van een vrijstelling voor alleen verwerkingen die worden uitgevoerd door onderwijsinstellingen met betrekking tot de gegevens van leerlingen aangaande het beheer van hun persoonsgegevens, voor zover de verwerking geschiedt met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is. Hierbij geldt dat de voorwaarde dat de verwerking geen andere bijzondere categorieën van persoonsgegevens betreft zoals bedoeld in artikel 9, eerste lid, AVG en dat artikel 9, tweede lid, sub d, AVG niet van toepassing is.

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

gebruikt worden, 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 voor hen doen. Na de uitvoering van de centrale DPIA moet daarom ieder schoolbestuur de uitkomsten van 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 het eventuele aanvullende risico's en bepaalt het zelf of er nog mitigerende maatregelen moeten worden genomen.

SIVON helpt besturen door in de centrale DPIA de meest voorkomende risico's voor schoolbesturen vast te leggen. 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[7], aangevuld met onderwijs-specifieke informatie uit de voormalige: *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0).* 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)"[8].

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 beveiliging en (web)technologieën;
- Analyse van de wijze waarop het systeem voorziet in logging en de wijze waarop dit door de onderwijsinstelling gemonitord en gecontroleerd kan worden;
- Overleg met betrokken schoolbesturen en leverancier over (aanvullende) mitigerende maatregelen;
- Opstellen en bespreken DPIA-rapportage.

7. Funderend onderwijs referentie architectuur (FORA)

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

[7] Model DPIA Rijksdienst v3.0.pdf (kcbr.nl)
[8] https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_nl.pdf

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 informatie-huishouding vragen (Norm GO.04 informatiearchitectuur van het Normenkader IBP[9]).

Voor het funderend onderwijs is de FORA (Funderend Onderwijs Referentie Architectuur) ontwikkeld[10]. De FORA is een gestandaardiseerde methodiek die inzicht geeft in verplichte processen en onderwijsactiviteiten in het primair en voortgezet onderwijs. De FORA biedt inzicht in wat de bedrijfsfuncties zijn van een po- en vo-school. Het hoofdbedrijfsfunctiemodel beschrijft op hoofdlijnen wat een onderwijsorganisatie doet. Deze beschrijving wordt verdiept in het bedrijfsfunctiemodel, waarin nader wordt uitgewerkt hoe invulling wordt gegeven aan deze activiteiten. Op basis daarvan is het mogelijk om 'referentiecomponenten' toe te voegen. Referentiecomponenten zijn typen systemen, zoals een LAS, een Toetssysteem, of een ELO, met bijbehorende functionaliteiten ('applicatiefuncties').

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

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

4. Motivering DPIA ESIS

1. Verplichting uitvoeren DPIA

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

Bij het onderzoek naar het LAS/LVS ESIS (van leverancier Rovict B.V., hierna Rovict) is gebleken dat het uitvoeren van een DPIA verplicht is op grond van onder meer artikel 35 AVG, aangezien de verwerking van persoonsgegevens binnen het LAS/LVS aan meerdere criteria voldoet.

Er is sprake van op grote schaal verwerking van bijzondere categorieën van persoonsgegevens. Hierdoor is er sprake van een 'hoog risicoverwerking'.

Volgens het overzicht van de European Data Protection Board, de opvolger van de WP29, wordt aan vier criteria voldaan. Ook hierdoor spreken we van een 'hoog risicoverwerking'. Er is namelijk sprake van een verwerking van 'gevoelige gegevens' (1) die kunnen leiden tot 'evaluatie of scoretoekenning'(2), omdat er binnen ESIS leer- en testresultaten worden verwerkt over een langere periode en deze resultaten zichtbaar zijn voor gebruikers (leerkrachten en leerlingen). Daarnaast heeft deze verwerking van persoonsgegevens betrekking op kinderen onder de 16 jaar. Deze vorm van gegevensverwerking vereist een extra bescherming omdat het hier 'kwetsbare personen' (3) betreft. Tot slot is er sprake van 'op grote schaal verwerkte gegevens' (4) omdat binnen ESIS de gegevens van alle leerlingen (en in mindere mate van leerkrachten) worden

[9] https://normenkaderibp.kennisnet.nl/informatiebeveiliging/domein-1-bestuur/go-04-informatiearchitectuur/
[10] https://fora.wikixl.nl/index.php/Hoofdpagina
[11] https://fora.wikixl.nl/index.php/Referentiecomponentenmodel

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

Bovendien is er volgens de lijst van de Autoriteit Persoonsgegevens ook 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. Daarnaast is er sprake van '7. Gezondheidsgegevens'. Dit gaat over grootschalige verwerkingen van gegevens over gezondheid door o.a. (speciaal)onderwijsinstellingen. Ook het voldoen aan deze criteria stelt het uitvoeren van een DPIA verplicht.

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

2. Scope van deze DPIA

Deze DPIA heeft betrekking op het digitale leerlingadministratie- (LAS) ESIS-A en leerlingvolgsysteem (LVS) ESIS-B, dat door Rovict als leverancier wordt geleverd aan scholen voor primair en speciaal (basis)onderwijs.

ESIS-A omvat:

- leerlingenadministratie
  - inclusief EckID opslag
- Inrichting
  - Bestuur/school
  - Groepen
  - Medewerkers
  - Rollen en rechten
  - Hulptabellen

ESIS-B omvat:

- Leerlingdossiers
  - summatief
  - formatief[12]

ESIS-A en ESIS-B vormen samen een digitale oplossing om onderwijsinstellingen te ondersteunen bij hun administratieve taken rondom aanmeldingen, inschrijvingen, studievoortgang, leerlingbegeleiding en kwaliteitszorg.

In deze DPIA richten we ons alleen op de functionaliteit zoals hierboven aangegeven (gezamenlijk: ESIS) en de mogelijke risico's die het gebruik van dit digitale leerling- en onderwijsvolgsysteem met zich meebrengt.

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

3. Buiten scope

Rovict biedt middels ESIS de mogelijkheid om de basisfunctionaliteit uit te breiden met diverse modules op onderwijsgerelateerde vlakken en om bijvoorbeeld koppelingen te maken met

[12] Summatief: betekent *samenvattend* of *beoordelend aan het einde*. In het onderwijs en bij beoordelingen gaat het om het meten van wat iemand heeft geleerd op een vast moment, zoals bij een eindtoets of examen. Formatief: in het onderwijs betekent formatief letterlijk 'vormend'. Het is een manier van werken waarbij het leerproces centraal staat, en niet het eindresultaat.

systemen van andere (externe) partijen. Er is uitsluitend gekeken naar de basisfunctionaliteit van ESIS en dus niet naar de optionele modules en de inhoud van andere aanleverende en afnemende koppelingen.

Er is dus expliciet niet gekeken naar modules zoals Schoolrapporten, Groepsplannen en Kompas. Deze zijn geen onderdeel van de basisfunctionaliteit van ESIS.

Ook de specifieke inhoud van koppelingen tussen ESIS en andere systemen zijn geen onderdeel van deze DPIA, zoals die met ESIS API (OPK), Google, Microsoft, HR-systemen, OSO, ROD en UWLR/EDU-V of andere (externe) partners.

5. Deel A: Gegevensverwerkingsanalyse

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

1. Beschrijving van het gegevensverwerkende proces

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

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

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

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

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

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

2. Persoonsgegevens

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

Betrokkenen
In ESIS worden persoonsgegevens verwerkt van leerlingen van de scholen, ouders/verzorgers van de leerlingen en van medewerkers (leerkrachten en begeleiders) van de school.

Persoonsgegevens
Binnen ESIS worden de persoonsgegevens en typen persoonsgegevens zoals aangegeven in onderstaande tabel van betrokkenen verwerkt.

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

Tabel 3.1 Persoonsgegevens

Categorie gegevens	**Specificatie**	**Betrokkenen**		
		Onderwijsdeelnemer	**Ouder/voogd / verzorger**	**Medewerker**
Contactgegevens	Voorna(a)m(en)	X	X	X
	Voorletter(s)	X	X	X
	Achternaam	X	X	X
	Geslacht	X	X	X
	Woonadres	X	X	X
	Postcode	X	X	X
	Woonplaats	X	X	X
	Telefoonnummer	X	X	X
	E-mailadres (privé)	X	X	
	E-mailadres (school)	X		X
Burgerservicenummer (BSN) of PGN	BSN/PGN	X		
Onderwijsdeelnemer-nummer	Een administratienummer dat Onderwijsdeelnemers identificeert	X		
ECK-iD		X		
Nationaliteit		X	X	X
Geboortedatum		X	X	X
Geboorteplaats		X	X	X
Financiële gegevens met het oog op het berekenen, vastleggen en innen van gelden en bijdragen	Bankrekeningnummer			X
	Facturenadministratie			X
Gegevens over gezondheid*	Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de Betrokkene of op verzoek van Betrokkene worden verwerkt, een en ander voor zover noodzakelijk voor het onderwijs	X		

Godsdienst*	Gegevens betreffende de godsdienst of levensovertuiging van de Betrokkene, voor zover die noodzakelijk zijn voor het onderwijs, of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs	X	X	
Studievoortgang	Klas / leerjaar / ILT-code	X		
	Examinering			
	Studievoortgang en/of studietraject	X		
	Begeleiding Onderwijsdeelnemers, inclusief handelingsplan	X		
	Aan- en afwezigheidsregistratie	X		
Onderwijsorganisatie	Gegevens met het oog op de organisatie van het onderwijs (zoals een rooster) en het verstrekken of ter beschikking stellen van leermiddelen	X		
Beeldmateriaal	Foto's en videobeelden (beeldmateriaal) van Betrokkene met of zonder geluid van activiteiten van de Onderwijsinstelling	X		
Gebruikersgegevens	Diagnostische gegevens, loggegevens, metadata			X
	IP-adres			X
Andere Persoonsgegevens, namelijk;	NNCA (niet-Nederlands culturele achtergrond)	X		
	OPDC (Orthopedagogisch didactisch centrum)	X		
	TLV (Toelaatbaarheidsverklaring)	X		
	COA (Centraal Orgaan opvang Asielzoekers)	X		
	Vluchtelingstatus	X		
	Tehuis	X		
	Nieuwkomersgegevens	X		
	Vervolgonderwijs	X		

	Uitstroom(profiel)	X		
	Ondersteuningsniveau	X		
	Vrije velden	X		X
	Authenticatiegegevens			X
	Wettelijk gezag, waaronder de relatie		X	

Extra invulvelden

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

Op de "Leerlingkaart" bestaat bijvoorbeeld de mogelijkheid voor onderwijsinstellingen om, naast de eerder genoemde lijst van verwerkte persoonsgegevens, ook aanvullende gegevens te verwerken, zoals het geval is als er bijvoorbeeld een veld “Vluchteling” wordt toegevoegd.

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

3. Gegevensverwerkingen

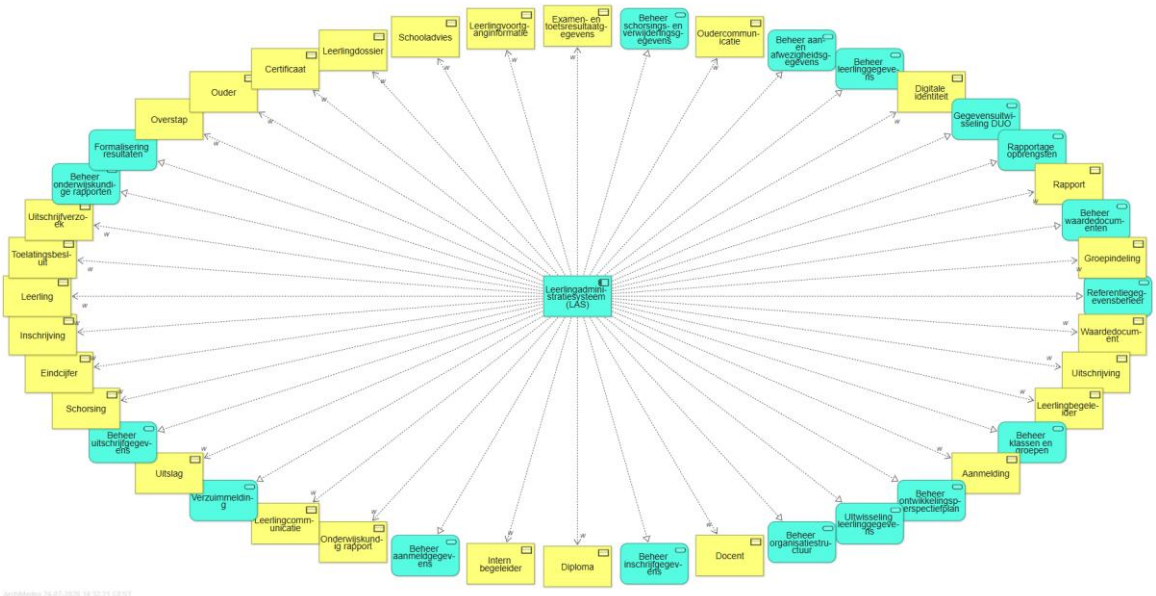
Voor het schetsen van de reikwijdte van de gegevensverwerkingsanalyse wordt gebruik gemaakt van de referentiearchitectuur (de FORA[13] voor het primair en voortgezet onderwijs).

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

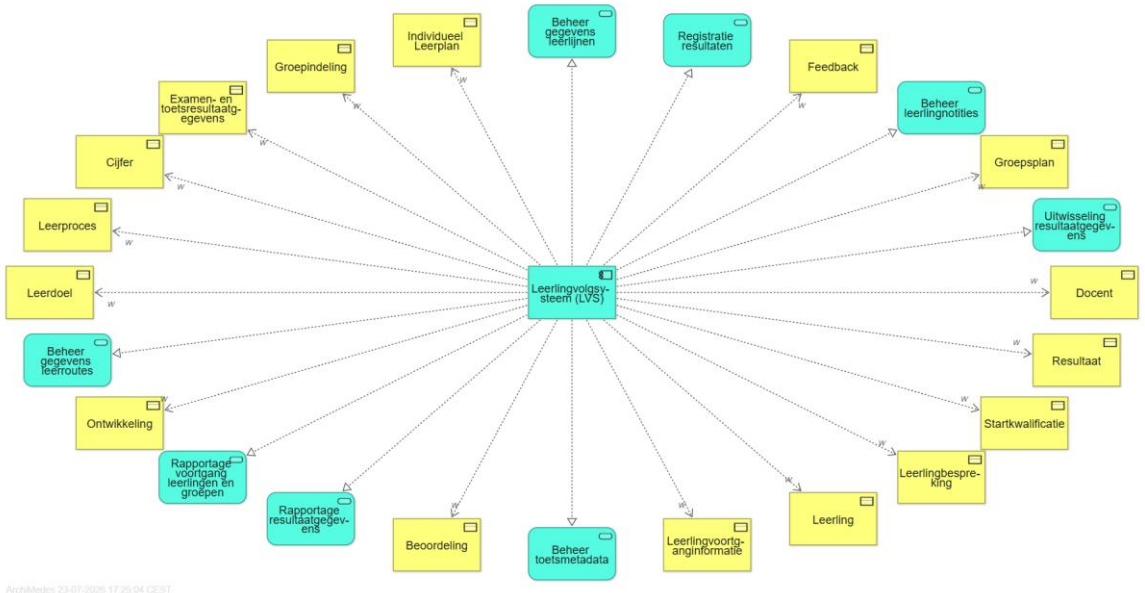
ESIS kan in termen van FORA worden geduid als:

1. Leerlingadministratiesysteem (LAS)
   (Zie Leerlingadministratiesysteem (LAS) - Funderend Onderwijs Referentie Architectuur voor vergroting van de afbeelding hieronder).

[13] https://www.wikixl.nl/wiki/fora/index.php/DPIA.



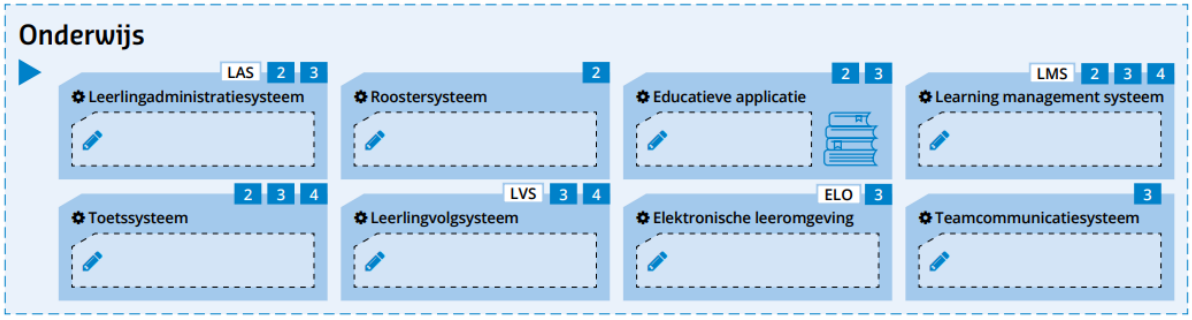
2. Leerlingvolgsysteem (LVS)
(Zie Leerlingvolgsysteem (LVS) - Funderend Onderwijs Referentie Architectuur voor vergroting van de afbeelding hieronder).



Applicatielandschap

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

Schets de applicatie in de context van het applicatielandschap, bijvoorbeeld via de FORA.

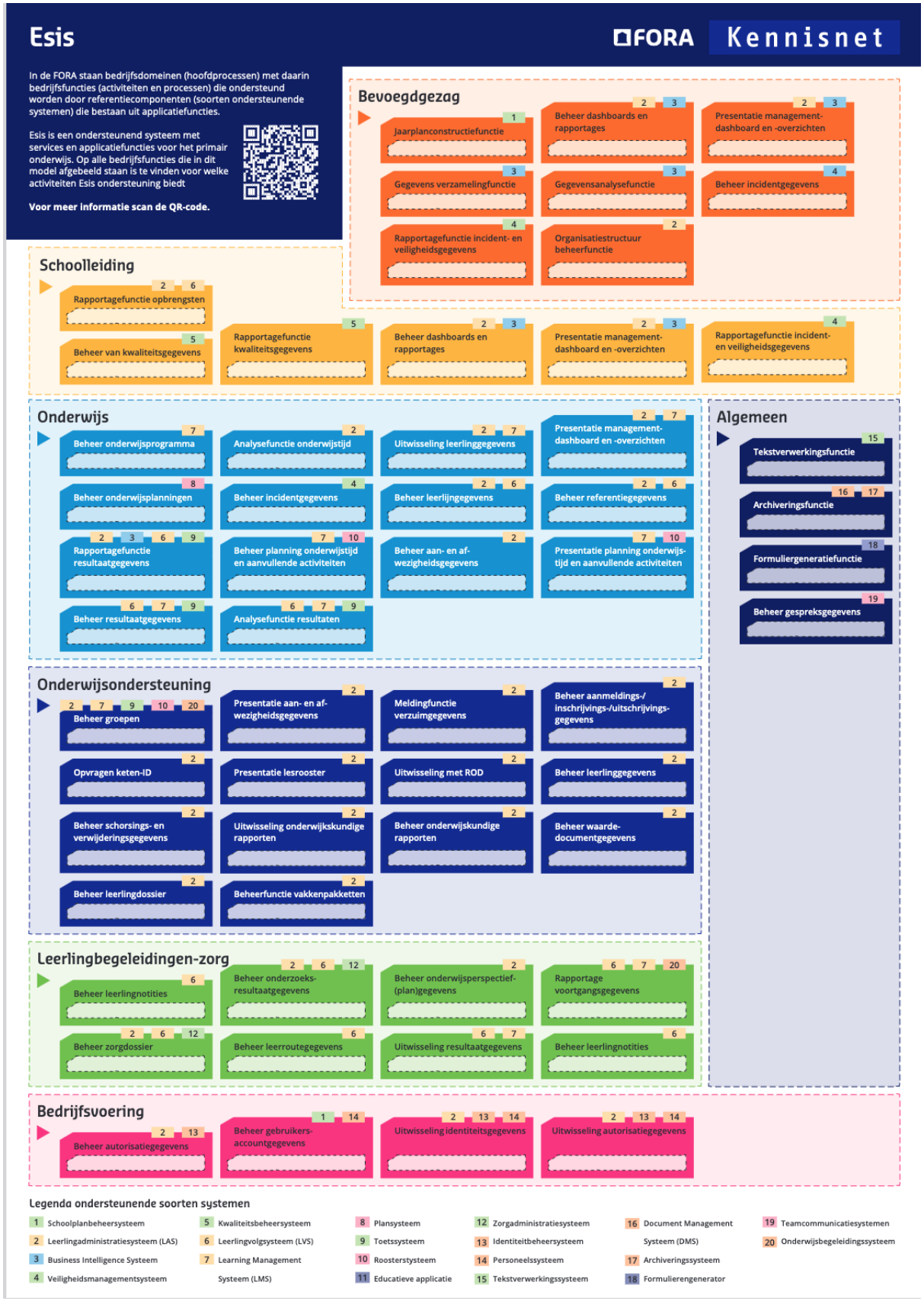


Gegevensstromen/stroomschema

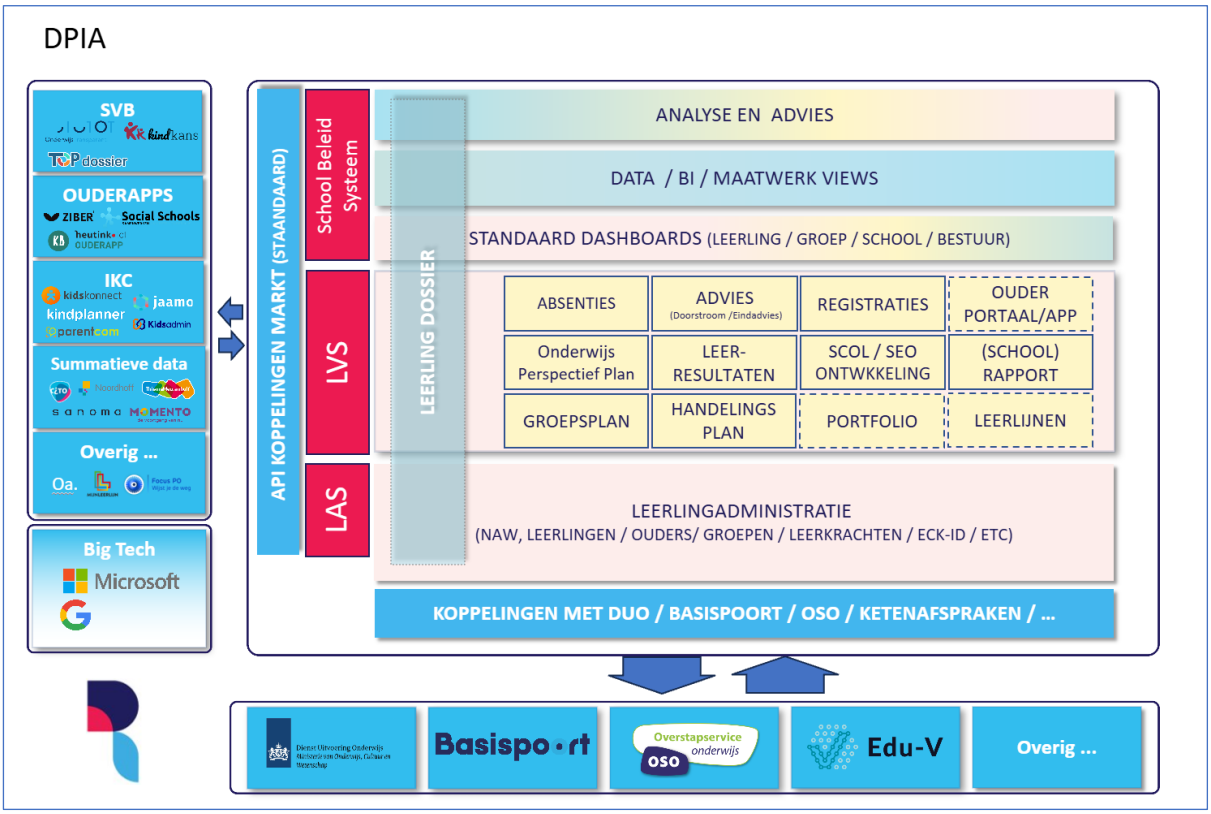
Omdat de gegevensverwerkingen gecompliceerd kunnen zijn en het niet altijd gemakkelijk is om het geheel van gegevensverwerkingen in woorden uit te drukken, is het van belang om de gegevensverwerkingen te visualiseren, aan de hand van een input-proces-output model, stroomschema of workflow.

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

Zie onderstaande afbeelding (versie juli 2023). Deze DPIA richt zich alleen op: [2] Leerlingadministratiesysteem (LAS), en [6] het Leerlingvolgsysteem (LVS).
https://fora.wikixl.nl/index.php/Esis


Esis
FORA
Kennisnet
In de FORA staan bedrijfsdomeinen (hoofdprocessen) met daarin bedrijfsfuncties (activiteiten en processen) die ondersteund worden door referentiecomponenten (soorten ondersteunende systemen) die bestaan uit applicatiefuncties.
Esis is een ondersteunend systeem met services en applicatiefuncties voor het primair onderwijs. Op alle bedrijfsfuncties die in dit model afgebeeld staan is te vinden voor welke activiteiten Esis ondersteuning biedt
Voor meer informatie scan de QR-code.
Bevoegdgezag
Jaarplanconstructiefunctie
Beheer dashboards en rapportages
Presentatie management-dashboard en -overzichten
Gegevens verzamelingfunctie
Gegevensanalysefunctie
Beheer incidentgegevens
Rapportagefunctie incident- en veiligheidsgegevens
Organisatiestructuur beheerfunctie
Schoolleiding
Rapportagefunctie opbrengsten
Beheer van kwaliteitsgegevens
Rapportagefunctie kwaliteitsgegevens
Beheer dashboards en rapportages
Presentatie management-dashboard en -overzichten
Rapportagefunctie incident- en veiligheidsgegevens
Onderwijs
Beheer onderwijsprogramma
Analysefunctie onderwijstijd
Uitwisseling leerlinggegevens
Presentatie management-dashboard en -overzichten
Beheer onderwijsplanningen
Beheer incidentgegevens
Beheer leerlijngegevens
Beheer referentiegegevens
Rapportagefunctie resultaatgegevens
Beheer planning onderwijstijd en aanvullende activiteiten
Beheer aan- en af-wezigheidsgegevens
Presentatie planning onderwijs-tijd en aanvullende activiteiten
Beheer resultaatgegevens
Analysefunctie resultaten
Algemeen
Tekstverwerkingsfunctie
Archiveringsfunctie
Formuliergeneratiefunctie
Beheer gespreksgegevens
Onderwijsondersteuning
Beheer groepen
Presentatie aan- en af-wezigheidsgegevens
Meldingfunctie verzuimgegevens
Beheer aanmeldings-/ inschrijvings-/uitschrijvings-gegevens
Opvragen keten-ID
Presentatie lesrooster
Uitwisseling met ROD
Beheer leerlinggegevens
Beheer schorsings- en verwijderingsgegevens
Uitwisseling onderwijskundige rapporten
Beheer onderwijskundige rapporten
Beheer waarde-documentgegevens
Beheer leerlingdossier
Beheerfunctie vakkenpakketten
Leerlingbegeleidingen-zorg
Beheer leerlingnotities
Beheer onderzoeks-resultaatgegevens
Beheer onderwijsperspectief-(plan)gegevens
Rapportage voortgangsgegevens
Beheer zorgdossier
Beheer leerroutegegevens
Uitwisseling resultaatgegevens
Beheer leerlingnotities
Bedrijfsvoering
Beheer autorisatiegegevens
Beheer gebruikers-accountgegevens
Uitwisseling identiteitsgegevens
Uitwisseling autorisatiegegevens
Legenda ondersteunende soorten systemen
1 Schoolplanbeheersysteem
2 Leerlingadministratiesysteem (LAS)
3 Business Intelligence Systeem
4 Veiligheidsmanagementsysteem
5 Kwaliteitsbeheersysteem
6 Leerlingvolgsysteem (LVS)
7 Learning Management Systeem (LMS)
8 Plansysteem
9 Toetssysteem
10 Roosterstysteem
11 Educatieve applicatie
12 Zorgadministratiesysteem
13 Identiteitbeheersysteem
14 Personeelssysteem
15 Tekstverwerkingssysteem
16 Document Management Systeem (DMS)
17 Archiveringssysteem
18 Formulierengenerator
19 Teamcommunicatiesystemen
20 Onderwijsbegeleidingssysteem

In onderstaand overzicht is door Rovict het landschap van ESIS uitgewerkt. Voor deze DPIA is de scope het LAS/LVS, zoals eerder aangegeven.



Koppelingen

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

Wél binnen de scope zijn de koppelingsmogelijkheden zelf die vanuit ESIS worden gefaciliteerd.

De onderwijsinstelling activeert of deactiveert zelf het koppelvlak. Hierbij wordt om een formele akkoordverklaring gevraagd aan de onderwijsinstelling. De gebruikersvoorwaarden worden hierbij beschikbaar gesteld met uitleg over de aard van de koppeling, koppelingspartner en uit te wisselen gegevens. De koppeling start pas met uitwisselen van gegevens als de onderwijsinstelling in beide systemen een identieke zelf bedachte verificatiecode heeft ingevoerd. Tevens zijn deze handelingen zichtbaar in het Koppelinglogboek en een bevestigingsemail wordt gestuurd naar de contactpersoon van de onderwijsinstelling.

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

De toegang tot ESIS kan beveiligd worden via het instellen van 2FA. Dit kan door de onderwijsinstelling als ‘default’ setting worden ingesteld. ESIS biedt dit niet zelf als ‘default setting’ aan. Daarnaast kan een beveiligde inlog via ‘Single Sign On’ (SSO) worden ingericht via een inlogkoppeling met Microsoft/SSO of Google/SSO, waar veel schoolbesturen gebruik van maken.

Op deze wijze is het ook mogelijk om via de SSO (Single Sign On) 2FA/MFA toe te passen en af te dwingen bij gebruikers.

De HR-koppeling maakt het mogelijk om voor medewerkers geautomatiseerd ESIS-accounts aan te maken en rollen toe te kennen, dan wel – bij uitdiensttreding - de toegang van een medewerker tot ESIS geautomatiseerd te sluiten. Dit is ook het geval bij wisseling van functie; de rollen en daarmee de bevoegdheden binnen ESIS worden zo geautomatiseerd bijgewerkt. Dit verhoogt het niveau van beveiligde en gecontroleerde toegang.

Adaptiviteit

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

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

De FORA[14] is gebruikt om de verwerkingsdoeleinden te bepalen.

De verwerkingsdoeleinden sluiten aan bij de in het Privacyconvenant[15] opgenomen verwerkingsdoeleinden.

a. de opslag van leer- en toetsresultaten;

b. het terugontvangen door het schoolbestuur van leer- en toetsresultaten;

c. de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer;

d. analyse en interpretatie van leer- en toetsresultaten;

e. het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen;

f. de indeling en aanpassing van roosters;

g. het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;

h. het begeleiden en ondersteunen van leerkrachten / docenten en andere medewerkers binnen het schoolbestuur;

i. de communicatie met Onderwijsdeelnemers en ouders en medewerkers van het schoolbestuur;

j. monitoring en verantwoording, met name ten behoeve van: (prestatie)metingen van het schoolbestuur, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vormen) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;

k. het voor zover noodzakelijk en wettelijk toegestaan uitwisselen van Persoonsgegevens met Derden, waaronder:

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

1. toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;
2. samenwerkingsverbanden in het kader van passend onderwijs en regionale samenwerkingen;
3. partijen betrokken bij de invulling van stage- of leer-werkplekken;
4. het leveren van Persoonsgegevens aan schoolbesturen in geval van overstappen tussen schoolbesturen en bij vervolgonderwijs;
5. het in opdracht van het schoolbestuur leveren van Persoonsgegevens aan een andere partij;

l. het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen het schoolbestuur en de Leverancier;

m. het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;

n. 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;

o. de continuïteit, verbetering en de goede werking van het Digitale Onderwijsmiddel in opdracht van het schoolbestuur conform de afspraken die zijn gemaakt tussen het schoolbestuur 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;

p. het door het schoolbestuur beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van het schoolbestuur op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek;

q. het door het schoolbestuur voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren;

r. het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen;

s. het behandelen van geschillen;

t. financieel beheer;

u. de uitvoering of toepassing van een Unierechtelijke of lidstaatrechtelijke wettelijke bepaling of regeling.

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

Tabel 4.1 Verwerkingsdoeleinden en verwerking

Doeleinde	**Code**[16]	**FORA – hoofdproces** (3. Gegevensverwerkingen)	**FORA – subproces** Toelichting
de opslag van leer- en toetsresultaten;	D1	Onderwijsevaluatie	Resultatenregistratie Beoordeling

[16] Variant-modelbijlage-1-bij-model-verwerkersovereenkomst-4_0.docx

het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten;	D2	Onderwijsevaluatie	Resultatenregistratie Beoordeling
de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer;	D3	Leerlingbegeleiding	Monitoring en begeleiding voortgang leerroute en leerproces Onderwijsbegeleiding Voortgang- en resultatenweergave Leerroutebijstelling
analyse en interpretatie van leer- en toetsresultaten;	D4	Leerlingbegeleiding	Monitoring en begeleiding voortgang leerroute en leerproces
het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen;	D5	Onderwijsevaluatie. Leerlingbegeleiding	Resultatenregistratie. Monitoring en begeleiding voortgang leerroute en leerproces
de indeling en aanpassing van roosters	D6	Onderwijsvoorbereiding	Planning en roostering
het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs;	D7	Zorgbegeleiding en -coördinatie. Leerlingbegeleiding	Vorming zorgdossier Onderwijsbegeleiding
het begeleiden en ondersteunen van leerkrachten/docenten en andere medewerkers binnen de Onderwijsinstelling;	D8	Personeel en organisatie	
de communicatie met Onderwijsdeelnemers en ouders en met medewerkers van de Onderwijsinstelling;	D9	Facilitering leerlingcommunicatie. Facilitering oudercommunicatie. Samenwerken en communiceren medewerkers en extern	
monitoring en verantwoording, met name ten behoeve van: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vormen) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs;	D10	Verantwoording	
het voor zover noodzakelijk en wettelijk toegestaan uitwisselen van Persoonsgegevens met Derden, waaronder:	D11		
o toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak;	D11	Leerlingbegeleiding en -zorg. Instroom, doorstroom, uitstroom	Organisatie passend onderwijs. Zorgbegeleiding en -coördinatie.

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

het door de Onderwijsinstelling beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek;	D16	Onderwijsevaluatie. Onderwijsvoorbereiding. Beleid en planning	Opleidingontwikkeling. Materiaalontwikkeling
het door de Onderwijsinstelling voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren;	D17	Beleid en planning	Kwaliteitszorg
het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen;	D18	Instroom, doorstroom, uitstroom	Inschrijving en leerlinggegevensbeheer
het behandelen van geschillen;	D19	Klachten en bezwaren	Registratie klachten en bezwaren. Klachtbehandeling
Financieel beheer;	D20	Financieel beheer en bekostiging	
de uitvoering of toepassing van een Unierechtelijke of lidstaatrechtelijke wettelijke bepaling of regeling;	D21		
andere doeleinden ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces) en het begeleiden en volgen van Onderwijsdeelnemers (in hun leerproces), namelijk	D22	Zelf invullen door de onderwijsinstelling aan de hand van FORA-bedrijfsfuncties	

5. Betrokken partijen

De hieronder genoemde partijen zijn betrokken bij de gegevensverwerking.

Tabel 5.1 Betrokken partijen en gegevensverwerking

Naam partij	AVG-rol	Functie/ taak	Betrokken persoons-gegevens	Verstrekker of ontvanger	De volgende personen hebben toegang tot deze pgg
Onderwijs-instelling	Verwerkings-verantwoordelijke	Beheer en toepassing van het digitaal onderwijsmiddel	Alle genoemde persoonsgegevens	Verstrekker	Directie, schoolleiders, leerkrachten, administratief medewerkers, ICT- en applicatiebeheerders, Intern begeleiders, zorgcoördinatorenen externe specialisten.
DUO/ROD	Andere Verantwoordelijke (derde)	DUO Register Onderwijsdeelnemers (ROD). Het Register Onderwijsdeelnemers (ROD) bevat leerlinggegevens van het basisonderwijs, voortgezet onderwijs, middelbaar beroepsonderwijs (mbo) en hoger onderwijs. De Dienst Uitvoering Onderwijs (Rijksoverheid) registreert beleids- en bekostigingsgegevens. ESIS is gekoppeld met o.a. de ROD.	Leerling-gegevens	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Onderwijs-inspectie	Andere Verantwoordelijke (derde)	De Onderwijsinspectie (Rijksoverheid) heeft geen directe koppeling, maar krijgt wel gegevens aangeleverd en zo nodig toegang tot ESIS ten behoeve van onderwijs toezicht.	Mogelijk: alle gegevens in de database	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Samenwerkingsverband Passend Onderwijs	Andere Verantwoordelijke (derde)	Samenwerkingsverbanden Passend Onderwijs ontvangen gegevens uit ESIS, vaak via een gezamenlijke informatievoorziening zoals Kindkans of OnderwijsTransparant	Relevante gegevens in het kader van de begeleiding en zorg van leerlingen en nadere ondersteuning	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Gemeente	Andere Verantwoordelijke (derde)	Gezondheidsdiensten (GGD/JGZ) van de gemeente en leerplichtambtenaren ontvangen gegevens over de plaatsing en	Plaatsing en aan/afwezigheid van leerlingen	Ontvanger	Geen toegang tot de persoonsgegevens in de database.

		aan- of afwezigheid van leerlingen.			
Hulp- of zorgverleners	Andere Verantwoordelijke (derde)	Het kan hierbij gaan om bijvoorbeeld orthopedagogen, schoolmaatschappelijk werkers of logopedisten die al dan niet in dienst van de school gegevens verwerken.	Noodzakelijke gegevens (inzake de gezondheid en / of begeleiding)	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Kennisnet	Verwerker	Kennisnet levert de Overstap Service Onderwijs (OSO) waarmee het leerlingdossier uitgewisseld kan worden met een andere LAS (in het PO en VO). Ook levert Kennisnet het ECK iD (pseudo-ID) aan bij het LAS via de Nummervoorziening	Onderwijskundig rapport en eventuele noodzakelijke persoonsgegevens voor de goede begeleiding en zorg omtrent leerlingen	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Uitgeverijen en Leveranciers van digitaal leermateriaal, LVS-systemen of leerplatformen (optioneel)	Andere Verantwoordelijke (derde)	Uitgeverijen ontvangen via Basispoort, een centrale voorziening voor toegang tot leermiddelen, gegevens. Daarnaast zijn er rechtstreekse koppelingen met leveranciers van leerlingvolgsystemen en leerplatformen.	Noodzakelijke gegevens voor de toegang verlening en het functioneren van leermiddelen	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Rovict B.V.	Verwerker	Aanbieder digitaal onderwijsmiddel	Alle genoemde persoonsgegevens	Ontvanger	Binnen Rovict is een autorisatiematrix vastgesteld waarbij toegang op basis van 'need to know' toegang wordt verkregen. De systeembeheerder heeft geen toegang tot de persoonsgegevens in de database, tenzij dit gebeurt op verzoek van de onderwijsinstelling. Dan wordt volgens geldende support/beveiligingsprocessen gewerkt.
Previder	Subverwerker	Hosting programmatuur en dataopslag	Alle genoemde persoonsgegevens	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Microsoft (Azure)	Subverwerker	Hosting programmatuur en dataopslag	Alle genoemde persoonsgegevens; Absentiegegev	Ontvanger	Geen toegang tot de persoonsgegevens in de database.

			ens, leerling-, groep-, medewerkersgegevens		
Synaxion	Subverwerker	Hosting management dashboard in Azure	Studievoortgang; Leerlinggegevens, tussenresultaten, eindopbrengsten, advies+uitstroomgegevens, Gebruikersgegevens	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Zendesk	Subverwerker	Helpdesk-registratie	Medewerkergegevens, contactpersonen: Naam, E-mailadres, Telefoonnummer, indien opgenomen in het supportverzoek of de correspondentie; Gegevens die door de indiener van een supportverzoek worden verstrekt: Inhoud van het supportverzoek en bijbehorende correspondentie en eventuele bijlagen; Leerlinggegevens, voor zover deze door de indiener worden verstrekt en noodzakelijk zijn voor de behandeling van het betreffende supportverzoek. Dit kan gegevens betreffen uit de categorieën leerlinggegevens zoals	Ontvanger	Geen toegang tot de persoonsgegevens in de database.

			opgenomen in tabel 1 verwerkersovereenkomst		
Posthog	Subverwerker	Gebruikersanalyse	Gebruiks- en technische gegevens, waaronder bezochte pagina's en gebruikte functionaliteiten, apparaat- en browsergegevens, IP-adres, sessiegegevens en technische identificatoren	Ontvanger	Geen toegang tot de persoonsgegevens in de database
Medewerkers	Betrokkene / geautoriseerde	Medewerkers, over het algemeen betreft dit de schoolleiding, IB-ers en de leerkrachten incl. de invallers voor langere duur.	Noodzakelijke persoonsgegevens op basis van 'need to know' en 'least privilege'.	Betrokkene / geautoriseerde	Binnen de onderwijsinstelling is een autorisatiematrix vastgesteld waarbij toegang op basis van 'need to know' toegang wordt verkregen.
Ouders/verzorgers	Betrokkene	Ouders/verzorgers van de ingeschreven leerlingen. Het kan soms ook gaan om een voogd. Of om de contactgegevens van familie, kennissen van het kind in geval van nood.	Noodzakelijke persoonsgegevens	Betrokkene	Ouders/verzorgers
Leerlingen (incl aspirant- en oud-leerlingen)	Betrokkene	Onderwijsdeelnemers die zijn ingeschreven. Het kan ook gaan om de gegevens van oud-leerlingen in het kader van bewaarplicht of alumni-activiteiten.	Alle gegevens	Betrokkene	Betrokkene
Stagiaires	Betrokkene / geautoriseerde	Bijvoorbeeld studenten die voor langere tijd aan de school zin verbonden.	Noodzakelijke persoonsgegevens op basis van 'need to know' en 'least privilege'.	Betrokkene / geautoriseerde	Binnen de onderwijsinstelling is een autorisatiematrix vastgesteld waarbij toegang op basis van 'need to know' toegang wordt verkregen.

6. Belangen bij de gegevensverwerking

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

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

Naam partij	Belangen
Onderwijsinstelling	Het hebben van een goed werkend en betrouwbaar digitaal leerlingvolg- en administratiesysteem.
DUO/ROD	Het via ROD uitwisselen door onderwijsinstellingen van gegevens van leerlingen en studenten uit met DUO, zoals inschrijvingen en diplomagegevens.
Onderwijsinspectie	Toezicht kunnen houden op de kwaliteit van het onderwijs.
Samenwerkingsverband Passend Onderwijs	Wettelijke taak uit kunnen voeren inzake passend onderwijs en juiste ondersteuning van de leerling.
Gemeente	Het kunnen uitvoeren van de wettelijke taak van gezondheidsdiensten (GGD/JGZ) van de gemeente en leerplichtambtenaren door gegevens te ontvangen over de plaatsing en aan- of afwezigheid van leerlingen.
Hulp- of zorgverleners	Zorgplicht en ondersteuning uit kunnen voeren, evenals juiste begeleiding van de leerling.
Kennisnet	Leveren van de Overstap Service Onderwijs (OSO) waarmee het leerlingdossier uitgewisseld kan worden met een andere LAS (in het PO en VO). Ook levert Kennisnet het ECK iD (pseudo-ID) aan bij het LAS via de Nummervoorziening.
Uitgeverijen en Leveranciers van digitaal leermateriaal, LVS-systemen of leerplatformen (optioneel)	Leveren van gegevens aan uitgeverijen via Basispoort, een centrale voorziening voor toegang tot leermiddelen. Idem in geval van rechtstreekse koppelingen met leveranciers van leerlingvolgsystemen en leerplatformen.
Rovict B.V.	Het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Previder	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Microsoft	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Synaxion	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Zendesk	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Posthog	Het ondersteunen bij het leveren aan de onderwijsinstelling van een goed werkend digitaal volg- en administratiesysteem en een commercieel belang.
Medewerkers	Toegang kunnen hebben tot relevante gegevens voor het uitvoeren van hun onderwijstaken en begeleiding van leerlingen.
Ouders/verzorgers	Inzicht kunnen hebben in de voortgang en ontwikkeling van hun kind, communicatie met school en toegang tot relevante gegevens.
Leerlingen (incl aspirant- en oud-leerlingen)	Het ontvangen van gepersonaliseerd onderwijs, inzicht in eigen leerresultaten en begeleiding tijdens de schoolloopbaan.

Stagiaires	Praktijkervaring kunnen opdoen binnen een onderwijsomgeving door toegang tot relevante gegevens onder toezicht van bevoegde medewerkers.

7. Verwerkingslocaties

De gegevensverwerkingen vinden plaats op de volgende locaties.

Tabel 7.1 Verwerkingslocaties

Naam partij	Statutaire vestigingsplaats (sub-) verwerker	Beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt verwerkt door deze subverwerker	Plaats/land van opslag en verwerking persoonsgegevens en doorgifte mechanisme indien buiten de EER
Rovict B.V.	Soest (NL)	Leverancier/verwerker	Nederland
Previder	Hengelo (NL)	Subverwerker	Nederland
Microsoft	Redmond (VS)	Subverwerker	Ierland
Synaxion	Eindhoven (NL)	Subverwerker	Noord Europa
Zendesk	San Francisco (VS)	Subverwerker	Ierland
Posthog	Delaware (VS)	Subverwerker	Duitsland

8. Data Transfer Impact Assessment (DTIA)

De AVG bevat specifieke regels voor de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER). In beginsel mogen persoonsgegevens alleen worden overgedragen aan landen buiten de EER als het land een 'passend beschermingsniveau' heeft. Dat niveau kan op verschillende manieren worden bepaald: een multinational kan bindende bedrijfsvoorschriften vaststellen (BCR's), de EU-standaardcontractbepalingen (SCC) toepassen of alleen overdragen aan landen waarvoor de Europese Commissie een zogeheten adequaatheidsbesluit[17] heeft genomen.

Rovict maakt voor ESIS gebruik van subverwerkers, zowel gevestigd binnen als buiten de EER. De subverwerkers die buiten de EER zijn gevestigd, vallen allemaal onder het adequaatheidsbesluit dat is uitgevaardigd door de Europese Commissie, in dit geval het EU-US Data Privacy Framework (EU-US DPF) (situatie juli 2026). Hierdoor is Rovict niet verplicht om een DTIA uit te voeren op haar subverwerkers.

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

9. Technieken en methoden van gegevensverwerking

Artikel 32 van de AVG schrijft voor dat er passende technische en organisatorische maatregelen genomen moeten worden om een op het risico afgestemd beveiligingsniveau te waarborgen. Om inzicht te krijgen in welke mate er vorm wordt gegeven aan deze abstracte formulering wordt gebruik gemaakt van de voor de verwerkers opgestelde standaard DPIA-vragenlijst. Deze vragenlijst is door Rovict ingevuld en geeft een belangrijk deel inzicht in o.a. de genomen technische beheersmaatregelen en informatiebeveiliging. Het gebruik van bepaalde technieken en

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

methoden van gegevensverwerking kunnen aanvullende risico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, AI/algoritmes, cloud, nieuwe technologie, profilering en big dataverwerkingen.

Rovict voert voor wat betreft ESIS geen (semi-) geautomatiseerde besluitvorming toe en maakt binnen ESIS geen gebruik van AI/algoritmes of andere nieuwe technologieën. Daarnaast is vastgesteld dat binnen ESIS geen sprake is van 'Big data verwerkingen'[18] doet.

Voor wat betreft 'profilering' en het verwerken van bijzondere persoonsgegevens (gegevens betreffende de gezondheid) zijn voor deze DPIA de beveiligingsmaatregelen onderzocht, waaronder bijvoorbeeld de encryptie op twee lagen.

Informatiebeveiliging

Bovendien is er technisch onderzoek verricht naar ESIS, welke uitkomsten en bevindingen als volgt zijn beoordeeld voor deze DPIA:

- Rovict beschikt voor de gegevensverwerking via het systeem ESIS over een ISO 27001-2023/A1:2024 certificaat dat geldig is tot 6 april 2029. SIVON heeft het certificaat en de verklaring van toepasselijkheid beoordeeld en akkoord bevonden.
- Volgend uit deze ISO 27001 certificering, beschikt Rovict voor ESIS over een werkend ISMS (Information Security Management Systeem). Hierin is onder andere documentatie inzake het uitvoeren van risicoanalyses en behandelingen/beoordelingen daarvan gedurende het DPIA-proces opgenomen.
- Binnen het onderwijsveld wordt daarnaast gebruikt gemaakt van het ROSA[19] certificeringsschema. Door het bepalen van de BIV-classificatie (laag/midden/hoog) voor de onderdelen 'Beschikbaarheid', 'Integriteit' en 'Vertrouwelijkheid' worden de daarop van toepassing zijnde beheersmaatregelen inzichtelijk. De ROSA-rapportage is een onderdeel van de beveiligingsbijlage van de verwerkersovereenkomst.

  Ook voor ESIS is het ROSA-certificeringsschema gebruikt. In een initiële selfassessment kwam Rovict daarin uit op een BIV-niveau wat niet in overeenstemming was met de aard en inhoud van ESIS (Midden-Midden-Hoog). In diverse constructieve overlegrondes tussen Rovict en SIVON is het BIV-niveau bepaald op Hoog-Hoog-Hoog, wat betekent dat voor alle onderdelen het hoogste niveau van beveiligingsmaatregelen van toepassing is.
- Over het algemeen geeft Rovict aan dat is voldaan aan de vereiste maatregelen. In enkele gevallen werd er niet voldaan. Vervolgens heeft SIVON gecontroleerd of de daadwerkelijk genomen beheersmaatregelen in overeenstemming zijn met de BIV-classificatie-eisen.

  Uit deze beoordeling zijn de volgende zaken naar voren gekomen:
- Voor wat betreft de categorie **'Beschikbaarheid'** geeft Rovict aan dat voor het onderdeel Herstel gebruik wordt gemaakt van twee verschillende datacenters, en automatische spillover. Recovery tests werden één keer per jaar uitgevoerd. Voor de classificatie Hoog is twee keer per jaar vereist. Dit is inmiddels door Rovict doorgevoerd waardoor aan dit onderdeel wordt voldaan.
- Voor het onderdeel Onderhoud worden volgens Rovict kritieke punten direct opgepakt en verwerkt. Ook alle security patches en updates worden direct doorgevoerd. Dit is gedurende

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

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

het DPIA-traject aantoonbaar gedocumenteerd, waardoor dit onderdeel naar Voldaan is bijgesteld.

- Voor de categorie **'Integriteit'** is vastgesteld dat voor wat betreft de categorie Onweerlegbaarheid de functionaliteit ruim voldoet. Onderwijsinstellingen (beheerders) kunnen zelf een uitgebreid activiteitenlog downloaden en monitoren. Hiermee loopt ESIS vooruit op de eis uit het Normenkader IBP, dat voorschrijft dat de onderwijsinstelling de logging zelfstandig moet kunnen monitoren. Ook de ISO 27001-norm gaat ervan uit dat de verwerkingsverantwoordelijke zelf verantwoordelijk is voor de monitoring van loggegevens.

- Met betrekking tot de integriteit van de logfiles, is er een mogelijkheid voor root-admins om deze te wijzigen. Er wordt geen gebruik gemaakt van zogenaamde privileged access management, waarmee vastlegging en logging van gebruik van de rechten als root-admin wordt geborgd. Bij Rovict zijn er slechts enkele medewerkers die deze rechten hebben. Hiervoor wordt een alternatief protocol opgesteld.

- In de categorie **'Vertrouwelijkheid'** wordt nog niet volledig voldaan aan het onderdeel Levenscyclus gegevens. Er is vooralsnog slechts één termijn beschikbaar, zijnde 5 jaar. Dit is door Rovict inmiddels op de ontwikkelagenda gezet, zodat splitsing in 2 en 5 jaar mogelijk wordt. Zie hoofdstuk 11, Bewaartermijnen voor meer informatie. Er is gedurende het DPIA-traject wel al een aanpassing van de opschoningstermijn doorgevoerd (wekelijks). Ook het *by default* aanzetten van automatische opschoning is op de ontwikkelagenda gezet.

- Met betrekking tot het onderdeel Transport en fysieke opslag wordt op dit moment nog niet volledig voldaan aan de beveiligingsmaatregel van encryptie op twee niveaus (zowel op de virtuele schijf als op recordniveau). Het risico hierbij is dat data, wanneer deze (on)bedoeld door bevoegden en onbevoegden benaderd worden, leesbaar is. Rovict heeft gedurende het DPIA-traject toegezegd om de encryptie op twee lagen gefaseerd uit te breiden naar alle kolommen waar dit noodzakelijk is. Hiermee wordt de extra beveiliging en het beschermen van gegevens op basis van de classificatie (H) gerealiseerd.

- Naast het onderzoeken van de ROSA-vereisten, is ook beoordeeld hoe **Privacy by Default** wordt nageleefd. Hieronder worden de beoordeelde aspecten daarvan weergegeven.

- Met betrekking tot meerfactor-authenticatie (MFA of 2FA): ESIS beschikt over deze optie, echter deze wordt nog niet *by default* afgedwongen bij gebruikers. Gedurende het DPIA-traject heeft Rovict dit op de ontwikkelagenda gezet, waardoor het in de toekomst wel standaard wordt aangezet voor nieuwe klanten.

  Ondanks dat ESIS 2FA nog niet *by* default aanbiedt, kan de onderwijsinstelling dit zelf instellen en afdwingen. Hierop moet door de onderwijsinstelling beleid worden gemaakt, waarbij ook SSO met bijvoorbeeld Office 365 of Google kan worden meegenomen.

- De exportfunctionaliteit binnen ESIS is voor een aantal standaard aangeboden rollen *by default* beschikbaar. Scholen kunnen echter ook zelf de rollen en rechten inrichten en naar eigen inzicht exports/downloads aan- of uitzetten per rol. Bovendien heeft de beheerder de mogelijkheid om exporteren standaard voor iedereen uit te zetten. Deze manier van omgaan met export-/downloadbevoegdheden is een goed voorbeeld van *privacy by default.*

- In het exportmenu in ESIS wordt standaard, als laatste stap in het genereren van een export, de optie geboden om de export via ESIS te mailen. Hier zit geen beperking op, en de gebruiker krijgt ook geen waarschuwingsbericht. Bovendien is de mailfunctionaliteit waarin dit wordt aangeboden, niet beveiligd conform de huidige standaard (NTA 7516). Dit wordt als een hoog risico beschouwd. Rovict onderkent dit risico en zal de mailfunctionaliteit in de komende maanden uitfaseren.

- De onderwijsinstelling beschikt zoals eerder vastgesteld, over functionaliteit om zelf de logging te controleren inzake welke gebruiker welke gegevens heeft ingezien (ook waar het bijvoorbeeld gezondheidsgegevens betreft). De onderwijsinstelling kan in deze loginformatie ook het gebruik van de exportfunctionaliteit en wijziging van cijfers monitoren. Hierdoor is er inzicht in welke gebruiker, welke exports heeft uitgevoerd en is er monitoring op afwijkend

gedrag mogelijk met betrekking tot deze functionaliteit en cijferwijzigingen.

- Ook is onderzocht in hoeverre admins/beheerders toegang hebben tot de persoonsgegevens, inclusief bijzondere persoonsgegevens. Daaruit is gebleken dat de rol van applicatiebeheerder standaard geen rechten op leerlinggegevens heeft en zichzelf geen additionele rollen kan toekennen. Er is altijd een andere persoon nodig om dit te faciliteren.

  De rol van 'Supervisor' die wel alle toegang heeft, zonder beperkingen, is al enige jaren niet meer beschikbaar als standaard rol en kan ook niet meer als standaard rol uitgegeven worden. Onderwijsinstellingen die vanuit historie nog met deze rol werken, worden door Rovict actief geadviseerd om deze rol te ontmantelen.

- In ESIS is het voor beheerders niet mogelijk om in te loggen op het account van een gebruiker ("inloggen als"). Hiervoor moeten zij een rol aannemen. Een goed voorbeeld van *privacy by default.*

- Rovict biedt voor het toekennen van autorisaties in ESIS een aantal standaard rollen aan. Onderwijsinstellingen kunnen echter naar eigen inzicht zelf autorisaties aanpassen of aanmaken, waarmee zij zelf kunnen bepalen wie welke gegevens kan verwerken. Rollen kunnen worden uitgezet, op alleen lezen of op volledige toegang (inclusief wijzigen) gezet worden. Dit kan tot op functionaliteitsniveau. Het is mogelijk om in ESIS een volledig overzicht te genereren van alle rollen en gebruikers, inclusief hun activiteiten.

- Binnen ESIS is het niet mogelijk dat gebruikers zichzelf tijdelijk toegang geven tot een andere groep. Dit moet via een andere, hiervoor bevoegde gebruiker gebeuren. Bij de standaard rollen is dit een andere persoon dan degene die toegang heeft tot de leerlingdossiers. Hierdoor is er altijd een check op de toegang tot persoonsgegevens van andere leerlingen dan die van de eigen groep.

- Gedurende het DPIA-traject heeft Rovict het standaard tonen van het BSN op de leerlingenkaart verwijderd, waardoor deze niet meer onnodig in beeld komt. Hetzelfde geldt voor optionele velden zoals Geboortetijdstip, Gedoopt en Gezindte.

- Aangezien er gegevens over absentie (bijzondere persoonsgegevens) worden gedeeld via Microsoft Azure, is nagegaan én vastgesteld dat dit op de gewenste versleutelde (encrypted) wijze gebeurt.

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

IAMA: mensenrechten in beeld bij algoritmes
Indien uit voornoemde vragenlijst blijkt dat er gebruik wordt gemaakt van AI-technologie is beoordeeld of er sprake is van een hoog risico.

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

Uit het onderzoek is gebleken dat in ESIS geen gebruik wordt gemaakt van AI-technologie. Hierdoor is er geen sprake van een hoog risico algoritme en is het niet vereist om een Impact Assessment Mensenrechten en Algoritmes (IAMA) uit te voeren op ESIS.

10. Juridisch en beleidsmatig kader

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

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

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

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

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

De specifieke wettelijke grondslagen zijn verder uitgewerkt in hoofdstuk 12.

11. Bewaartermijnen

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

Voor de persoonsgegevens in ESIS zijn de volgende bewaartermijnen van toepassing:

Een bewaartermijn van twee (2) jaar (na uitschrijven leerling of beëindiging van de relatie met de medewerker) voor persoonsgegevens die niet onder de uitzonderingscategorie van vijf (5) jaar vallen, in overeenstemming met de huidige wet- en regelgeving en de handleiding bewaartermijnenoverzicht van Kennisnet (versie januari 2025), alsmede het bewaartermijnenoverzicht van Kennisnet (versie 1.3, juli 2025)[20].

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

- Besluit bekostiging WPO 2022[21]:

  Art. 11 Inhoud leerlingenadministratie

  1. De directeur van een school draagt er zorg voor dat een overzichtelijke leerlingenadministratie beschikbaar is van:

     a. de inschrijving, de uitschrijving en het verzuim van de leerlingen op de school;
     b. de gegevens van de leerlingen en hun ouders die noodzakelijk zijn voor de berekening van de bekostiging; en
     c. indien het een speciale school voor basisonderwijs betreft, de verklaring bedoeld in artikel 40, achtste lid, van de wet.

  Art. 12 Bewaren gegevens

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

[20] Zie Kennisnet: Bewaren en vernietigen van gegevens - Normenkader informatiebeveiliging en privacy voor het onderwijs.

[21] wetten.nl - Regeling - Besluit bekostiging WPO 2022 - BWBR0046159.

- Besluit uitwisseling leer- en begeleidingsgegevens[22]:

  Art. 7a. Bewaartermijn
  Het onderwijskundig rapport (OKR) wordt bewaard tot vijf jaar na uitschrijving van de leerling. Ook het ontwikkelingsperspectief (OPP – indien van toepassing), eindtoets en schooladvies maken onderdeel uit van OKR.

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

N.B.: totdat de sectorale selectielijsten voor po en vo zijn vastgesteld[23], is het advies aan de scholen gegeven om géén informatie en documentatie te vernietigen rondom

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

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

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

ESIS biedt een functionaliteit aan om **leerlinggegevens** te verwijderen na 5 jaar. Het is echter de verantwoordelijkheid van de school om zowel de bewaartermijnen te bewaken als daadwerkelijk de gegevens te verwijderen. Het systeem is niet geautomatiseerd voor deze taken.

Via de optie 'Periodiek opschonen' kan de onderwijsinstelling Rovict de opdracht geven om dit automatisch periodiek te laten uitvoeren. De opschoning wordt sinds de zomer 2026 wekelijks uitgevoerd (was tweemaal per jaar). Tevens kan hier ook het Exceloverzicht van de opgeschoonde leerlingen gedownload worden.

De huidige 5-jaarstermijn in ESIS is echter niet conform wet- en regelgeving, zie hierboven. Rovict heeft toegezegd dit aan te passen (zie hoofdstuk 20, Maatregelen). Na uitschrijving van een leerling moeten gegevens in twee fases worden verwijderd, namelijk twee jaar na de uitschrijving van de leerling en vijf jaar na de uitschrijving. Dit dient er als volgt uit te zien:

- Tot 2 jaar nadat een leerling de school heeft verlaten mogen gegevens bewaard blijven. Na deze periode moeten door middel van een specifieke verwijderactie binnen ESIS alle toetsresultaten, vragenlijsten en documenten worden verwijderd.

- Tot 5 jaar nadat een leerling de school heeft verlaten moeten gegevens over verzuim en in- en uitschrijving bewaard blijven. Na deze periode moet door middel van een specifieke verwijderactie het gehele leerlingdossier verwijderd worden, en deze handeling mag niet meer worden teruggedraaid, zelfs niet via een restore van een back-up.

- Tot 5 jaar nadat een leerling de school heeft verlaten moet OKR bewaard blijven. Na deze periode kan door de huidige opschoningsoptie binnen ESIS door middel van een specifieke verwijderactie het gehele leerlingdossier worden verwijderd en deze handeling kan niet meer worden teruggedraaid, zelfs niet via een restore van een back-up.

[22] wetten.nl - Regeling - Besluit uitwisseling leer- en begeleidingsgegevens - BWBR0031619
[23] De PO-Raad en VO-raad hebben een sectorale groepsselectielijst voorbereid en door hun ALV's laten bekrachtigen. Deze lijst is echter nog niet als selectiebesluit vastgesteld op grond van de nieuwe Archiefwet en heeft daarom nog niet de status van een wettelijk geldende selectielijst voor alle schoolbesturen.

Opmerking

- Gegevens over bekostiging moeten zeven jaar bewaard worden. Dit hoort echter niet in een LAS/LVS thuis. De onderwijsinstelling zal deze gegevens, indien aanwezig in ESIS, na 5 jaar moeten overhevelen naar het financiële systeem.

- Wanneer een leerlingdossier wordt verwijderd, blijven de groepsgegevens (zoals notities en groepsdynamiek) van de groepen waarin deze leerling onderwijs heeft gevolgd, behouden in ESIS. Deze groepsgegevens kunnen echter handmatig worden verwijderd.

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

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

De onderwijsinstelling is hier zelf verantwoordelijk voor, dit gebeurt niet automatisch binnen ESIS. Tenzij het via de HR-koppeling is ingeregeld. Bij vertrek van medewerkers worden hun gegevens meestal gedeactiveerd maar niet verwijderd. De reden hiervoor is dat het belangrijk is om te kunnen traceren wie verantwoordelijk was voor bepaalde groepen, wie notities heeft gemaakt bij een leerling, of wie bepaalde documenten heeft aangemaakt. Daarom worden de gegevens van medewerkers bewaard voor de gehele schoolperiode van een leerling.

Daarnaast worden binnen ESIS persoonsgegevens van **ouders/verzorgers** verwerkt. Deze gegevens worden na 5 jaar automatisch verwijderd, tegelijk met het verwijderen van de leerlinggegevens.

Beëindiging contract ESIS

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

Back-up

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

6. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen

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

12. Rechtsgrond

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

Artikel 6 AVG kent 6 grondslagen:

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

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

ESIS is een gecombineerd leerlingadministratie én -volgsysteem (LAS en LVS) dat fungeert als centrale administratiesysteem voor onderwijsinstellingen in het primair onderwijs. Met ESIS is het mogelijk voor een onderwijsinstelling om gemakkelijk de leerlingadministratie te beheren én inzicht te krijgen in leerlingprestaties, met als doel de onderwijskwaliteit te verbeteren. ESIS kan worden uitgebreid met aanvullende modules. De scope van deze DPIA op ESIS richt zich enkel op de functionaliteit voor een LAS en LVS.

Het verwerken van persoonsgegevens via ESIS is geen doel op zich. Het doel is het administreren en volgen van onderwijsdeelnemers. Er is dus geen grondslag vereist voor het gebruik van ESIS als applicatie[26], er dient wel een grondslag te zijn voor het verwerken van de persoonsgegevens zelf. Daarnaast zullen we in deze paragraaf zien dat er een wettelijke plicht is voor een onderwijsinstelling om een leerling- en onderwijsvolgsysteem te gebruiken.

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

1. Leerlingen

Leerlingvolgsysteem (LVS)

De rechtsgrond voor de verwerking van persoonsgegevens die inzicht geeft in de voortgang van kennis en vaardigheden op het niveau van de leerling, de groep en de school binnen een leerling-

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

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

Dit vindt bevestiging in jurisprudentie[27] waarin wordt gesteld dat artikel 8 lid 1 en 2 WPO een voldoende rechtsgrondslag biedt zoals bedoeld in artikel 6 lid 1 sub c AVG voor het verwerken van persoonsgegevens in een leerlingvolgsysteem, ook als dat betrekking heeft op de sociaal-emotionele ontwikkeling van leerlingen. Ook wordt er benadrukt in dit verband dat de AVG niet vereist dat voor elke afzonderlijke verwerking specifieke wetgeving aanwezig is, zoals blijkt uit overweging 45 in de considerans bij de AVG. Het is voldoende dat er algemene wetgeving bestaat die als basis kan dienen voor diverse verwerkingen op grond van een wettelijke verplichting. Op basis hiervan kan ook de grondslag van wettelijke verplichting (art. 6 lid 1 sub c) voldoen als wettelijke grondslag.

Leerlingadministratiesysteem (LAS)

Het onderdeel leerlingadministratiesysteem wordt ingezet voor administratieve taken, zoals het registreren van persoonsgegevens van leerlingen, de in- en uitschrijving, het faciliteren van communicatie met ouders en het beheren van de schoolorganisatie. De noodzaak hiervoor is gelegen in het feit dat men moet voldoen aan wettelijke verplichtingen, zoals de leerplichtwet, WPO en de Wet register onderwijsdeelnemers, maar ook op de uitvoering van een taak van algemeen belang, zoals het organiseren van goed onderwijs. Hierdoor kan deze verwerking gebaseerd worden op artikel 6, lid 1, sub e van de AVG (taak van algemeen belang op grond van onderwijswetgeving). Hierbij geeft artikel 40b WPO en de Wet register onderwijsdeelnemers duidelijk aan welke persoonsgegevens moeten worden geadministreerd. In zoverre kan er ook sprake zijn van een rechtsgrond 'wettelijke verplichting' (sub c). Zie voor een uitwerking de tabel in hoofdstuk 10.

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

2. <u>Medewerkers</u>

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

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

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

Conclusie

De artikelen 11 jo. 45b lid 1 van de WPO, alsmede artikel 8 WPO bieden een solide wettelijke basis voor het verwerken van leerlinggegevens in het primair onderwijs. Onderwijsinstellingen kunnen zich voor wat betreft het leerlingadministratie en -volgsysteem hierbij primair beroepen op de grondslag *wettelijke verplichting* (artikel 6 lid 1 sub c AVG), omdat zij op grond van de WPO

[27] *Rechtspraak.nl* https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBOBR:2021:5776.

verplicht zijn de voortgang (ook sociaal-emotioneel) van leerlingen te monitoren. Aanvullend kan ook de grondslag *vervulling van een taak van algemeen belang* (artikel 6 lid 1 sub e AVG) een rol spelen, omdat scholen van overheidswege een publieke taak uitvoeren. Deze rechtsgrond kan dienen daar waar er mogelijk geen expliciete wettelijke grondslag is voor het verwerken van persoonsgegevens, zoals bepaald in de WPO en de Wet register onderwijsdeelnemers.

Een belangrijk aanvullend punt is dat, hoewel er duidelijke grondslagen zijn om persoonsgegevens van leerlingen en medewerkers te verwerken, scholen bij elke verwerking ook de AVG-beginselen (*zoals doelbinding, dataminimalisatie en transparantie*) in acht moeten nemen. Scholen moeten dus niet alleen kunnen terugvallen op een 'rechtsgrondslag' zoals bepaald in de AVG om te onderbouwen welke gegevens ze verwerken, maar ook kunnen aantonen dat de verwerking niet verder gaat dan noodzakelijk voor het onderwijsdoel, dat ze de gegevens niet langer bewaren dan strikt nodig, en dat ouders (en leerlingen zelf, voor zover van toepassing) en medewerkers duidelijk worden geïnformeerd over het hoe en waarom van de gegevensverwerkingen. Deze invulling van deze AVG- beginselen[28] is essentieel om de verwerking van persoonsgegevens ook in de praktijk rechtmatig, behoorlijk en transparant te laten plaatsvinden.

Tabel 12.1 Rechtsgrond

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

[28] Zie artikel 5 AVG.

		o.b.v. onderwijswetgeving).
Het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 11 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
De indeling en aanpassing van roosters.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
Het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgend van onderwijs.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Tevens artikel 9 lid 2 sub g jo. artikel 30 lid 2 sub a UAVG. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
De communicatie met Onderwijsdeelnemers en ouders en met medewerkers van de Onderwijsinstelling.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 11 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
Monitoring en verantwoording, met name ten behoeve van: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vormen) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
Het voor zover noodzakelijk en wettelijk toegestaan uitwisselen van Persoonsgegevens met Derden, waaronder: - Toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak; - Samenwerkingsverbanden in het kader van passend onderwijs en regionale samenwerkingen; - Partijen betrokken bij de invulling van stage- of leer- werkplekken; - Het leveren van Persoonsgegevens aan Onderwijsinstellingen in geval van	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag). Artikel 1 en 4c WPO (inspectie). Artikel 18a WPO (samenwerkingsverband).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).

overstappen tussen Onderwijsinstellingen en bij vervolgonderwijs; - Het in opdracht van Onderwijsinstelling leveren van Persoonsgegevens aan een andere partij.	Artikel 42 WPO (onderwijskundig rapport).	
Het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag). Artikel 28 AVG.	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
De continuïteit, verbetering en goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
Het door de Onderwijsinstelling beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden verglijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
Het door de Onderwijsinstelling voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).

Het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
De uitvoering of toepassing van een Unierechtelijke of lidstaatrechtelijke wettelijk bepaling of regeling.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 12 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).
Andere doeleinden ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces) en het begeleiden en volgen van Onderwijsdeelnemers (in hun leerproces), namelijk het kunnen inschrijven en plaatsen van leerlingen.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8 en 45b WPO. Artikel 11 WPO. Wettelijke grondslag (en/of taak van algemeen belang (of openbaar gezag).	De conclusie is dat het inzetten van een leerling- en onderwijsvolgsysteem zoals ESIS is toegestaan op grond van artikel 6 lid 1 sub c (*wettelijke grondslag*) en / of e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).

13. Bijzondere persoonsgegevens

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

Bijzondere persoonsgegevens:

Gezondheidsgegevens

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

Artikel 30 van de Uitvoeringswet AVG (UAVG) beschrijft enkele uitzonderingen inzake gegevens over gezondheid. Volgens art. 30 lid 2 sub a UAVG is het verbod om gegevens over gezondheid te verwerken niet van toepassing op onderwijsinstellingen, voor zover de verwerking met het oog op de speciale behandeling van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is. In de Wet op het primair onderwijs (WPO) wordt dit eveneens behandeld in artikel 8 lid 4 WPO[29].

Wettelijk gezien mag een onderwijsinstelling dus gezondheidsgegevens verwerken van leerlingen, maar hierop gelden de beginselen van de AVG, waaronder dataminimalisatie en '*need to know'*. Bij scholen is dat dus beperkt tot begeleiding of speciale voorzieningen die nodig zijn voor de

[29] Zie ook: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/onderwijs/leerlingdossiers.

leerlingen om deel te nemen aan het onderwijs. In de praktijk vertaalt zich dit door deze informatie door een beperkt aantal medewerkers te laten verwerken in ESIS.

Gevoelige Persoonsgegevens:

BSN

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

Open tekstvelden

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

14. Doelbinding

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

15. Kinderrechten-afweging (Best Interests Assessment Children)

Artikel 3 van het Verdrag inzake de rechten van het kind, schrijft voor dat bij alle maatregelen betreffende kinderen - ongeacht of deze worden genomen door openbare of particuliere instellingen, rechterlijke instanties, bestuurlijke autoriteiten of wetgevende lichamen - de belangen van het kind de eerste overweging (moeten) vormen. Deze belangenafweging gaat verder dan een veilige gegevensverwerking maar ziet ook op de mogelijke gevolgen van de verwerking.

Met schoolbesturen als leden van SIVON in het primair en voortgezet onderwijs, betekent dit dat SIVON in haar DPIA's rekening houdt met onder andere 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 ESIS 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[30].

De afweging bestaat uit 4 stappen:

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

Hieronder wordt beschreven welke rechten 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

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

dat het kind in overeenstemming met zijn of haar ontwikkelende capaciteiten, een stem heeft (kan hebben) in zaken die hem of haar aangaan.

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

2. Wat is het effect van de gegevensverwerking en gebruik van ESIS 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 ESIS:

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

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

3. Is dit effect wenselijk

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

4. Zijn er aanvullende maatregelen noodzakelijk 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 ESIS hebben op de kinderrechten, zijn over een brede linie tegen het licht gehouden zonder dat daarbij is gebleken dat er sprake is van een niet te rechtvaardigen inbreuk.

16 a. Noodzakelijkheid

Verwerking van persoonsgegevens met behulp van digitale onderwijsmiddelen door onderwijsinstellingen vindt plaats ten behoeve van het verzorgen van onderwijs, waaronder 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 bijna alle door ESIS te verwerken persoonsgegevens noodzakelijk zijn in relatie tot het doel van de gegevensverwerking.

De verwerkingen door de onderwijsinstelling via ESIS vinden plaats om door middel van een digitaal systeem de gegevens van leerlingen te administreren en ontwikkelingen/vorderingen bij te

houden. Tevens is de gegevensverwerking noodzakelijk in het kader van de wettelijke verplichtingen om onderwijs te verzorgen.

In het kader van dataminimalisatie worden echter nog een aantal persoonsgegevens van medewerkers verplicht uitgevraagd waar dat niet nodig is. In het verleden werden LAS/LVS-systemen ook gebruikt voor het administreren van gegevens van medewerkers. Tegenwoordig gebeurt dit meestal in aparte HR-systemen, zoals Visma of AFAS. Sommige klanten van Rovict gebruiken deze functionaliteit binnen ESIS echter nog wel.

Wanneer er in een dergelijk geval medewerkers in het systeem worden opgenomen, bijvoorbeeld om leerkrachten aan het systeem te koppelen, wordt automatisch de geboortedatum '1-1-1900' ingevuld. De school kan deze datum weliswaar aanpassen, maar dat is in principe niet de bedoeling.

De HR-functionaliteit binnen ESIS wordt op termijn volledig uitgefaseerd.

NB**:** De verwerking van persoonsgegevens binnen deze HR-functionaliteit valt buiten de scope van deze DPIA en is daarom niet nader onderzocht.

Het uitvoeren van de verwerkingen en toepassen van alle andere soorten persoonsgegevens die zijn vastgelegd, is noodzakelijk om ESIS op de gewenste manier te kunnen gebruiken.

16. b. Proportionaliteit en subsidiariteit

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

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

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

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

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

17. Rechten van de betrokkenen

Art. 15, lid 1, van de AVG beschrijft dat iedere betrokkene het recht heeft om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens[31]*.*

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

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

SIVON heeft onderzocht en vastgesteld dat, met betrekking tot de uitoefening van rechten van betrokkenen, scholen die ESIS gebruiken, zelfstandig kunnen voorzien in de afhandeling van verzoeken van betrokkenen (veelal van ouders). Mocht een school hier niet uitkomen, dan ondersteunt Rovict de school bij het voldoen aan de verplichtingen van de verwerkingsverantwoordelijke inzake de rechten van betrokkenen.

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

Tabel 17.1

Recht van betrokkene	Toelichting procedure	Eventuele beperking verwerking[32]
Het recht op informatie	De onderwijsinstelling dient als verwerkingsverantwoordelijke te zorgen voor een: • Openbaar gepubliceerde privacyverklaring op de website; • Intern gepubliceerde privacyverklaring; • Publicatie in de schoolgids.	n.v.t.
Het recht van inzage	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht op rectificatie	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht op gegevenswissing	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht op beperking van de verwerking	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht op overdraagbaarheid van gegevens	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.
Het recht van bezwaar	De Onderwijsinstelling kan op verzoek van de betrokkene dit recht waarborgen.	n.v.t.

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

Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit	Dit is niet aan de orde. De onderwijsinstelling neemt de uitkomsten van de leer- en toetsresultaten mee in de eigen beoordeling van de leerling.	n.v.t.

18. Beoordeling verwerkersovereenkomst

Voor leveranciers die deelnemer (of medestander) zijn van het Convenant digitale onderwijsmiddelen en privacy 4.0 (ook wel: Privacyconvenant Onderwijs, hierna: Convenant) of de opvolger daarvan, zijnde het keurmerk Edu-V, en gebruik maken van het daarbij horende model verwerkersovereenkomst, vindt een toetsing plaats welke wordt afgezet tegen de vereisten van het convenant/Edu-V. Dit wordt de theoretische toets genoemd. Aanvullend hierop vindt ook, mede aan de hand van de inzichten die deze DPIA heeft gebracht, een praktische toets plaats. Hierbij is een vergelijk gemaakt tussen de in de theorie genoemde afspraken en de verwerkingen die in de praktijk plaatsvinden. De hiervoor gebruikte toetsingskaders zijn via https://sivon.nl/toetsen-verwerkersovereenkomsten-2/ terug te vinden.

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

Voor Rovict is de verwerkersovereenkomst met versiedatum oktober 2026 getoetst. Na diverse revisierondes en aanpassingen is uiteindelijk een nieuwe versie (november 2026) van de verwerkersovereenkomst opgesteld. Het toetsrapport hiervan is opgenomen in bijlage 3. De bevindingen komen terug in de risicotabel van hoofdstuk 19 (risico 2 en 3).

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 Britse toezichthouder[33] om risico's te classificeren. Hierbij wordt een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade). Zie ook bijlage 2.

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

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

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 twee vervolgstappen:

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

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

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 ESIS wordt ingezet of dat het risico het systeem zelf betreft (de applicatie).

De risico's worden ook ingedeeld via de MAPGOOD-methodiek[34] om inzicht te krijgen in de verschillende risico's van de verwerking.

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

Tabel 19.1 Risico's:

Risico nr.	Mapgood	Risico-omschrijving	Oorzaak	Gevolg	Kans	Impact	Risico	Proces en/of systeem-risico+ verantwoordelijke
1	MO	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregelen toegepast.	Wijziging logfiles is mogelijk door root-admins. Geen priviledged access management toegepast.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	2	3	6	Proces (Rovict)
2	P	Onrechtmatig bewaren van persoonsgegevens.	Bewaartermijnen niet conform wet- en regelgeving door onderwijsinstelling uit te voeren. Bewaartermijn voor alle persoonsgegevens is standaard op 5 jaar ingesteld. (NB: Rovict heeft hierover gedurende meerdere jaren vragen gesteld aan Kennisnet maar geen eenduidig antwoord ontvangen)	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	3	3	9	Systeem (Rovict)
3	P	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregelen toegepast. De 'Vertrouwelijkheid' van de BIV-	Onvoldoende encryptie op de database 'at rest', er ontbreekt een encryptielaag op een aantal kolommen in de database. Op diverse kolommen is dit wel al gerealiseerd.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	3	3	9	Systeem (Rovict)

[34] Zie bijlage B voor nadere uitleg

		classificatie in het ROSA certificeringsschema is als 'Hoog' gekwalificeerd, hier wordt nog niet volledig aan voldaan.						
4	P M O	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregel en toegepast en geen 'privacy by default'.	Er wordt geen 2FA voor beheerders en andere gebruikers by default afgedwongen. NB: voor nieuwe klanten wordt dit wel al afgedwongen, Huidige klanten zitten in een overgangsperiode.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	3	3	9	Systeem (Rovict)
5	P M O	Onrechtmatig delen van persoonsgegevens. Er worden onvoldoende beveiligingsmaatregel en toegepast en geen 'privacy by default.	Gegenereerde exports kunnen zonder beperking als bijlage vanuit ESIS gemaild worden, via een onbeveiligde mailfunctionaliteit.	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	3	3	9	Systeem (Rovict)
6	P M O	Geen toepassing van dataminimalisatie	Er wordt een persoonsgegeven (geboortedatum medewerker) verplicht uitgevraagd, welke niet noodzakelijk is. (Dit wordt standaard door systeem gevuld met 1-1-1900).	Dit kan leiden tot misbruik van gegevens en is een risico voor de rechten en vrijheden van betrokkenen.	1	3	3	Systeem (Rovict)

8. Deel D: Beschrijving voorgenomen maatregelen

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

De AVG bepaalt in artikel 5 lid 1 sub f 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 geldt:
    a. de maatregel is beperkt in tijd, en wordt uitgevoerd in een realistisch tijdpad (in verhouding tot het te mitigeren risico) met als uitgangspunt maximaal één jaar;
    b. de maatregel is concreet, uitvoerbaar en controleerbaar;
    c. in de tussenliggende periode moet het bruto risico in voldoende mate te beheersen zijn (tussenmaatregelen);
    d. bij door de leverancier te nemen maatregelen, stemt deze met SIVON de implementatie daarvan af en controleert SIVON (achteraf) of de maatregel conform de afspraak is of wordt uitgevoerd. SIVON houdt hiertoe een (publieke) ITL (issue tracking list) bij.

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

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

20.1 Maatregelentabel

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (leverancier /school)	Rest-risico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum) maat-regel geïm-plemen-teerd
1	Onrechtmatige toegang tot persoonsgegevens. (Wijziging logfiles mogelijk)	6	Gebruik maken van priviledged access management, met een verplichte beschrijving van de reden gebruik root-admin rechten (aanvragen). Tevens loggen van die werkzaamheden via gescheiden accounts, zodat vastlegging en logging van gebruik van de rechten als root-admin wordt geborgd.	Rovict	3	Rovict voert aangepaste maatregel uit, waarbij d.m.v. protocol de 2 personen met root-adminrechten melding doen van werkzaamheden en deze daarmee worden vastgelegd. Er is na het doorvoeren van de maatregelen een restrisico.	Uiterste datum gereed: januari 2027 (Rovict)
2	Onrechtmatig bewaren van persoonsgegevens. (Bewaartermijnen niet conform wettelijke vereisten)	9	Mogelijkheid toevoegen om verschillende bewaartermijnen toe te passen.	Rovict	1	Er is na het doorvoeren van de maatregelen een minimaal en aanvaardbaar restrisico.	Uiterste datum gereed: juni 2027 (Rovict)
3	Er worden onvoldoende beveiligingsmaatregelen toegepast.	9	Alle als 'Hoog' geclassificeerde kolommen die nog niet als zodanig zijn beschermd, in de database encrypten.	Rovict	1	Er is na het doorvoeren van de maatregelen een minimaal en	Uiterste datum gereed: april 2027

	(dubbele encryptie)					aanvaardbaar restrisico.	(Rovict)
4	Onrechtmatige toegang tot persoonsgegevens (2FA)	9	Gebruik 2FA by default instellen (technisch) Onderwijsinstelling: 2FA instellen en afdwingen. Daarbij ook via SSO bijv. Office 365 en Google meenemen. (technisch en organisatorisch)	Rovict Onderwijsinstelling	1	Rovict stelt dit voor nieuwe klanten al standaard in. Voor huidige klanten is daar geen mogelijkheid voor. Als de onderwijsinstelling de gesuggereerde maatregelen doorvoert, is het restrisico aanvaardbaar.	Maatregelen te nemen op niveau onderwijsinstelling
5	Onrechtmatig delen van persoonsgegevens. (Exports toevoegen aan onbeveiligde mail)	9	Verwijderen standaard optie in exportmenu om export als bijlage toe te voegen aan mail. (technisch) Onderwijsinstelling: afspraken maken over het genereren en mailen van exports en hier controle op uitoefenen (door logfiles te monitoren). (organisatorisch)	Rovict Onderwijsinstelling	0	Rovict verwijdert de volledige mailfunctionaliteit uit ESIS, waardoor er na doorvoeren hiervan geen restrisico meer aanwezig is.	Uiterste datum gereed: Maart 2027 (Rovict)
6	Geen dataminimalisatie	3	Verplichte veld 'Geboortejaar' medewerker verwijderen (technisch) Onderwijsinstelling: afspraken maken dat standaard vulling veld 'geboortejaar' niet wordt gewijzigd. (organisatorisch)	Rovict Onderwijsinstelling	0	Rovict faseert de hele HR-functionaliteit uit, waardoor er na doorvoeren hiervan geen restrisico meer aanwezig is.	Uiterste datum gereed: december 2027 (verwijderen geboortedatum) (Rovict)

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 ESIS 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 ESIS. Het vergt ook dat de basis op orde is van onder andere het besturingssysteem waarop het draait, de kennis en kunde van de gebruiker en het hebben en toepassen van relevant beleid. Organisatie-specifieke risico's die hiermee gepaard gaan zijn opgenomen in onderstaande tabel.

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	Het bestuur heeft een eigen privacycoördinator of privacy officer aangesteld.		
2	De bestuur heeft een (externe) Functionaris Gegevensbescherming aangesteld.		

3	Het bestuur heeft de volgende formele structuren geïmplementeerd: een autorisatiebeleid, toegangsbeheer, toewijzing van verantwoordelijkheden en eigenaarschap betreffende gegevensverwerking.		
4	Het bestuur beschikt over een gedetailleerd autorisatiebeleid, inclusief een autorisatiematrix, specificeert welke 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.		
5	Het bestuur beschikt over een datalekprotocol/beleid en past dit actief toe.		
6	Het bestuur beschikt over een wachtwoordbeleid en past dit actief toe.		
7	Het bestuur beschikt over een bewaartermijnenbeleid en protocol opschonen en past dit actief toe.		
8	Het bestuur beschikt over een actueel IBP beleid en heeft deze laten vaststellen.		
9	Het bestuur beschikt over een procedure rechten van betrokkenen en past dit actief toe.		
10	Het bestuur beschikt over een DPIA beleid en laat minimaal eens per drie jaar DPIA's herbeoordelen.		
11	Het bestuur beschikt over een gedragscode met richtlijnen hoe gebruikers op een verantwoorde en veilige manier gebruik mogen maken van ICT-middelen en internet en past dit actief toe. Daarbij is specifieke aandacht voor het opslaan, printen, e-mailen en andere vormen van uitwisseling van gedownloade bestanden vanuit de applicatie.		
12	Het bestuur werkt volgens een PDCA-cyclus m.b.t. de AVG waarbij er periodiek wordt gekeken of men compliant is en wat er verbeterd kan worden.		
13	Het bestuur voldoet aan de transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over het gebruik van digitale leermiddelen.		
14	Het bestuur voldoet aan de transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over de wijze waarop de ouders (of leerlingen > 16 jaar) hun rechten kunnen uitoefenen.		

Risicotabel 2. **Algemene applicatiespecifieke risico's**
De volgende risicotabel bevat beheersmaatregelen die bedoeld zijn om de algemene risico's, die inherent zijn aan de verwerking, te adresseren. Deze maatregelen zijn tevens van toepassing op vergelijkbare verwerkingen bij andere leveranciers. Ze omvatten diverse aspecten, zoals het afsluiten van passende verwerkersovereenkomsten en het verstrekken van instructies aan medewerkers over het invullen van gegevens in open velden.

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	Het bestuur heeft de Verwerkersovereenkomst met verwerker beoordeeld, getekend en gearchiveerd. Hier zijn onder meer afspraken vastgelegd over		

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

	schaduwadministratie op verschillende schijven en mappen van medewerkers.		
15	Het bestuur neemt verantwoordelijkheid voor het veilig koppelen van ESIS met andere koppelpartijen.		
16	Het bestuur neemt verantwoordelijkheid dat gebruikers van de applicatie afdoende zijn/worden getraind in het gebruik ervan.		

Risicotabel 3
Tenslotte zijn hieronder de risico's uit de centrale DPIA en uit de praktijkbeoordeling opgenomen, die op schoolniveau gemitigeerd moeten worden.

Risico	Te nemen maatregel	Uitgevoerd?	Opmerking/toelichting
Risico op onjuiste of onrechtmatige verwerking van leerlinggegevens.	De onderwijsinstelling biedt medewerkers een gerichte instructie of training aan over het juist verwerken van persoonsgegevens in de applicatie, met speciale aandacht voor gevoelige en bijzondere gegevens, zoals leerresultaten, medische informatie en rubrieken met vrije invulvelden en leerlingnotities.		
Risico op verzending van (bijzondere) persoonsgegevens zonder passende beveiligingsmaatregelen.	De onderwijsinstelling zal gebruikers instrueren over het juiste gebruik van de e-mailfunctie binnen de applicatie en worden op de hoogte gesteld van het aanwezige veilig alternatief voor het versturen van berichten met gevoelige of bijzondere persoonsgegevens naar derden.		
Risico op organisatorische kwetsbaarheid.	De onderwijsinstelling beschikt over een taak – en werkprocesbeschrijving voor de accountbeheerder(s) en applicatie-beheerder(s) van de applicatie en daarnaast is er nagedacht over een back-up voorziening voor het bovenschoolse applicatiebeheer.		
Risico op onvoldoende naleving van de procedures.	De onderwijsinstelling heeft middels een '*Inrichtingsdocument*' specifiek de regels vastgelegd omtrent de inrichting, gebruik, beheer en controles van de applicatie.		
Risico op onduidelijkheid over eindverantwoordelijk.	De onderwijsinstelling heeft een proceseigenaar voor de applicatie aangesteld.		
Risico op verwerking zonder geldige rechtsgrondslag.	De organisatie heeft afzonderlijke verwerkersovereenkomsten met de koppelpartners beoordeeld, ondertekend en gearchiveerd.		
Risico op het uitwisselen van te veel gegevens met derde partijen.	De onderwijsinstelling controleert vooraf het koppelvlak op inhoud en noodzaak.		
Risico op het uitwisselen van te veel persoonsgegevens met derde partijen.	De onderwijsinstelling voert periodiek controles uit, op de actualiteit van de koppelvlakken (Slapende - nieuwe – openstaande aanvragen). De uitgevoerde		

	controles en afwijkingen worden gedocumenteerd.		
Risico op overtreding van het beginsel van gegevensbeperking	De onderwijsinstelling hanteert standaard groepsautorisatie voor alle gebruikersaccounts en bepaalt zelf, afhankelijk van de rol, of de mogelijkheid om deze tijdelijk op te heffen aan of uit staat.		
Risico op ongeautoriseerde of onrechtmatige toegang tot persoonsgegevens.	De onderwijsinstelling controleert periodiek de opgegeven reden voor tijdelijke opheffing van een groepsautorisatie. De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
Risico op ongeautoriseerde toegang.	De onderwijsinstelling voert periodieke controles uit op gebruikersaccounts (Slapende, accounts zonder actieve aanstelling – accounts zonder 2FA) en onderneemt actie of verwijdert deze indien nodig. De uitgevoerde controles en afwijkingen worden gedocumenteerd.		
Risico op onrechtmatige of onnodige verwerking van persoonsgegevens.	De onderwijsinstelling heeft duidelijke afspraken vastgelegd over het invoeren van gegevens in open velden en over dataminimalisatie. Dit kan bijvoorbeeld aan de hand van vastgesteld beleid of protocollen die zijn geïmplementeerd. Hierin is bepaald of het gebruik van vrije invulvelden noodzakelijk is en zo ja voor welke informatie. Ook is gedefinieerd wat wordt verstaan onder dataminimalisatie (bijv. niet het geboortejaar medewerkers aanpassen). Over deze uitgangspunten is duidelijk gecommuniceerd met alle medewerkers die gebruik maken van de applicatie.		
Risico op ongeautoriseerde toegang.	De onderwijsinstelling heeft de juiste autorisaties ingericht en duidelijke afspraken vastgelegd inzake het genereren van exportbestanden. De beschikbare logbestanden worden hier regelmatig op gecontroleerd.		
Risico op ongeautoriseerde toegang.	De onderwijsinstelling heeft technische of organisatorische beheersmaatregelen genomen om ervoor te zorgen dat de downloadmap van elke lokale computer regelmatig wordt geleegd.		
Risico op ongeautoriseerde toegang.	De onderwijsinstelling heeft standaard tweefactorauthenticatie (2FA) ingeschakeld voor alle medewerkersaccounts met toegangsrechten, inclusief de beheerdersaccountants.		
Risico van onopgemerkt verlies van bescherming.	De onderwijsinstelling controleert periodiek de instellingen voor het inschakelen van 2FA-authenticatie voor gebruikers.		

Risico van te ruime toegang tot (gevoelige) gegevens.	De vastgestelde autorisaties zoals (stapel-)rollen en rechten binnen de onderwijsinstelling worden periodiek gecontroleerd op het juist toepassen hiervan of passend bij de actuele werkzaamheden (met name stapelrollen).		
Risico op geen sluitend autorisatiebeheer en verhoogd risico op datalek.	De onderwijsinstelling heeft een einddatum ingesteld voor tijdelijke krachten, afgestemd op de noodzakelijke duur, met een maximum van één schooljaar.		
Risico op schending van bewaartermijn en het beginsel van minimale gegevensverwerking	Bij het opschonen van persoonsgegevens, na verlopen bewaartermijn, worden gegevens verwijderd uit het leerlingdossier, en ook uit de groepsdocumenten in de Groepsmap.		
Risico op schending van bewaartermijn en het beginsel van minimale gegevensverwerking	Bekostigingsgegevens (o.a. TLV) worden na de termijn van 5 jaar verwijderd uit ESIS en overgeheveld naar het financieel systeem.		
Risico op schending van bewaartermijn en het beginsel van minimale gegevensverwerking	Adresgegevens van (oud-)leerlingen worden door de school uitsluitend met toestemming van de leerling bewaard (buiten ESIS) voor het organiseren van reünies.		

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

In aanvulling op de in de centrale DPIA gevonden risico's en maatregelen, heeft de implementatie en gebruik van ESIS 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 ESIS 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 ESIS.

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

De FG is [wel/niet] betrokken geweest bij uitvoering en opstellen van de lokale DPIA voor [naam schoolbestuur]. Beschrijving rol FG schoolbestuur bij deze DPIA

Het advies van de FG is […].

F. Visie betrokkenen

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

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

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

G. Conclusie

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

Deze conclusie verandert, 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 ESIS 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 moeten 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 Rovict een aantal maatregelen neemt. Hiernaast moet het schoolbestuur maatregelen nemen of treffen om de benoemde risico's te beperken. Dit gaat om 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 ESIS, 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 ESIS. Zorg hierbij voor functiescheiding waarbij in geval van autorisatieverlening gewerkt wordt met het vier-ogenprincipe.
3. het informeren de leerlingen, hun ouders en medewerkers over deze DPIA en de (mogelijke) gevolgen voor de rechten en vrijheden die deze betrokkenen.
4. [BESCHRIJF HIER DE MAATREGELEN ZOALS OPGENOMEN BIJ HET ONDERDEEL "Overwegingen implementatie en lokale DPIA"]

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

I. Aanbevelingen

Naast de hiervoor genoemde bevindingen en maatregelen, zijn er een aantal aanbevelingen die buiten scope van deze DPIA vallen omdat zij niet binnen de invloedssfeer van (de leverancier van]

ESIS liggen, terwijl deze aanbevelingen cq. maatregelen wel 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 ESIS [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.

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

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

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

Toelichting MAPGOOD-methode

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

Mens – de mensen die nodig zijn om het informatiesysteem te beheren en gebruiken, denk aan: directe en indirecte gebruikers, en functioneel en technisch applicatiebeheer.

Apparatuur – de apparatuur die nodig is om het informatiesysteem te laten functioneren, denk aan: webserver, applicatieserver, beheer van werkplekken en werkplekken van gebruikers.

Programmatuur – de programmatuur waaruit het informatiesysteem bestaat, denk aan: de diverse applicaties die gebruikt worden.

Gegevens – de gegevens die door het systeem worden verwerkt, denk aan: basisregistraties, financiële verantwoording en vergunningen.

Organisatie – de organisatie die nodig is om het informatiesysteem te laten functioneren, denk aan: beheer-, gebruikers- en ontwikkelorganisatie.

Omgeving – de omgeving waarbinnen het informatiesysteem functioneert, denk aan: locatie, serverruimte en werkplekken.

Diensten – de externe diensten die nodig zijn om het systeem te laten functioneren, denk aan: technisch systeembeheer, netwerkinfrastructuur en onderhoudscontracten met externe dienstverleners.

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

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

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

Hulpmiddel beoordelen score laag, midden en hoog

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

Bijlage 3: Toetsrapport verwerkersovereenkomst

< in de PDF-versie van de DPIA staat hier de PDF van het officiële toetsrapport>