DPIA Entree Federatie

een SSO-dienst van Kennisnet

Versie 1.0 (oktober 2024)

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	Ferdy IJsselmuiden (DPIA-projectmanager) Marcel de Rijke (Informatiebeveiligingsspecialist) Hans-Peter Ligthart (portfoliomanager IBP) Job Vos (senior adiviseur privacy)
Met dank aan	Mark Teunissen, Stichting Portuur Peter Harmsen, Tabor College
Auteurs model DPIA (v.1.2)	Hans-Peter Ligthart (portfoliomanager IBP SIVON) Job Vos (jurist en adviseur IBP SIVON) Ferdy IJsselmuiden (DPIA-projectmanager)

Inhoudsopgave

1. Samenvatting

In het moderne onderwijs is de Entree Federatie, ontwikkeld door Kennisnet[1], van vitaal belang voor scholen in Nederland. Het biedt een centrale toegangsoplossing tot verschillende digitale diensten en platforms. Zowel het voortgezet onderwijs als het middelbaar beroepsonderwijs maken gebruik van deze dienst, die ook bekend staat als een Single Sign On (SSO) dienst. Met deze dienst kunnen gebruikers direct toegang krijgen tot de diverse leermiddelen en diensten van de school zonder telkens apart in te hoeven loggen. De Entree Federatie is een facilitator voor de uitwisseling van gegevens tussen de onderwijsinstelling en de dienstaanbieder (bijvoorbeeld uitgever). Deze authenticatiedienst laat zich daarom omschrijven als een soort 'super login'. Daarnaast kenmerkt deze dienst zich ook door het delen met de dienstaanbieder van een standaard set aan minimale gegevens per inlogpoging. Binnen Entree Federatie worden dit de attributen genoemd en bestaan onder andere uit de naam van de gebruiker en het ECK-id.

Entree Federatie is een dienst waar de gebruikers doorgaans geen besef van hebben dat ze deze gebruiken terwijl deze in de tussentijd essentieel is voor het verkrijgen van de digitale toegang tot de verschillende (leer)middelen waar de school licenties voor heeft aangekocht.

Voorafgaand aan het gebruik van een van de leermiddelen van een school, worden persoonsgegevens via de Entree Federatie verwerkt voor authenticatiedoeleinden. Tijdens deze authenticatie wordt beoordeeld of degene die inlogt wel echt de persoon is die hij zegt te zijn. Een DPIA is uitgevoerd om deze verwerking te beoordelen.
Uit het DPIA-onderzoek is gebleken dat de Entree Federatie een veilige methode biedt voor het tot stand brengen van deze koppeling, en de basis biedt om hiervoor alleen minimale en noodzakelijke gegevens beschikbaar te stellen. Bovendien is er tijdens het authenticatieproces geen sprake van opslag van de zogenoemde attributen waarmee de authenticatie plaatsvindt. Dit proces vindt dus "on-the-fly" of ook wel "real-time" plaats.

<u>Samenwerking</u>
De samenwerking tijdens het DPIA-proces met Kennisnet op de dienst Entree Federatie was ronduit positief te noemen. De open werkwijze, goede gesprekken en gemotiveerde houding om verbetervoorstellen door te voeren hebben ontzettend bijgedragen aan het onderzoek en identificatie van de risico's. Daarover gesproken, een belangrijke verbetering van de dienst op het gebied van informatiebeveiliging is het verhogen van de BIV-classificatie op het gebied van de Integriteit van Midden naar Hoog. Nadat SIVON en Kennisnet hier inhoudelijk overeenstemming hadden bereikt is er vlot toegewerkt naar acties en deadlines om dit ook in de praktijk te realiseren. De gedane toezeggingen op dit gebied zorgen ervoor dat de dienst nog een stuk veiliger en robuuster is geworden.
Ook de deelnemende scholen hebben belangrijke praktijkinzichten gebracht die wezenlijk waren voor het begrip van de werking van de dienst.

Voor wat betreft de informatiebeveiliging is gekozen voor het gebruik van het robuuste SAML-mechanisme wat zorgdraagt voor een versterking van de beveiliging van de koppeling

[1] https://www.kennisnet.nl/entree-federatie/

en draagt bij aan de gebruikerservaring voor de scholen. Verder is Kennisnet ISO 27001 gecertificeerd, de dienst Entree Federatie valt onder deze certificering. Dit betekent dat informatiebeveiligingsbeleid cyclisch is verankerd binnen Kennisnet.

Na de implementatie van de overeengekomen maatregelen door zowel de scholen als Kennisnet zijn er voor het gebruik van Entree Federatie geen verdere restrisico's.
Kort na de deadline van de implementatietermijn zal SIVON een update van deze ontwikkelingen op haar website plaatsen.

Risico's en maatregelen:

De volgende risico's zijn uit het DPIA-onderzoek naar voren gekomen waarvan één hoog risico is en drie risico's in ingeschat op midden. Na implementatie van de hierna genoemde maatregelen worden alle risico's verlaagd tot een laag, acceptabel risico.

1.Risico: midden

Verwerking vindt mogelijk plaats in strijd met het uitgangspunt van **dataminimalisatie**. De aanbieders (leveranciers van bijvoorbeeld leermiddelen) die aanvullende attributen voorwaardelijk stellen voor hun dienstverlening motiveren onvoldoende waarom deze gegevens noodzakelijk zijn. Hierdoor is de inschatting als school moeilijk te maken of de uitgevraagde attributen noodzakelijk en proportioneel zijn.

Maatregel:

School: de school die akkoord gaat met het beschikbaar stellen van aanvullende attributen aan de leverancier heeft deze beoordeeld op de noodzakelijkheid. Bij onduidelijkheid is nadere uitvraag van de motivering vereist. De school heeft een proces aanwezig voor het beheer en de controle op het gebruik van Entree Federatie.
NB: de (aanvullende) attributen moeten ook in de verwerkersovereenkomst met de dienstaanbieder staan opgenomen.

Kennisnet: Kennisnet verzoekt de dienstaanbieders indringender om gedetailleerd te motiveren waarom aanvullende attributen voor de koppeling noodzakelijk zijn, zodat scholen goed kunnen inschatten of deze verwerking voldoet aan de beginselen van proportionaliteit en subsidiariteit.
In dit kader zal ook een nieuwe oproep aan de dienstaanbieders worden gedaan om alsnog te voorzien in deze motivering.

2.Risico: hoog

De **informatiebeveiliging** op het gebied van de Integriteit is onvoldoende. Er wordt nog niet volledig voldaan aan de maatregelen die op basis van het ROSA-schema[2] moeten zijn

[2] In deze standaard worden afspraken gemaakt over het (basis)niveau van informatiebeveiliging en privacy voor toepassingen die worden gebruikt binnen in het onderwijs (PO, VO, MBO en HO). Het bepaalt het niveau

geïmplementeerd uitgaande van een BIV-classificatie waarbij de Integriteit op Hoog is gezet. Kennisnet heeft Integriteit op Midden geclassificeerd. Er wordt wel voldaan aan de maatregelen die passen bij de classificatie Midden. Hierdoor is ook onduidelijkheid ontstaan ten aanzien van de classificatie van Integriteit, die in de verwerkersovereenkomst op Hoog staat en in het ROSA-schema op Midden.

Maatregel:

Kennisnet: Kennisnet dient de maatregelen die horen bij 'integriteit Hoog' te implementeren en aan te passen in het ROSA-schema. Hierover zijn concrete afspraken gemaakt met SIVON hetgeen tot de concrete toezegging heeft geleid dat Kennisnet voor uiterlijk eind 2024 zal voldoen aan de betreffende maatregelen. Hierdoor is er geen sprake meer resterende restrisico's.

3.Risico: midden

De inhoud van de **verwerkersovereenkomst** is niet in overeenstemming met de feitelijke verwerkingen. Ten aanzien van de inhoud van de verwerkersovereenkomst zijn de volgende vier gebreken geïdentificeerd.

1. Gebrek aan transparantie en controle over de verwerking van de gegevens. In de tabel van de 'onderwijsdeelnemer' staat het vinkje bij Gebruikersgegevens, waaronder diagnostische gegevens en logging niet aangevinkt is terwijl deze gegevens tijdens het proces wel worden verwerkt.
2. Gebrek aan transparantie en controle over de verwerking van de gegevens. In de tabellen staat dat er tijdens de authenticatie geen persoonsgegevens worden opgeslagen. Dit klopt echter niet voor de gepseudonimiseerde logging.
3. Onjuiste informatievoorziening ten aanzien van de toegepaste beveiligingsmaatregelen. De BIV-classificering in bijlage 2 van de verwerkersovereenkomst staat ten aanzien van de Vertrouwelijkheid ten onrechte op Hoog.
4. De support-tickets worden te lang bewaard en/of niet op tijd verwijderd.

Maatregelen:

Kennisnet:

1. Aanpassen van de verwerkersovereenkomst door aan te vinken dat logging-gegevens bij deelnemers worden verwerkt.
2. Voorzien van duiding over de soort persoonsgegevens die worden verwerkt en voor welk doel in de verwerkersovereenkomst.
3. Verwerkersovereenkomst op gebied van toegepaste BIV-kwalificatie in overeenstemming brengen met de praktijk.

---

voor Betrouwbaarheid, Integriteit en Vertrouwelijkheid van een toepassing en schrijft op basis daarvan de benodigde maatregelen voor (zie Toetsingskader)

4. Aanpassing proces voor labelen support-tickers voor Entree Federatie waarvoor Kennisnet verwerker is, en deze support-tickets na sluiting na 2 jaar verwijderen.

Ten aanzien van de hiervoor benoemde maatregelen is met Entree Federatie overeengekomen dat de verwerkersovereenkomst hierop wordt aangepast voor het begin van het nieuwe schooljaar (uiterlijk augustus 2024). Het werkproces voor verwijderen van gesloten support-tickets wordt binnen één jaar aangepast.

4.Risico: midden

Onrechtmatige verwerking door dienstaanbieder bij inloggen zonder licentie.
Bij het koppelen via de Entree Federatie naar serviceproviders wordt de uitwisseling van de attributen gefaciliteerd. In gevallen waar een licentie is beëindigd of er geen gebruik meer wordt gemaakt, moet ook de koppeling worden beëindigd binnen Mijn Entree Federatie of intrekking van het ARP-formulier. Bij nalaten hiervan resulteert dit in het onbedoeld beschikbaar stellen van persoonsgegevens van een leerling aan een (inmiddels) onbevoegde partij, indien de leerling tracht in te loggen bij deze partij.

Maatregel:

School: de school dient een proces aanwezig te hebben voor het beheer en de controle op de koppelingen met dienstaanbieders die ervoor zorgt dat wanneer een licentie afloopt de koppeling direct wordt ingetrokken. Door het intrekken van deze koppeling in Mijn Entree door de school, worden er geen persoonsgegevens uitgewisseld als de leerling daar toch probeert in te loggen.

2. Introductie en achtergrond DPIA

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

Privacy is enerzijds het recht om met rust te worden gelaten. Anderzijds gaat het over het recht om gegevens over jezelf te kunnen controleren. Als je bij alles wat je doet, gevolgd wordt én je denkt of weet dat dit gevolgen voor jou kan hebben, dan pas je jouw gedrag daarop aan. Zonder het recht op privacy kan een mens niet vrij zijn. Privacy is een randvoorwaarde in een democratische samenleving. Daarom blijft het belangrijk dat scholen privacy goed organiseren. Het beschermen van privacy gaat niet zonder het beschermen van persoonsgegevens; gegevens van betrokkenen mogen immers niet in verkeerde handen vallen. Daarom spreken we vaak over IBP: Informatiebeveiliging en privacy. Een onderdeel daarvan is het gebruik van veilige en verantwoorde ICT-middelen. Een Data Protection Impact Assessment (DPIA) zou je ook kunnen omschrijven als een privacytoets en is een hulpmiddel om vast te stellen of de IBP van een ICT-applicatie op orde is!

I. DPIA

Schoolbesturen of colleges van bestuur (CvB) zijn als verwerkingsverantwoordelijken verplicht om te onderzoeken of persoonsgegevens voldoende beschermd zijn. Daarvoor voeren zij een privacytoets uit: een Data Protection Impact Assessment uit (DPIA). In de AVG wordt dit een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Een DPIA wordt uitgevoerd op een applicatie of verwerking van persoonsgegevens door een leverancier (verwerker). De DPIA wordt uitgevoerd conform de eisen van artikel 35 lid 7 AVG. Bij een DPIA wordt het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens onderzocht. Vastgesteld wordt of het gebruik van persoonsgegevens (verwerking) een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen (leerlingen, hun ouders en medewerkers). De uitkomst van de DPIA is o.a. een rapportage met daarin een overzicht van geclassificeerde risico’s voor de rechten en vrijheden van betrokkenen en mitigerende maatregelen. Mitigerende maatregelen zijn maatregelen die het risico beperken. Alleen indien de hoge risico's voldoende worden beheerst door mitigerende maatregelen, is een gegevensverwerking toegestaan.

Bij applicaties die door veel verwerkingsverantwoordelijken – op dezelfde wijze – worden gebruikt, is het zinvol om deze DPIA samen uit te voeren. Denk bijvoorbeeld aan een leerlingadministratiesysteem. Hierdoor hoeft niet elk schoolbestuur zelf het spreekwoordelijke wiel uit te vinden. SIVON voert daarom in opdracht van OCW namens de gehele onderwijssector zogenaamde **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. Door samen op te trekken staan schoolbesturen via SIVON sterker in de gesprekken met de leverancier. En voor deze leveranciers is duidelijk dat afspraken over verbeteringen alleen via SIVON worden gemaakt in plaats van met vele individuele onderwijsinstellingen. Door deze centrale DPIA's uit te voeren op veel gebruikte systemen, helpt SIVON schoolbesturen op weg om veilig en verantwoord gebruik te maken van persoonsgegevens en ICT.

Schoolbesturen moeten volgens de AVG zelf afwegen wat de risico's zijn voor de rechten en vrijheden van betrokkenen. Dat kan SIVON niet doen. Na de uitvoering van de centrale DPIA moet daarom ieder schoolbestuur de uitkomsten uit de centrale DPIA op hun organisatie toepassen. Daarvoor moeten zij nog wel een **lokale DPIA** uitvoeren en daarin een eigen afweging maken. SIVON helpt besturen hiermee doordat in de centrale DPIA de meest voorkomende risico's voor schoolbesturen worden bepaald. De centrale DPIA wordt voor de lokale DPIA als uitgangspunt genomen, waarbij het schoolbestuur enkel nog een eigen afweging moet maken of de meest voorkomende risico's en maatregelen ook voor hen gelden en of zij nog aanvullende risico's zien op basis van hun eigen omstandigheden.

II. Verplichting 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 (AP) die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van aan DPIA verplicht is[3]. 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.

Beoordeling DPIA Entree Federatie

Tijdens de uitvoering van het authenticatieproces door Entree Federatie worden op een grootschalige schaal en op dagelijkse basis gegevens verwerkt van een kwetsbare groep, te weten minderjarige leerlingen. Omdat er bij deze verwerking wordt voldaan aan een tweetal criteria uit zowel het DPIA besluit[4] als de EDPB-richtsnoeren, betekent dit dat er een DPIA-verplichting geldt op basis van artikel 35 van de AVG.

De Europese toezichthouder European Data Protection Board (EDPB) omschrijft in de Richtsnoeren DPIA negen criteria die relevant zijn bij beoordeling of de verwerking "waarschijnlijk een hoog risico inhoudt". Relevant voor de DPIA op Entree Federatie zijn de volgende criteria:

[3] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf
[4] wetten.nl - Regeling - Besluit lijst verwerkingen persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens - BWBR0042812 (overheid.nl)

Op grote schaal verwerkte gegevens én *gegevens met betrekking tot kwetsbare betrokkenen*.

In de meeste gevallen kan een verwerkingsverantwoordelijke ervan uitgaan dat voor een verwerking die aan twee van deze criteria voldoet een DPIA moet worden uitgevoerd. Hoe groter het aantal criteria waaraan een verwerking voldoet, hoe waarschijnlijker het is dat ze een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen, en dus een DPIA vereist is, ongeacht de maatregelen die de verwerkingsverantwoordelijke voornemens is te nemen. In sommige gevallen kan een verwerkingsverantwoordelijke echter oordelen dat een verwerking die aan slechts één van deze criteria voldoet een DPIA vereist.

Toelichting criteria:
op grote schaal

Een aantal van de criteria is enkel van toepassing bij verwerking op grote schaal. In de AVG wordt niet gedefinieerd wat grootschalig is. De AP en de EDPB geven aan dat met name de volgende factoren in aanmerking moeten worden genomen bij het bepalen of een verwerking op grote schaal wordt uitgevoerd:

- het aantal betrokkenen, hetzij als een specifiek aantal hetzij als een deel van de relevante populatie;
- het volume van gegevens en/of het bereik van verschillende gegevensitems die worden verwerkt;
- de duur, of het permanente karakter, van de gegevensverwerkingsactiviteit;
- de geografische omvang van de verwerkingsactiviteit.

Doordat het inloggen op applicaties via Entree Federatie op een landelijke schaal plaatsvindt door veel leerlingen en leerkrachten/docenten is er sprake van ‘op grote schaal'. De meeste voortgezet onderwijs- (vo) en MBO scholen gebruiken Entree voor ten minste 10 verschillende applicaties. Er wordt ongeveer 145 miljoen keer[5] ingelogd via Entree in een schooljaar.

Gegevens met betrekking tot kwetsbare betrokkenen

De verwerking van gegevens met betrekking tot kwetsbare betrokkenen is een criterium vanwege de machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke, wat betekent dat de natuurlijke personen mogelijk niet in staat zijn om gemakkelijk in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen. Kwetsbare betrokkenen kunnen kinderen omvatten (kinderen kunnen worden geacht niet in staat te zijn om bewust en bedachtzaam in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens), werknemers, kwetsbaardere segmenten van de bevolking die speciale bescherming behoeven (geesteszieken, asielzoekers, bejaarden, patiënten enz.), en in elk geval waarin een onevenwichtigheid in de relatie tussen de positie van de betrokkene en de verwerkingsverantwoordelijke kan worden vastgesteld.

[5] Zie: https://www.kennisnet.nl/artikel/6832/entree-federatie-ervaringen-uit-de-praktijk/

De Autoriteit Persoonsgegevens (hierna: AP) heeft veelvuldig aangegeven dat de gegevens van minderjarige leerlingen kwalificeren als gevoelig. Zie in dit kader bijvoorbeeld de volgende passage uit de brief van de AP aan het Ministerie van Onderwijs, Cultuur en Wetenschap[6]: “Kinderen hebben recht op een passende invulling van hun grondwettelijke recht op bescherming van persoonsgegevens en dienen te worden beschermd tegen schendingen van dat grondrecht. Een juiste borging van dat grondrecht vergt extra aandacht bij kinderen. Zij hebben volgens de AVG, het Handvest en het Verdrag inzake de rechten van het kind recht op specifieke bescherming. De AP stelt daarom voorop dat bij het inschatten van de risico’s aangaande de verwerking van persoonsgegevens in voldoende mate de specifieke risico’s voor kinderen moeten worden geïdentificeerd en onderzocht. Dit vergt een nauwkeurige analyse van de specifieke risico’s voor kinderen en de uitwerking die deze risico’s hebben op kinderen van verschillende leeftijden. Daarbij is het onvoldoende om kinderen te positioneren als betrokkenen met alleen een lagere leeftijd, aangezien kinderen zich minder bewust zijn van de betrokken risico’s en gevolgen van de verwerking van hun persoonsgegevens. Daarbij kunnen risico’s een andere impact en uitwerking hebben op kinderen dan op volwassenen. Het stelselmatig vastleggen van gegevens over het gedrag en de ontwikkeling van kinderen kan leiden tot risico’s zoals discriminatie en uitsluiting. Bovenstaande leidt tot de conclusie dat er bij de verwerking van persoonsgegevens van kinderen extra zorgvuldig zal moeten worden onderzocht welke risico’s er spelen en welke waarborgen passend zijn.”

III. Toetsing rolverdeling verwerkingsverantwoordelijke en verwerker

Bij de DPIA wordt uitgegaan van een rolverdeling tussen school en leverancier gebaseerd op de Algemene verordening gegevensbescherming (AVG). Onder de AVG is een schoolbestuur **verwerkingsverantwoordelijke** die te allen tijde de controle moet houden over de persoonsgegevens (privacy) van haar leerlingen, hun ouders en medewerkers. Het schoolbestuur bepaalt dus voor welke doelen deze gegevens mogen worden gebruikt. Een leverancier van software waarin de persoonsgegevens ‘van de school’ zijn opgenomen, wordt **verwerker** genoemd. Deze mag die persoonsgegevens niet zomaar voor eigen doeleinden gebruiken. Gebruik van persoonsgegevens bijvoorbeeld voor de verbetering van de dienst, is dus niet zomaar toegestaan. Het (her)gebruik van persoonsgegevens van leerlingen, hun ouders en medewerkers wordt daarom door het schoolbestuur vastgesteld. Het gaat hierbij om gerechtvaardigde legitieme (zakelijke) doeleinden. Vaak zal een leverancier die persoonsgegevens wil hergebruiken, de gegevens moeten pseudonimiseren of anonimiseren zodat ze niet meer (direct) herleidbaar zijn tot personen.

In alle gevallen is het uitgangspunt dat de leverancier verwerker is en dat verwerking van persoonsgegevens beperkt is tot legitieme doeleinden. Een leverancier kan ook persoonsgegevens verwerken als verwerkingsverantwoordelijke. Denk hierbij aan de

[6] Brief AP aan Ministerie van Onderwijs, Cultuur en Wetenschap 31 mei 2021, raadpleegbaar via https://open.overheid.nl/repository/ronl-04a1a178-a812-407c-a4ac-28e649d66b1f/1/pdf/advies-autoriteit-persoonsgegevens-inzake-google-g-suite-for-education.pdf.

gegevens van de beheerder van de dienst, die gegevens geregistreerd om een rekening te sturen etc.

IV. Centrale DPIA versus lokale DPIA

Een centrale DPIA wordt uitgevoerd door SIVON op systeemniveau. Een centrale DPIA toetst of en wat de impact is van het gebruik (verwerking) van het systeem in relatie tot de bescherming van persoonsgegevens. Hoe kan het systeem veilig gebruikt worden en welke (extra) maatregelen en instellingen zijn daarvoor nodig?

De toetsing of er sprake is van adequate gegevensbescherming, wordt in het kader van een DPIA ingegeven door de:

1. **gegevensverwerkingsanalyse:** kenmerken van de (voorgenomen) gegevensverwerkingen: een beschrijving van de voorgenomen verwerkingen, een complete inventarisatie van de te verwerken persoonsgegevens, de verwerkingsdoeleinden en werking van het systeem,
2. **rechtmatigheid van de gegevensverwerkingen:** beoordeling van de rechtsgrond, de noodzaak, evenredigheid en verenigbaarheid van de voorgenomen verwerkingen in relatie tot de verwerkingsdoeleinden,
3. **aanwezige risico's**: beoordeling van de gevolgen van de verwerkingen voor de rechten en vrijheden van de betrokkenen,
4. **maatregelen:** adequate technische en organisatorische (beveiligings)maatregelen die zijn of worden genomen om de gevolgen (van de risico's) te beperken.

In het proces rondom de uitvoering van de DPIA, worden o.a. de volgende elementen uitgevoerd en opgeleverd:

1. Het beoordelen van (privacy) afspraken in de verwerkersovereenkomst en vastleggen van eventuele (verbeter)afspraken;
2. Het (technisch) toetsen van het systeem of dit voldoet aan de gemaakte afspraken;
3. Het maken van afspraken over maatregelen die nog niet zijn genomen maar op grond van de DPIA wel nodig zijn;
4. Een correcte implementatie van het systeem binnen de school;
5. Omgang door gebruikers en beheerders met de systemen (beleid en gedragscodes).

In de centrale DPIA worden de punten 1, 2 en 3 uitgevoerd door SIVON. Het schoolbestuur krijgt aanbevelingen voor punt 4 (bijvoorbeeld in de vorm van een technische handleiding). De school zal zelf met punt 5 aan de slag moeten.

In de lokale DPIA neemt de school – voor zover van toepassing – de punten 1, 2, en 3 over. Hierbij past de school de centrale bevindingen toe op de eigen organisatie: zijn alle onderdelen ook van toepassing op eigen organisatie? Er wordt beschreven op welke wijze op de school invulling wordt gegeven aan de implementatie (punt 4). Daarbij wordt overwogen of er nog specifieke risico's spelen en maatregelen nodig zijn die niet in de centrale DPIA benoemd zijn. De school zorgt zelf voor punt 5: een school zal zelf interne richtlijnen moeten opstellen wie toegang heeft tot welke persoonsgegevens en data en hoe

het verstrekken en intrekken van autorisaties georganiseerd is, etc. Welke handelingen je met welke ICT-middelen mag uitvoeren ligt vast in een intern beleid of gedragscode.

De lokale DPIA is dus 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.

V. Gebruik model

De centrale DPIA volgt het model van de Rijksoverheid[7], aangevuld met onderwijs-specifieke informatie uit de *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*[8]. Het model is daarnaast aangepast aan specifieke informatie over het systeem en aangevuld met een model lokale DPIA.

Hierbij wordt rekening gehouden met de richtlijn van de gezamenlijke Europese toezichthouders, (EDPB) die in de Richtsnoeren voor gegevensbeschermingseffectbeoordelingen (2016/679, 4 april 2017) overwegen:

"De [EDPB] stimuleert de ontwikkeling van sectorspecifieke kaders voor gegevensbeschermingseffectbeoordelingen. De reden hiervoor is dat dergelijke kaders kunnen steunen op specifieke sectorkennis, wat betekent dat de gegevensbeschermingseffectbeoordeling kan worden gericht op de bijzonderheden van een bepaald type verwerking (bijvoorbeeld bepaalde soorten gegevens, bedrijfsactiva, mogelijke effecten, bedreigingen, maatregelen). Dit betekent dat de gegevensbeschermingseffectbeoordeling de problemen kan aanpakken die zich voordoen in een bepaalde economische sector, bij gebruik van specifieke technologieën of bij uitvoering van bepaalde soorten verwerkingen."

Deze DPIA bestaat derhalve uit 5 delen:

- Deel A is de beschrijving kenmerken gegevensverwerkingen (gegevensverwerkingsanalyse).
- Deel B is de beoordeling rechtmatigheid gegevensverwerkingen.
- Deel C is de beschrijving en beoordeling risico's voor de betrokkenen.
- Deel D is de beschrijving voorgenomen maatregelen die risico's moeten beperken.
- Deel E is het model lokale DPIA.

VI. Scope van deze DPIA

Deze DPIA heeft tot doel helder inzicht te verschaffen in het gebruik van Entree Federatie binnen het onderwijs. Entree Federatie is een publieke toegangsdienst van Kennisnet welke

[7] rapportagemodel-dpia-rijksdienst-v2-0-aangepast-cf-toegangscontrole.docx (live.com)
[8] https://aanpakibp.kennisnet.nl/app/uploads/Handreiking-DPIA-v1.0-1.pdf

tot doel heeft om op een gemakkelijke manier toegang te bieden tot digitale leermaterialen en educatieve diensten.

Leerkrachten en leerlingen kunnen via de aangeboden techniek vanuit hun werkomgeving direct inloggen op de digitale aanbieders van leermiddelen. In het overzicht van aangesloten diensten kom je verschillende partijen tegen, zoals de uitgevers Noordhoff en Malmberg[9]. Deze aanbieders leveren hoofdzakelijk online lesmateriaal en educatieve diensten. De kern van de dienst Entree Federatie is het mogelijk maken van een veilige en efficiënte inlogprocedure voor gebruikers, waarbij één keer inloggen toegang biedt tot alle materialen van verschillende aanbieders van lesmateriaal die de school heeft ingekocht. Dit wordt gerealiseerd door middel van een *Single Sign On* dienst (SSO), die beoogt op een uniforme en transparante wijze een minimale set persoonsgegevens te delen met de aangesloten partijen. De DPIA op deze dienst richt zich daarom op de aspecten van identificatie, authenticatie, gegevensuitwisseling en het beheer van (technische) diensten binnen het systeem.

Binnen de scope van de DPIA vallen specifieke verwerkingen, waaronder:

- **Het authenticatieproces:** Dit houdt in dat attributen (persoonsgegevens) van de onderwijsinstelling worden doorgegeven aan de aangesloten dienstverlener tijdens het authenticatieproces, waarbij de gebruiker inlogt op de betreffende dienst.
- **Support & beheer:** Hierbij worden contactgegevens van beheerders en hun acties (logging) namens de organisatie vastgelegd in "Mijn Entree Federatie" en/of de beheermodule van Entree Federatie.

De DPIA geeft daarmee een gestructureerd overzicht van de specifieke verwerkingen die plaatsvinden binnen het Entree Federatie-systeem in het onderwijs, en legt de focus op het waarborgen van privacy en gegevensbescherming binnen deze context.

VII. Buiten scope

Buiten scope van de DPIA valt de mogelijkheid om een persoonlijk account aan te maken voor Entree Federatie via de website van Kennisnet (**Entree Account**). Dit is o.a. mogelijk wanneer een school niet is aangesloten op Entree Federatie[10]. Voor deze verwerking is Kennisnet zelf verwerkingsverantwoordelijke.

Ook de **aanbieders** (leveranciers) die aansluiten op Entree Federatie zijn buiten scope. Het gaat om het door een school in gebruik nemen van een aanbieder die is gekoppeld aan de toegang via Entree Federatie. De omgeving en verwerkingen binnen de educatieve leermiddelen en digitale diensten of andere op het portaal van Entree Federatie

[9] Entree Federatie Catalogus (kennisnet.nl)
[10] https://www.kennisnet.nl/diensten/entree-federatie/account/

aangesloten diensten en aanbieders van online lesmateriaal waartoe Entree Federatie haar inlogdiensten verleend vallen buiten de scope van de DPIA.

De **beoordeling van de motivatie op de aanvullende attributen**: aanbieders kunnen ten behoeve van de koppeling met Entree Federatie verzoeken om zogenoemde Aanvullende attributen. De beoordeling van de noodzakelijkheid valt buiten de scope van deze DPIA. Dit betreft een beoordeling door de school.

VIII. Methodiek

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

- Beoordeling van de verwerkingen, (verwerkers)overeenkomsten, de te verwerken persoonsgegevens in relatie tot het doel, de rechtmatigheid, alsmede in hoeverre de verwerking van de persoonsgegevens voldoet aan de beginselen van de AVG, de risico's en de maatregelen;
- Beoordeling van de BIV-kwalificatie aan de hand van het ROSA certificeringsschema;
- Beoordeling van de mogelijkheid om als verwerkingsverantwoordelijke te voldoen aan rechten van betrokkenen;
- Beoordeling van de default settings (privacy by design);
- Analyse van de wijze waarop het systeem voorziet in logging en de wijze waarop dit door de onderwijsinstelling gemonitord kan worden;
- Opstellen rapportage;
- Overleg met leverancier over (aanvullende) maatregelen.

De centrale DPIA is uitgevoerd in de periode van oktober 2023 tot mei 2024 door SIVON met medewerking van de schoolbesturen van het Tabor College te Hoorn en Stichting Portuur gevestigd in de Achterhoek en Twente.

IX. Definitie van verschillende gegevens

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.

Aanbieders zijn leveranciers van digitale onderwijsmiddelen zoals educatie leermiddelen, digitale diensten of andere op het portaal van Entree Federatie aangesloten diensten waartoe leerlingen en medewerkers van de school via Entree Federatie op inloggen. De (diensten en software van) aanbieders zijn buiten scope van deze DPIA.

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.

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

Gevoelige persoonsgegevens gaan over gegevens die volgens de 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[11] zwaardere eisen gesteld aan de beveiliging van de gegevens.

Inhoudelijke gegevens betreft 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

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

persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijkt en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormt. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers. Denk hierbij aan:

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

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

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

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

Pseudonieme persoonsgegevens Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis 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[12].

Privacyconvenant Onderwijs

Het Convenant digitale onderwijsmiddelen en privacy vertaalt de AVG naar de onderwijspraktijk. Het bevat afspraken over het omgaan met persoonsgegevens bij het gebruik van digitale leermiddelen en toetsen. Dankzij het convenant weten scholen en aanbieders wat ze over en weer van elkaar mogen verwachten, zijn de afspraken werkbaar in de praktijk en heeft iedereen dezelfde gemeenschappelijke uitleg bij deze afspraken. Het Convenant Digitale Onderwijsmiddelen en Privacy 4.0 en de bijbehorende documenten, zoals de Model Verwerkersovereenkomst en het Reglement, zijn terug te vinden op www.privacyconvenant.nl.

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

3. 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

Entree Federatie is een product van Kennisnet[13] dat via een platform eenvoudige en snelle toegang biedt tot digitale leermiddelen en educatieve diensten. Kennisnet ondersteunt scholen bij de professionele inzet van ICT en treedt hierbij in de rol van ontwikkelaar en dienstverlener van publieke ict-voorzieningen zoals Entree Federatie.

Door eenmaal in te loggen via deze Single Sign On dienst (hierna: SSO), krijgen gebruikers toegang tot alle diensten van aanbieders van online (les)materiaal die zijn aangesloten op het portaal van Entree Federatie. Deze koppeling vindt “onder water” plaats. Als gebruiker klik je dus op de aanbieder van jouw keuze waardoor het inloggen automatisch plaatsvindt.

Daar waar je als gebruiker in het andere geval per aanbieder, zoals een uitgever, inlogt met verschillende gebruikersnamen en wachtwoorden, biedt de SSO-dienst van Entree Federatie eenvoudige toegang tot verschillende partijen.

Dit platform is kosteloos voor alle gebruikers, inclusief de aangesloten scholen en aanbieders.

Entree Federatie kenmerkt zich door op een transparante manier inzicht te geven in de gedeelde persoonsgegevens met de aangesloten partijen en de veilige authenticatie techniek welke aan de hand van SAML-verzoeken[14] plaatsvindt. Het systeem kan worden gebruikt met zowel een eigen schoolaccount als een Entree-account.

Entree Account

Voor scholen zonder Identity Provider kan gebruik worden gemaakt van inloggen bij aanbieders aan de hand van een Entree Account. Dit is een dienst, in beheer bij Kennisnet, voor eindgebruikers welke kan worden aangemaakt via de website[15] van Kennisnet. Het aanmaken van dit account gaat door middel van het invoeren van een naam en mailadres. Vervolgens kan met dit account toegang worden verkregen tot de verschillende aanbieders. Toegang tot gevoelige informatie zoals leerling- en/of leerkrachtgegevens is echter niet mogelijk. Hoewel met dit account op bij verschillende leveranciers kan worden ingelogd zal de toegang beperkt zijn tot de algemene en openbare informatie. Entree Account is een

[13] Wie wij zijn - Wie wij zijn (kennisnet.nl)

[14] SAML staat voor **Security Assertion Markup Language** en is een van de meest gebruikte standaarden voor het uitwisselen van authenticatiegegevens. SAML maakt veilige Single Sign-On mogelijk. Gebruikers hoeven zich eenmalig te authentiseren waarna zij niet meer opnieuw hoeven aan te loggen.

[15] https://www.kennisnet.nl/entree-federatie/mijn-account/

persoonsgebonden account en dus geen schoolaccount dat valt onder de directe verantwoordelijkheid van de onderwijsinstelling.

Toelichting Entree Federatie: *Is uw school niet aangesloten op Entree Federatie? Of heeft u geen schoolaccount? Dan kunt u eenvoudig zelf een persoonlijk Entree Account aanmaken. U heeft hiervoor alleen een uniek e-mailadres nodig. De toegang tot educatieve content is met een Entree Account mogelijk beperkt tot algemeen beschikbaar materiaal, omdat de aanbieders niet weten bij welke school u hoort.*

Technische infrastructuur

De SSO-dienstverlening van de Entree Federatie is een technische infrastructuur: een centraal knooppunt waarlangs alle authenticatieverzoeken worden afgehandeld. Zo hoeft een onderwijsinstelling niet zelf met alle aanbieders te koppelen, maar volstaat één koppeling met de Entree Federatie.
De leerling of leerkracht logt in op de eigen (school)omgeving en kan vanuit daar rechtstreeks toegang krijgen tot de door de school ingekochte aanbieders van digitale leermiddelen. De feitelijke uitwerking hiervan is dat er op deze manier direct geklikt kan worden op de snelkoppeling van bijvoorbeeld een uitgever welke zonder verdere inloghandelingen toegang biedt tot de inhoud.

Technische werking Entree Federatie

De werking van Entree Federatie is een samenspel van aanbieders van een digitaal leermiddel of educatieve dienst (Service Provider), de beheerders van de identiteiten (Identity Providers) en de dienst Entree Federatie (EF).
Entree Federatie identificeert en authentiseert de identiteiten van leerlingen, studenten en medewerkers van een onderwijsinstelling. Dit doet zij door een attributenset op te vragen bij de Identity Provider van de school. Tijdens de authenticatie filtert Entree Federatie de benodigde attributen voor het goed functioneren van de aangesloten dienst van de aanbieder.

<u>Digitale aanmelding “Mijn Entree Federatie”</u>

De school heeft de mogelijkheid om diensten van aanbieders te activeren of deactiveren in "Mijn Entree Federatie[16]”. Dit is de digitale omgeving die vanuit de school te gebruiken is en waar vanuit toestemming gegeven kan worden voor zowel de toegang tot de aanbieders ten behoeve van de leerlingen en medewerkers als het akkoord gaan met eventuele Aanvullende attributen en hoe de aanbieder hiermee omgaat. Hierover later meer (zie hoofdstuk 16a.).
Binnen deze digitale omgeving kan de school een keuze maken over welke diensten zij willen gebruiken. Toegang tot deze digitale omgeving kan enkel via E-herkenning[17].

[16] Mijn Entree Federatie - Entree Federatie (kennisnet.nl)
[17] E-herkenning is een digitale identificatiemethode in Nederland die bedrijven en organisaties gebruiken om veilig en betrouwbaar online toegang te krijgen tot diverse overheidsdiensten en zakelijke dienstverleners. eHerkenning | Homepage

Daarnaast kan er binnen deze omgeving inzicht worden verkregen in hoeveel authenticaties er per maand plaatsvinden en het aantal per aanbieder (digitaal (leer)middel).

Mijn Entree Federatie

Inloggen als beheerder bij mijn Entree Federatie gaat door middel van multi factor authenticatie. De rol van beheerder wordt doorgaans vervult door een ICT-coördinator of applicatiebeheerder. Gebruikers zoals leerlingen en leerkrachten hebben geen toegang tot de “Mijn Entree Federatie” omgeving. De volgende door de aanbieder beschikbaar te stellen informatie wordt aan de gebruiker getoond binnen de digitale omgeving van “Mijn Entree Federatie":

- Motivering aanvullende attributen;
- Is het Privacyconvenant ondertekend (ja/nee);
- Waar de persoonsgegevens worden verwerkt (binnen/buiten EER);
- De eindgebruikerslicentie van de dienst (voorzien van een linkje).

Voorafgaand aan de acceptatie/koppeling van een dienstaanbieder binnen Mijn Entree Federatie dient de school akkoord te gaan met de volgende door Entree Federatie gestelde condities aan de hand van het aanvinken van een checkbox:

- *De benodigde attributen worden door uw IdP met de dienstaanbieder gedeeld.*
- *De school draagt de verantwoordelijkheid om met de dienstaanbieder een verwerkersovereenkomst af te sluiten.*
- *De school sluit, indien nodig, een licentieovereenkomst af met de dienstaanbieder.*

□ *Ik verklaar dat ik de condities ken en accepteer*

Vervolgens kan de bevestiging van de aanvraag plaatsvinden door op de ACTIVEREN knop te drukken.

Logging binnen Mijn Entree Federatie ziet op elke wijziging die betrekking heeft op de aan- of afmelding bij een dienstaanbieder. De logging op het niveau van leerlingen en leerkrachten kan worden bekeken vanuit de Identity Provider (IDP) van de desbetreffende school. Detectie vanuit meermaals onjuist inloggen is enkel zichtbaar vanuit de IDP van de school, dit betekent dat risico's ten aanzien van zogenoemde brute force aanvallen vanuit de school gemitigeerd moeten worden.

Niet-digitale aanmelding

Voor de scholen die (nog) geen gebruik maken van de digitale omgeving kan gebruik worden gemaakt van ARP-formulieren. ARP is een afkorting van attribute release policy. Dit is een schriftelijk verzoek van een onderwijsinstelling aan Stichting Kennisnet ten behoeve van de dienst Entree Federatie om informatie van een gebruiker door te geven aan een aanbieder. Deze informatie ziet op de standaard en aanvullende attributen (zie voor de ’standaard’ en aanvullende attributen: paragraaf 2 van dit hoofdstuk.) Deze fysieke aanvraagprocedure zal worden uitgefaseerd zodat op termijn enkel nog via de digitale omgeving van Mijn Entree

Federatie de toegang tot diensten en de daarvoor gebruikte persoonsgegevens kan worden beheerd.

Aanbieders

Entree Federatie stelt voorwaarden aan de aanbieder welke zijn vastgelegd in de aansluitovereenkomst. Een van deze voorwaarden is dat de aanbieder een adequaat beleid heeft voor de behandeling van datalekken en de gebruiker onmiddellijk zal informeren bij een datalek met betrekking tot de geleverde dienst. Verder neemt de aanbieder maatregelen en vervolgstappen om de gevolgen van het datalek te beperken en herhaling te voorkomen, deze verplichting geldt ook voor de mogelijke derde partijen die zij inschakelt. Verder wordt met de aanbieder overeengekomen dat op verzoek van de gebruiker de aanbieder aanvullende beveiligingsmaatregelen zal treffen in geval van een datalek, bedreiging of incident met betrekking tot de beschikbaarheid, integriteit of vertrouwelijkheid van de dienst. Tot slot wordt de aanbieder verplicht zorgvuldig en veilig om te gaan met de dienst en de verstrekte identificatie-, authenticatie- en/of autorisatiegegevens. Entree Federatie heeft aangegeven zonder concrete aanleiding geen onderzoeken uit te voeren naar de naleving van deze vereisten.

Gegevensuitwisseling.

Entree Federatie slaat tijdens het authenticatieproces geen persoonsgegevens op, de koppeling vindt realtime plaats. Het fungeert als een facilitator voor de uitwisseling van gegevens tussen de Identity Provider van de onderwijsinstelling en de dienstaanbieder.

2. Persoonsgegevens

Entree Federatie slaat tijdens het authenticatieproces geen persoonsgegevens op. Het fungeert echter als een facilitator voor de uitwisseling van gegevens tussen de Identity Provider van de onderwijsinstelling (bijvoorbeeld een Leerling Administratie Systeem) en de dienstaanbieder (bijvoorbeeld een digitale uitgever). Hoewel er geen sprake is van de opslag van persoonsgegevens in dit proces is er wel sprake van een verwerking in de zin van de AVG, immers vindt de uitwisseling van attributen plaats.

De volgende categorieën van persoonsgegevens worden verwerkt:

- *Leerlingen (onderwijsdeelnemer)*
- *Medewerkers onderwijsinstelling*

Persoonsgegevens

Ten behoeve van de koppeling via Entree Federatie kunnen de onderstaande attributen beschikbaar worden gesteld aan de aanbieder.

Standaard attributentabel

Attribuutnaam	Beschrijving	Formaat	Voorbeeld en doelbinding
uid	Uniek ID van de gebruiker. Dit is een versleutelde versie van de gebruikersnaam en het employeeNumber, gevolgd door de omgeving (realm)	hash@realm	qj7cks8qdz9ph54@petteflatcollege Hiermee herkent de dienstaanbieder de gebruiker, zodat deze 'single sign on' kan inloggen vanaf de schoolomgeving
givenName	Voornaam	vrij tekstveld	Pietje Wordt doorgegeven om de gebruiker op een vriendelijke manier aan te kunnen spreken
eduPersonAffiliation**	Rol	student, employee, staff of affiliate	Student Wordt doorgegeven om docenten te kunnen onderscheiden van leerlingen. Docenten krijgen vaak andere functionaliteit aangeboden in de educatieve applicaties van de dienstaanbieders
nlEduPersonHomeOrganizationId	BRIN nummer van de instelling	vrij tekstveld	11ZZ03 Hiermee herkent de dienstaanbieder de Entree koppeling van de school, zodat de gebruiker gerelateerd kan worden tot lesmateriaal van de school, of in groepen van de school geplaatst kan worden
nlEduPersonHomeOrganization	Naam van de instelling	vrij tekstveld	Petteflat College Wordt gebruikt om leesbaar te communiceren om welke school het gaat

Attribuutnaam	Beschrijving	Formaat	Voorbeeld en doelbinding
eckId *	Uniek ECK pseudoniem voor leerling of docent [2]	tekstveld	Het ECK ID wordt gebruikt om de leerling uniek te identificeren in de keten. Dit attribuut wordt alleen doorgegeven als uw school via een separate procedure heeft getekend voor het gebruik van het ECK ID.

Aanvullende attributentabel

Attribuutnaam	Beschrijving	Formaat	Voorbeeld
nlEduPersonRealId [1]	Onversleutelde versie van het uid	[userId]@[realm]	pietjepukkelen@petteflatcollege
nlEduPersonProfileId	ECK keten-ID Indien een school meerdere administraties voert kan het administratienummer worden toegevoegd achter het @, zoals in het voorbeeld	leerlingnummer@administratienummer.schooldomein.nl	95312@1.kennisnet.nl
nlEduPersonTussenvoegsels	Tussenvoegsel	vrij tekstveld	van
sn	Achternaam	vrij tekstveld	Pukkelen
mail	E-mailadres	vrij tekstveld	pietjepukkelen@petteflatcollege.nl
initials	Initalen	vrij tekstveld	P.
nlEduPersonBirthDate	Geboortedatum	yyyymmdd	19801231
nlEduPersonProfile	Opleidingsnaam voorafgegaan door CREBO[spatie]. Optioneel kan BOL_ of BBL_ toegevoegd worden voor de opleidingsnaam	vrij tekstveld	2345 BOL_ICT.Gamedeveloper
nlEduPersonDepartment	Afdeling of sector	vrij tekstveld	Techniek
nlEduPersonUnit	Primaire klas/groep. Uniek binnen administratie / schooldomein	vrij tekstveld	H2A
ou	Klas of groep	vrij tekstveld	H2A

Attribuutnaam	Beschrijving	Formaat	Voorbeeld
nlEduPersonCohort	Startjaar	vrij tekstveld	2014
ocwILTRegistratiecode	ILT Registratiecode Conform bijlage I en II, behorende bij artikel 1 van de Regeling van de Minister OCW houdende vaststelling van de Elementcodetabel en Vakcodetabel VO en Volwasseneneducatie: nr. DUO/OND-2013/15135 M.	vier cijferige-code	0011
ocwILTLeerjaar	ILT Leerjaar Conform bijlage I en II, behorende bij artikel 1 van de Regeling van de Minister OCW houdende vaststelling van de Elementcodetabel en Vakcodetabel VO en Volwasseneneducatie: nr. DUO/OND-2013/15135 M.	1 cijfer	1
digiDeliveryId	ECK digitaal afleveradres	tekstveld	ED8AE607-WI3N-414C-T87A-624E74S7T005
nlEduPersonHomeOrganizationBranchId	Vestigingsnummer (BRIN 6)	String van 6 alfa-numerieke karakters	11ZZ03
nlEduPersonTargetedId	Badge ID	tekstveld	1234567890123456789 0

Persoonsgegevens	Medewerker	Stagiair / LIO	Vrijwilligers	Externen	Sollicitant	Minderjarige leerling
Algemene contactgegevens	X					X
Klas / leerjaar/ ILT-code	X					X
Gegevens met het oog op de organisatie van het onderwijs (zoals een rooster) en het verstrekken of ter beschikking stellen van leermiddelen	X					X

Persoonsgegevens	Medewerker	Stagiair / LIO	Vrijwilligers	Externen	Sollicitant	Minderjarige leerling
Feiten en waarderingen over iemand zijn gedragingen, eigenschappen of opmerkingen						
Geboortedatum	X					X
Personeelsnummer						
Nationaliteit en geboorteplaats						
Gezondheidsgegevens (op eigen verzoek t.b.v. beheersmaatregel)						
Godsdienst (op eigen verzoek t.b.v. beheersmaatregel)						
Gesprekscyclus (documenten)						
Ervaringen (werkervaring en opleidingen)						
Gegevens met betrekking tot financiën						
Beeldmateriaal						
Verzuimregistratie						
BSN						
Gebruiksgegevens	X					X

Overzicht tabel

De hiervoor genoemde informatie wordt samengebracht in één tabel. Hierin wordt direct het onderscheid gemaakt tussen de informatie uit de Standaard attributenset (S) en de Aanvullende attributenset (A).

Categorie betrokkene	Categorie persoonsgegevens	Persoonsgegeven	Bron/verkrijging persoonsgegeven
Minderjarige leerlingen	Algemene contactgegevens	Voornaam S Achternaam A E-mailadres A Initialen A Geboortedatum A	Identity provider school
Minderjarige leerlingen	Overige (contact)gegevens	UID*S	Identity provider

Categorie betrokkene	Categorie persoonsgegevens	Persoonsgegeven	Bron/verkrijging persoonsgegeven
		Rol (student/ employee, staff of affilliate) S BRIN nummer van de instelling S Naam van de instelling S Eckid ** S UID onversleuteld A ECK keten-ID*** A Opleidingsnaam A Afdeling of sector A (Primaire) klas/groep A Startjaar A ILT Registratiecode A ILT leerjaar A ECK digitaal afleveradres A Vestigingsnummer (BRIN 6) A Badge ID A	school
Medewerker	Algemene (contact)gegevens	UID*S Voornaam S Rol (student/ employee, staff of affilliate) S BRIN nummer van de instelling S Naam van de instelling S UID onversleuteld A Achternaam A E-mailadres A Initialen A Geboortedatum A Opleidingsnaam A Afdeling of sector A (Primaire) klas/groep A Startjaar A ILT Registratiecode A ILT leerjaar A ECK digitaal afleveradres A Vestigingsnummer (BRIN 6) A Badge ID A	Identity provider school

* UID: Uniek ID van de gebruiker. Dit is een versleutelde versie van de gebruikersnaam en het employeeNumber, gevolgd door de omgeving (realm).

** ECK-ID: Uit 128 karakters bestaand versleuteld uniek iD t.b.v. gegevensuitwisseling onderwijsmiddelen.

*** ECK-keten ID: Indien een school meerdere administraties voert kan het administratienummer worden toegevoegd achter het @, zoals in het voorbeeld.

3. Gegevensverwerkingen

De verwerkingen door Entree Federatie vinden primair plaats om leerlingen, leerkrachten en onderwijsondersteunende medewerkers (gebruikers) in staat te stellen om toegang te verlenen (authenticatie van de gebruiker) tot online educatief materiaal door middel van één uniforme inlogprocedure. Voor de opsomming van de verwerkingen die binnen de Entree Federatie plaatsvinden is aansluiting gezocht bij de referentiearchitectuur (FORA[18] voor het primair en voortgezet onderwijs) en de verwerkersovereenkomst. Verwerkingen bij het gebruik van SSO-toegangsvoorziening van Entree Federatie vinden plaats ten behoeve van de volgende FORA processen:

- Inkoop en contractbeheer, ICT ondersteuning en onderwijsuitvoering;
- Informatiebeveiliging en privacy;
- Instroom, doorstroom, uitstroom.

Deze FORA-processen behelzen de volgende feitelijke gegevensverwerkingen:

1. Faciliteren toegang tot aanbod leermateriaal. Authenticatie door middel van het koppelen van de identity provider met de serviceprovider;
2. Logging van activiteiten;
3. Technische ondersteuning.

Het authenticatieproces via Entree Federatie werkt als volgt:

Stap 1: De leerling logt, d.m.v. gebruikersnaam en wachtwoord, in op zijn schoolomgeving (bijvoorbeeld Active Directory of ELO)
Stap 2: De schoolomgeving vraagt de Entree Federatie (EF) om een cookie op de computer van de leerling te plaatsen (Identity Provider = schoolnaam.nl)
Stap 3: De versleutelde cookie wordt op de computer van de leerling geplaatst door EF
Stap 4: De leerling gaat naar een educatieve website
Stap 5: De website wil weten wie de onbekende gebruiker is
Stap 6: De website vraagt EF om de indentiteit van de gebruiker vast te stellen
Stap 7: EF leest het eerder geplaatste cookie uit (Identity Provider = schoolnaam.nl)
Stap 8: EF vraagt de identiteit op bij de Identity Provider die in het cookie staat (=schoolnaam.nl)
Stap 9: De Identity Provider levert de identiteit in de vorm van attributen (ID, Voornaam, Achternaam, etc.)
Stap 10: EF filtert en versleutelt de gegevens, de website ontvangt de identiteit van de leerling
Stap 11: De website bepaalt of de leerling toegang krijgt.

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

Filteren data
Wanneer een gebruiker zich succesvol geauthentiseerd heeft bij de Identity Provider, dan stuurt deze laatste een verklaring over de identiteit van de gebruiker (SAML assertion met attributen) naar de Entree Federatie hub. Entree Federatie op zijn beurt zet dit om in een nieuwe SAML assertion voor de Service Provider. Tijdens het opstellen van dit nieuwe bericht worden alleen de attributen uit de SAML assertion van de Identity Provider overgenomen die voldoen aan de Attribute Release Policy die is afgesproken met de Service Provider.

Feitelijk worden alleen de afgesproken attributen van het oude naar het nieuwe bericht gekopieerd. Dit alles gebeurt on the fly en de inhoud van deze berichten worden in transitie niet opgeslagen in het systeem van Entree Federatie.

Verzoek leverancier extra attributen lopende de dienstverlening
Kennisnet ontmoedigt het toevoegen van Aanvullende attributen nadat een productie koppeling van een dienst is geactiveerd. Er zijn dan namelijk scholen akkoord gegaan met een bepaalde attributenset en daar kan niet zonder toestemming van de scholen attributen aan worden toegevoegd.

Mocht een leverancier toch meer Aanvullende attributen willen dan moet zij een extra productie koppeling met Entree Federatie maken. Voor deze nieuwe koppeling wordt dan de uitgebreidere attributenset geconfigureerd. Vervolgens moet de leveranciers de scholen die de reeds bestaande koppeling gebruiken vragen om de nieuwe koppeling te activeren. Hiermee geven de scholen dan een akkoord op de nieuwe, uitgebreidere attributenset.
De leverancier heeft zelf niet de mogelijkheid om buiten dit proces om te beschikken over Aanvullende attributen.

Helpdesk
In overeenstemming met de verwerkersovereenkomst en de daarin besloten opdracht tot gegevensverwerking biedt Kennisnet, in de rol van verwerker, ondersteuning aan de (eind)gebruikers van Entree Federatie. In het geval van ondersteuningsbehoefte kunnen scholen contact opnemen met Entree Federatie via een telefoonnummer of een algemeen mailadres. Er is voor de gebruikers geen digitale helpdeskomgeving waarbinnen tickets geregistreerd en afgehandeld kunnen worden.

Dit zijn leerlingen en medewerkers van een school die aangesloten is op Entree Federatie en waarvoor de school verwerkingsverantwoordelijke is. Dit vindt plaats aan de hand van technische ondersteuning waarvoor Kennisnet gebruik maakt van Jira als ticketregistratieprogramma (support-tickets). Leerlingen en medewerkers kunnen zowel per mail als telefonisch contact opnemen om hun hulpvraag voor te leggen. Deze wordt vervolgens geregistreerd en afgehandeld. Lopende deze periode heeft de indiener toegang tot de omgeving binnen Jira waarin de status van de afhandeling van de ingediende melding

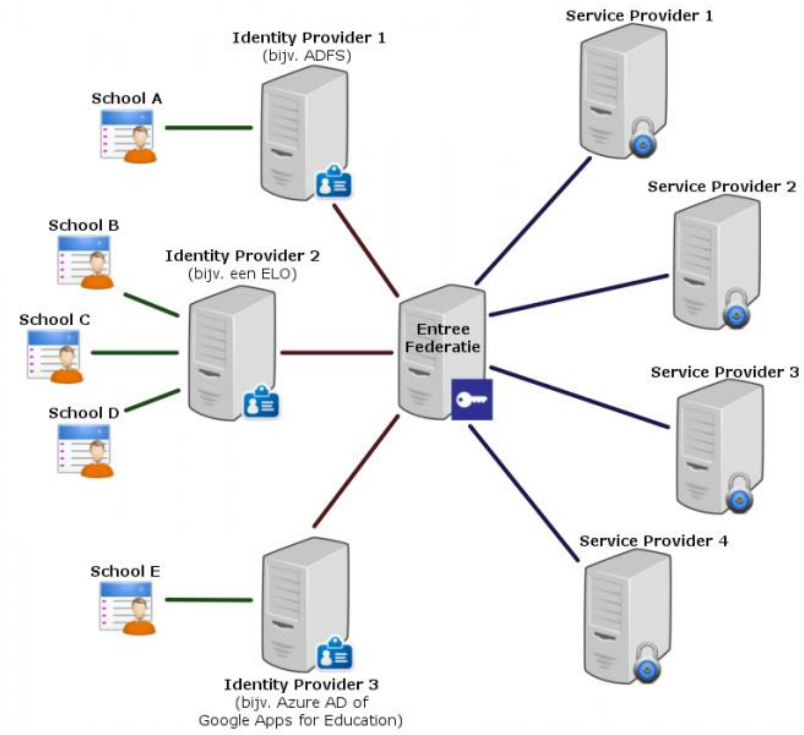
gevolgd kan worden. Het gaat hierbij doorgaans om contactgegevens van de persoon die ondersteuning vraagt en data van en over een verstoring van een federatieve inlog (bijvoorbeeld met screenshots van meldingsschermen). Kennisnet heeft kenbaar gemaakt dat de verwerking van persoonsgegevens die samenhangt met dit proces enkel plaatsvindt ten behoeve van het oplossen van de onderliggende melding. Er is niet gebleken dat Kennisnet buiten deze doeleinden treedt. Zo worden er bijvoorbeeld geen vragenlijsten uitgestuurd of producten door Kennisnet aangeboden.
Gevoelige informatie en persoonsgegevens in support-tickets die niet langer nodig zijn voor het oplossen van het issue, worden - bij sluiten van het support-ticket – verwijderd uit het support-ticket. Kennisnet analyseert de doorlooptijd en aantallen support-tickets om de dienstverlening aan scholen te verbeteren, hierbij gaat het om statistische informatie en niet informatie die in het ticket zelf is opgenomen.

Mailmogelijkheden
Kennisnet maakt gebruik van een open source mail transfer agent (Postfix) die op de server van de applicatie draait. Er wordt geen externe mailprovider gebruikt. De mails die verstuurd worden zijn gerelateerd aan het proces van het uitnodigen van beheerders van diensten in Mijn Entree Federatie. Scholen kunnen niet mailen via dit systeem en ontvangen ook geen e-mails.

Applicatielandschap
Entree Federatie geeft gebruikers in het po, vo en mbo toegang tot een groot aantal educatieve diensten met één login (ook wel bekend als Single Sign On of SSO). De federatie wordt gevormd door aanbieders van een educatieve dienst of content (Service Providers), beheerders van identiteiten (Identity Providers) en de applicatie van Kennisnet (Entree Federatie). De federatie is een hub tussen Identity Providers en Service Providers. Leerlingen en docenten met een account bij een aangesloten Identity Provider loggen in bij de diensten van de aangesloten Service Providers.

Een Identity Provider is de applicatie die voor de school de communicatie met Entree Federatie verzorgt. Voorbeelden van Identity Providers zijn: Elektronische Leeromgevingen (een centrale digitale omgeving die meestal door meerdere scholen wordt gebruikt), Active Directory Federation Service (ADFS), Google Apps for Education en Azure AD.

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



Koppelingen

De totstandkoming van de koppeling gaat via een SAML-verzoek (Security Assertion Markup Language):

SAML is een XML-gebaseerd protocol dat wordt gebruikt voor het uitwisselen van authenticatie- en autorisatiegegevens tussen de identiteitsprovider (IdP) en een serviceprovider (SP). Het biedt een gestandaardiseerde manier om claims over de identiteit en attributen van een gebruiker over te dragen na een succesvolle authenticatie. SAML is een beproefd protocol in Single Sign- On (SSO) scenario's, waarbij een gebruiker slechts één keer hoeft in te loggen om toegang te krijgen tot meerdere diensten.

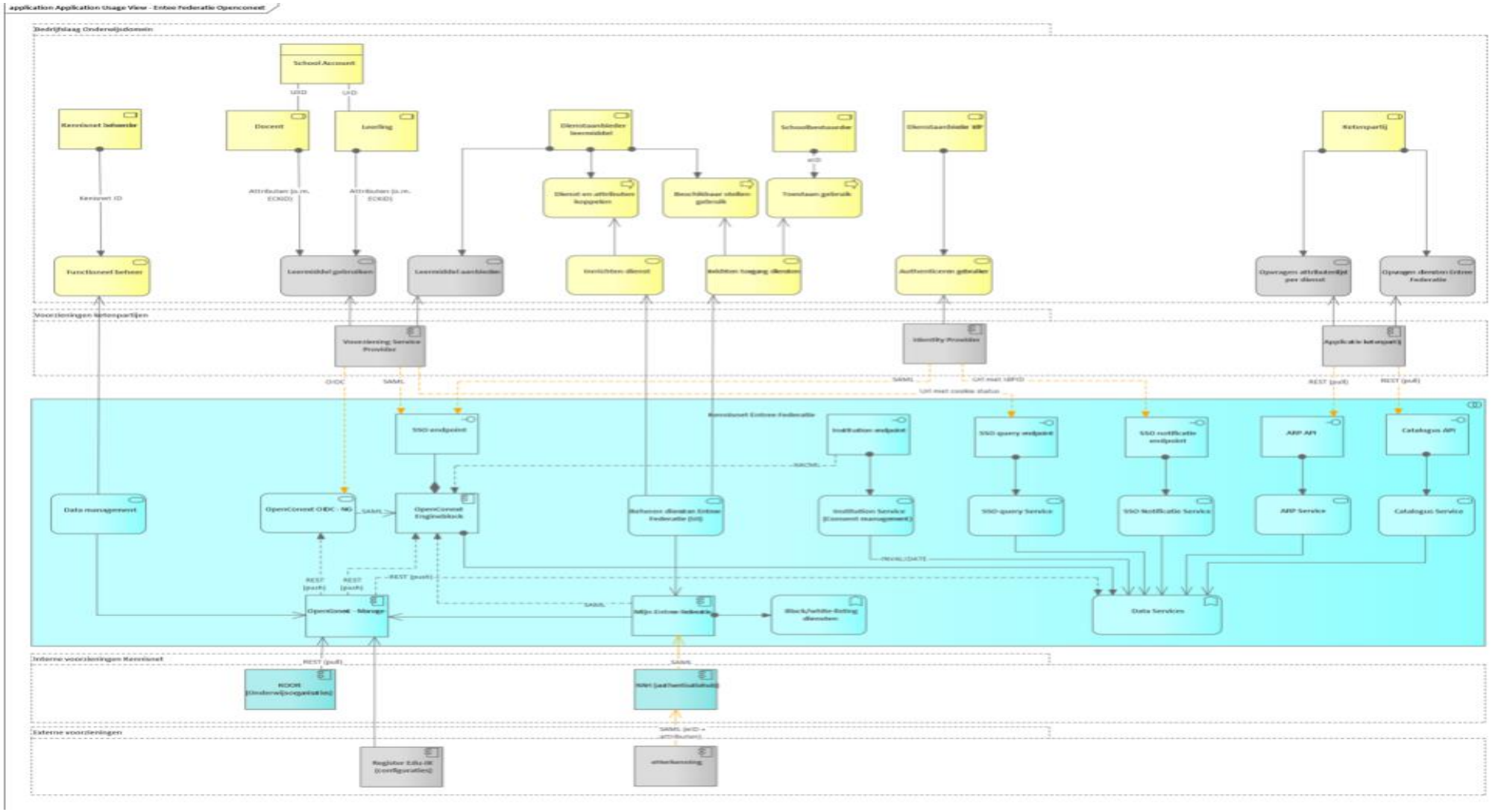
OIDC (OpenID Connect)

OIDC is een laag bovenop het OAuth 2.0-protocol en biedt een standaard voor het verifiëren van de identiteit van eindgebruikers.

Het maakt gebruik van JSON Web Tokens (JWT) voor de overdracht van claims tussen partijen. OIDC is ontworpen om eenvoudig te integreren met moderne web- en mobiele toepassingen en ondersteunt authenticatie met behulp van OAuth 2.0-protocollen.

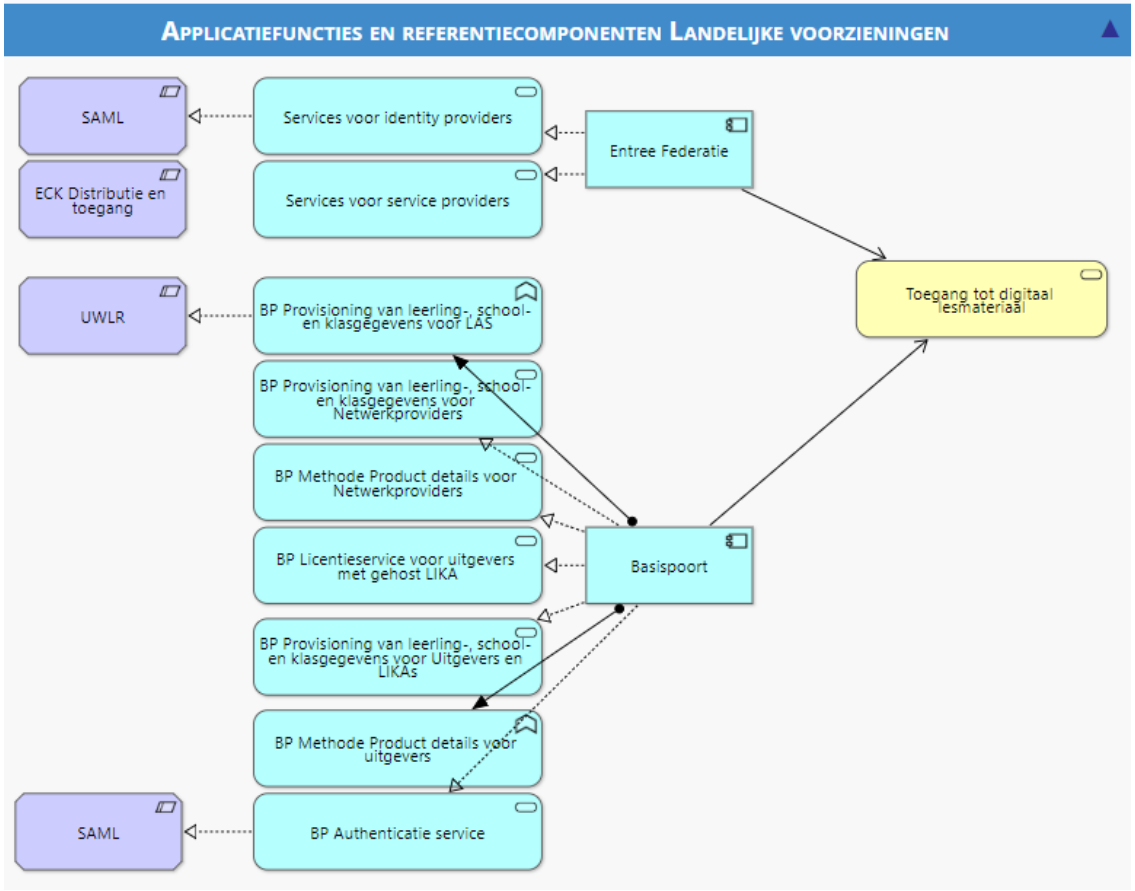
Gegevensstromen/stroomschema

Visualisatie gegevensverwerkingsproces.



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

Onderstaande visualisatie laat zien hoe Entree Federatie (SSO t.b.v. po, vo en MBO) zich verhoudt tot Basispoort (SSO t.b.v. po) ten aanzien van het tot stand komen van toegang tot digitaal lesmateriaal.



4. Verwerkingsdoeleinden

Het doel van de verwerking is het geven van toegang tot het aanbod van digitaal (leer)materiaal en beantwoord aan de doelbindingsvereisten uit het Privacyconvenant. De verwerkingsdoeleinden sluiten aan bij de in het Privacyconvenant[19] opgenomen verwerkingsdoeleinden:

De verwerkingsdoeleinden zijn schematisch weergegeven en gekoppeld aan de onderstaande verwerkingen:

Gegevensverwerking (par.3 Gegevensverwerkingen)	Doeleinde verwerking (par.4. Verwerkingsdoeleinden)	Toelichting
Faciliteren toegang tot aanbod leermateriaal.	**Authenticatieproces** Het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;	
Faciliteren toegang tot aanbod leermateriaal.	Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;	
Logging	De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens;	De authenticatie logging (leerlingen en medewerkers) wordt gepseudonimiseerd en blijft 13 maanden bewaard, deze logging wordt gebruikt voor rapportage doeleinden.
Faciliteren toegang tot aanbod leermateriaal.	De continuïteit, verbetering, goede werking van het Digitale Onderwijsmiddel in opdracht van	Hieronder valt ook de afhandeling van en ondersteuning bij

Zie: https://www.privacyconvenant.nl/downloads. Bijlage 1, onderdeel E. Doeleinden voor het verwerken van Persoonsgegevens. Voor Onderwijsinstellingen is in de toelichting een overzicht opgenomen van de relatie tussen de in onderdeel E benoemde verwerkingsdoeleinden en de (hoofd)bedrijfsfuncties in de FORA. Onderwijsinstellingen kunnen aan de hand van dit overzicht in de toelichting de specifieke verwerkingsdoeleinden selecteren die van toepassing zijn, aangevuld met de (hoofd)bedrijfsfuncties in de FORA.

Gegevensverwerking (par.3 Gegevensverwerkingen)	Doeleinde verwerking (par.4. Verwerkingsdoeleinden)	Toelichting
	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;	(technische) vragen en storingen ten behoeve van de werking van Entree Federatie;
Faciliteren toegang tot aanbod leermateriaal.	Het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.	

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, sub-verwerker, leverancier, derde en of ze verstrekker of ontvanger zijn. Benoem tevens welke personen/functies binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Naam partij	AVG-rol	Functie/taak	Betrokken persoonsgegevens	Verstrekker of ontvanger	De volgende personen/rollen hebben toegang deze pgg
Schoolbestuur	Verwerkingsverantwoordelijke	Beschikbaar stellen leermiddelen	(aanvullende) Attributenset	Verstrekker	Door school aangewezen ICT-coördinator
Entree Federatie (Kennisnet)	Verwerker	Voorzien in technische koppeling tussen school en serviceprovider	(aanvullende) Attributenset	Ontvanger en verstrekker	Beheerders Kennisnet
Vancis C&MS	subverwerker	Infrastructuurbeheerder	Kan bij storage en backups	Ontvanger	Geautoriseerde medewerkers t.b.v. beheer, onderhoud en oplossen technische storingen
Leerlingen en medewerkers	Betrokkene	Eindgebruiker	(aanvullende) Attributenset	Verstrekker	n.v.t.
Koppelpartners	Verwerker	Aanbieden digitale (leer)middelen	(aanvullende) attributenset	Ontvanger	Afhankelijk van instellingen de leerkracht en de koppelpartner

6. Belangen bij de gegevensverwerking

De belangen van de betrokken partijen zijn in essentie eenduidig: het op een veilige manier realiseren van de koppeling tussen de eindgebruiker (leerling/leerkracht) en de koppelpartner (digitaal (leer)middel). De belangen van de bij dit proces betrokken partijen zijn allemaal ondersteunend aan dit proces en spelen hier zelfs een onmisbare rol in.

Binnen de context SSO-dienst zijn verschillende partijen betrokken met specifieke AVG-rollen en functies.

Het schoolbestuur, in de rol van verwerkingsverantwoordelijke, heeft als taak het beschikbaar en toegankelijk stellen van leermiddelen ten behoeve van een goed werkend en betrouwbaar digitaal (leer)middel waarmee zij optimaal kan lesgeven en de leerling zich maximaal kan ontwikkelen.

Het belang van Entree Federatie als verwerker ziet op het aanbieden van de SSO-dienst ten behoeve van het koppelen tussen het schoolbestuur en de aanbieders van digitale (leer)middelen.

Het belang van de door Entree Federatie ingeschakelde subverwerker ziet op het bieden van ondersteuning t.b.v. opslag en backups.

Leerlingen en medewerkers zijn de uiteindelijke eindgebruikers die na de tot stand gekomen koppeling het (digitale) leermiddel in gebruik nemen, hierin ligt hun belang besloten.

Koppelpartners, in de rol van verwerker, bieden de digitale (leer)middelen aan.

7. Verwerkingslocaties

Partijnaam	Statutaire vestigings-plaats (sub-) verwerker	Beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt verwerkt door deze subverwerker	Plaats/land van opslag en verwerking persoonsgegevens en doorgifte mechanisme indien buiten de EER
Vancis C&MS	Nederland	Infrastructuurbeheerder t.b.v. de opslag en backup	N.v.t.

8. Data Transfer Impact Assessment (DTIA)

Omdat Entree Federatie gebruik maakt van één in Nederland gevestigde subverwerker en er geen sprake is van dataverwerking buiten de EER, is er geen noodzaak tot het uitvoeren van een DTIA.

9. Technieken en methoden van gegevensverwerking

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

Test op cookies en netwerkanalyse

Tijdens het verkrijgen van technische inzichten in de mogelijk gebruikte cookies en derde-partijen (subverwerkers) van Entree Federatie is gebruik gemaakt van een netwerkanalyse en een inlogsessie op de omgeving van Entree Federatie. Hierbij zijn geen opvallende technologieën (zoals Google Analytics, CDN of Google Fonts) waargenomen die mogelijk persoonsgegevens verwerken. Evenmin zijn er privacyschendende cookies aangetroffen.

Onderzoek Informatiebeveiliging

In september 2023 t/m januari 2024 heeft een globaal onderzoek plaatsgevonden naar de status van informatiebeveiliging van de applicatie Entree Federatie. Dit onderzoek is gebaseerd op informatie welke door Kennisnet is verstrekt en een compliance check op het ROSA classificatieschema. Er is geen technisch onderzoek uitgevoerd naar het implementatieniveau van beveiliging.

Uit dit onderzoek is de volgende informatie verkregen:

- Kennisnet is ISO27001 gecertificeerd sinds 2016. De Entree applicatie valt in scope van het certificaat.
- In de Verklaring van toepasselijkheid zijn alle vereisten relevant verklaard.
- Periodiek wordt de omgeving van Entree Federatie aan een pentest onderworpen. De meest recente is van april 2022. Het rapport is ingezien en de bevindingen zijn correct door Entree Federatie opgepakt en verholpen.
- In het ROSA model[20] wordt als classificatie Hoog, Midden, Midden (H-M-M) gehanteerd. In de verwerkersovereenkomst staat juist H-H-H. Bij navraag is aangegeven dat de classificatie op H-M-M correct is dus conform ROSA model. Het gehanteerde classificatieniveau is inconsistent met als risico dat bij de implementatie van beveiligingsmaatregelen een onjuist classificatieniveau wordt gehanteerd en dus onjuiste beveiligingsmaatregelen worden gehanteerd.
- Omdat voor Data in transfer ook gebruikers identificatie wordt doorgegeven door Entree Federatie van de ene toepassing naar een andere toepassingen dient de kwaliteit van deze informatie altijd correct te zijn. Er mogen geen fouten zitten in

[20] In deze standaard worden afspraken gemaakt over het (basis)niveau van informatiebeveiliging en privacy voor toepassingen die worden gebruikt binnen in het onderwijs (PO, VO, MBO en HO). Het bepaalt het niveau voor Betrouwbaarheid, Integriteit en Vertrouwelijkheid van een toepassing en schrijft op basis daarvan de benodigde maatregelen voor (zie Toetsingskader).

gebruikers identificatie. Volgens het ROSA model is dan voor Integriteit het niveau Hoog van toepassing en niet Midden.
- In de beantwoording van de beveiligingsmaatregelen uit het ROSA model gebaseerd op classificatieniveau H-M-M zijn geen afwijkingen gevonden.

Aanbevelingen

- Het advies is om Entree Federatie op eenduidige wijze te classificeren voor zowel het ROSA model als de classificatie benoemd in de verwerkersovereenkomst welke nu verschillen.
- De classificatie van Integriteit staat (volgens het Rosa model) nu op Midden terwijl deze volgens het ROSA model op Hoog dient te staan. Ook dienen de bij dit niveau behorende beveiligingsmaatregelen te worden geïmplementeerd.

IAMA: mensenrechten in beeld bij algoritmes

Omdat uit voornoemde DPIA-vragenlijst, interviews met Kennisnet en het verdere binnen deze DPIA verrichte onderzoek niet is gebleken dat er gebruik wordt gemaakt van AI technologie is de beoordeling van een eventueel hoog risico niet aan de orde geweest.

Dit betekent dat er geen Impact Assessment Mensenrechten en Algoritmes (IAMA) is uitgevoerd ten behoeve van het inzichtelijk maken van het voldoen aan de wettelijke verplichtingen en of er sprake is van een verantwoorde inzet van AI en algoritmen.

10. Juridisch en beleidsmatig kader

Onderstaande tabel geeft vorm aan de juridische en beleidsmatige fundamenten ten aanzien van het gebruik van een SSO-dienst binnen het onderwijs. De hieruit voortkomende verwerking van persoonsgegevens zijn inherent aan het doel van de verwerking, namelijk het koppelen van diensten aan een service provider.
Het Normenkader wordt op termijn een verplichting voor schoolbesturen om aan te voldoen. De relevante waarborgen die de SSO-dienst raken zijn daarom ook opgenomen in dit overzicht.

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
Faciliteren toegang tot aanbod leermateriaal	Wet op het primair onderwijs	Artikel 8 en 182, lid 12
Faciliteren toegang tot aanbod leermateriaal	Wet op het voortgezet onderwijs	Artikel 8.17, lid 10
Faciliteren toegang tot aanbod leermateriaal	Normenkader IBP	Hoofdstuk 10, Identity & Access Management
Logging	Normenkader IBP	Hoofdstuk 11.4 Security Management

11. Bewaartermijnen

Hoewel bij de kernactiviteit van Entree Federatie, namelijk de feitelijke koppeling tussen gebruiker en leermiddel, geen gegevens wordt opgeslagen en hierbij dus bewaartermijnen geen rol spelen wordt er wel gelogd en is er soms sprake van technische storingen die een oplossing behoeven. Bij het uitvoeren van deze “nevenverwerkingen” worden de volgende bewaartermijnen toegepast.

Nb: de logging op de activiteiten van de eindgebruikers (leerlingen/leerkrachten) wordt vastgelegd door de Identity Provider van de scholen. Dit kan bijvoorbeeld een LAS (leerling administratiesysteem) zijn of een database van Google of Microsoft. Entree Federatie heeft enkel de logging van succesvolle authenticaties van de eindgebruikers.

Gegevensverwerking	Verwerkingsdoeleinde	Categorie persoonsgegevens	Bewaartermijn en grondslag
Logging gebruikersgroep: 1. Eindgebruikers 2. Beheerders op school 3. Beheerders van dienstaanbieders 4. Beheerders van Kennisnet	Controle activiteit t.b.v. monitoring, foutanalyse beveiliging, analyse en troubleshooting	Gebruikersinformatie en sessie- en authenticatiegegevens.	13 maanden conform ROSA Uitgebreide logging t.b.v. foutanalyse 10 dagen
Technische ondersteuning	Oplossen inlogproblemen	Gebruikersinformatie waaronder de attributenset	Maximaal 2 jaar

Bewaartermijn support-tickets

Uit onderzoek is gebleken dat het verwijderen van deze support-tickets (waarvoor Kennisnet verwerker is) niet is gestandaardiseerd en/of dat deze tickets niet tijdig worden verwijderd. De afspraak is met Kennisnet gemaakt dat Kennisnet dit proces - binnen één jaar - aanpast waarbij support-tickets in het vervolg gelabeld worden (als verwerkersactiviteit van Kennisnet) en dat deze tickets na sluiting na twee jaar verwijderd zullen worden.

Kennisnet biedt ook ondersteuning aan gebruikers van Entree Accounts, waarbij door gebruikers zelf bij Kennisnet een Entree Account kan worden aangemaakt. Entree Account is buiten scope in deze DPIA. Voor deze tickets, alsmede support-tickets voor andere diensten van Kennisnet waarvoor Kennisnet verwerkingsverantwoordelijke is, worden de bewaartermijnen door Kennisnet bepaald. Hierbij geldt overigens ook dat Kennisnet gevoelige gegevens bij sluiting van het ticket verwijdert.

4. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen

12. Rechtsgrond

De grondslag van de gegevensverwerkingen zijn gebaseerd op de taak van algemeen belang.

Artikel 6 AVG, eerste lid, sub:

a) Toestemming van de betrokkene
b) Uitvoering van een overeenkomst
c) Wettelijke verplichting[21]
d) Vitaal belang van de betrokkene
e) Taak van algemeen belang[22] (of openbaar gezag)
f) Gerechtvaardigd belang

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.

Voor wat betreft de verwerking van persoonsgegevens binnen Entree Federatie, wordt in het onderstaande uiteengezet wat de regels zijn en de juridische basis is omtrent het aanbieden van leermiddelen in het primair onderwijs (hierna: po) en het voortgezet onderwijs (hierna: vo) en in het verlengde daarvan de verwerking van persoonsgegevens.

Inzet van digitale onderwijsmiddelen

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). Dit is een (wettelijke) kernactiviteit van scholen in het po en vo.

Artikel 182 lid 12 van de Wet op het primair onderwijs (hierna: WPO) geeft aan dat:

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

[21] 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.
[22] 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.

digitale dienst aanbiedt bestaande uit leerstof of toetsen en de daarmee samenhangende digitale diensten.

Artikel 8.17, lid 10 van de Wet Voortgezet onderwijs 2020 (hierna: WVO) geeft bijna identiek aan dat:

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

Dit geeft (indirect) aan dat een onderwijsinstelling in het kader van haar taken zoals bedoeld in de WPO en WVO, namelijk het geven van onderwijs, digitale leermiddelen mag inzetten en daarbij gebruik kan maken van ondersteunende digitale diensten (zoals Entree Federatie).

Het behoort tot de verantwoordelijkheid van de school om er voor zorg te dragen dat de leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen. Ondersteunend aan dit proces is het in gebruik nemen van een SSO-dienst.

Technische maatregelen

De AVG[23] schrijft voor dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen moeten nemen om de gegevensverwerking op een veilige manier te laten plaatsvinden.

Entree Federatie levert een veilige SSO-oplossing waardoor leerlingen (en medewerkers) op een veilige en uniforme manier toegang krijgen tot de aanbieders van digitale (leer)middelen. Op deze manier wordt ten aanzien van het inloggen vormgegeven aan de vereisten van artikel 32 AVG.

Verwerking/doeleinde (zie hiervoor 4. Verwerkingsdoeleinden)	Grondslag AVG	Toelichting
Het voorzien van een SSO-koppeling inclusief logging en technisch onderhoud t.b.v. de inzet van onderwijs bevorderende digitale (leer)middelen.	Artikel 6, eerste lid, onder e Taak van algemeen belang jo Artikel 8 en 182, lid 2 Wet op het primair onderwijs en artikel 8.17, lid 10 Wet op het voortgezet onderwijs 2020	De onderwijssector mag zich voor de uitvoering van uiteenlopende taken beroepen op het algemeen belang als verwerkingsgrondslag t.b.v. de noodzakelijke verwerkingen.

[23] Artikel 32 AVG, beveiliging van de verwerking

13. Bijzondere persoonsgegevens

Binnen de SSO-dienst van Kennisnet worden geen bijzondere, gevoelige of strafrechtelijke persoonsgegevens verwerkt.

14. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld dient beoordeeld te worden of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Gelet op het DPIA-onderzoek zijn er geen aanknopingspunten om te veronderstellen dat er sprake is van verdere verwerking. Wat betreft de doelbinding geven de bevindingen evenmin enige reden om aan te nemen dat hiermee in strijd wordt gehandeld. De verzamelde en verwerkte persoonsgegevens worden niet voor een ander doel gebruikt dan het beoogde.
De SSO-dienst verzamelt, verwerkt en deelt persoonsgegevens alleen met als doel gebruikers te verifiëren en toegang te verlenen tot geautoriseerde diensten, zoals vastgelegd in het initiële doel van de dienst.

15. Kinderrechten-afweging (Best Interests Assessment Children)

Voor de SSO-dienst van Kennisnet is er na een eerste beoordeling geen noodzaak voor een nadere analyse met betrekking tot de kinderrechten. Dit komt voort uit het feit dat de SSO-dienst primair gericht is op het faciliteren van gebruikersauthenticatie voor onderwijsgerelateerde digitale (leer)middelen. Gezien de aard van de dienst en het beperkte gebruik van persoonsgegevens voor het specifieke doel van identiteitsverificatie, zijn er geen directe negatieve gevolgen te verwachten voor de kinderrechten zoals beschreven in artikel 3 van het Verdrag inzake de rechten van het kind. De gegevensverwerking heeft geen impact op de ondersteuning en behoeften van kinderen met betrekking tot veiligheid, gezondheid, welzijn, familierelaties, ontwikkeling, identiteit, enzovoort.

Aangezien de SSO-dienst primair wordt gebruikt door schoolbesturen en zich richt op identiteitsverificatie, is het doel van de verwerking in lijn met de belangen van de betrokkenen (kinderen/leerlingen) zonder gebleken risico op schadelijke gevolgen voor hun rechten en vrijheden. De kinderrechtenafweging uit deze DPIA kan daarom worden beperkt tot het bevestigen dat het gebruik van de SSO-dienst leeftijdsadequaat is, en in overeenstemming is met de specifieke behoeften van de betrokken kinderen. Aanvullende maatregelen lijken daarom in dit geval niet noodzakelijk.

16 a. Noodzakelijkheid

Het doel van het opzetten van de SSO-dienst van Entree Federatie is voor een belangrijk deel gelegen in het verbeteren van de digitale veiligheid en in het bijzonder de beperking van de voor de koppeling noodzakelijke persoonsgegevens. Dit heeft vorm gekregen aan de hand van de ontwikkeling van de Standaard en Aanvullende attributenset die aan de

dienstaanbieder beschikbaar wordt gesteld. Authenticatie is niet mogelijk zonder verificatie van unieke kenmerken die aantonen dat de leerling bevoegd is om gebruik te maken van een leermiddel. Het beschikbaar stellen van de Standaard attributenset voldoet, rekening houdend met redelijke kosten, moeite en de stand van de techniek die van de aanbieder en het schoolbestuur verwacht kunnen worden aan het noodzakelijkheidsvereiste voor de verwerking van persoonsgegevens.

137 van de 228 dienstaanbieders vragen Aanvullende attributen uit. De noodzaak hiervan dient zorgvuldig onderbouwt te zijn door de dienstaanbieder. Uit onderzoek is gebleken dat de motivering voor de uitvraag van de Aanvullende attributen door de dienstaanbieders op dit gebied vaak beperkt is.
Het is een belangrijke rol van het schoolbestuur om een controle uit te voeren op de door de dienstaanbieder uitgevraagde Aanvullende attributenset. Voor de verstrekking hiervan moet ondubbelzinnige toestemming worden gegeven door de school. Wanneer er twijfels zijn over deze extra uitvraag is het aan het schoolbestuur om hierover in gesprek te gaan met de dienstaanbieder. Hierbij zal het schoolbestuur altijd (al dan niet samen met de dienstaanbieder) moeten motiveren en vastleggen per onderdeel van de Aanvullende attributenset wat de noodzaak is dat dit specifieke gegeven wordt uitgewisseld met de leverancier. Waarom wordt er bijvoorbeeld een geboortedatum van een leerling uitgevraagd?

16. b. Proportionaliteit en subsidiariteit

Bij het gebruik van de SSO-dienst worden, voor wat betreft de Standaard attributenset, uitsluitend noodzakelijke gegevens veilig via SAML gedeeld met de koppelpartners. Met betrekking tot de proportionaliteit kan worden gesteld dat de inbreuk op de persoonlijke levenssfeer en de bescherming van persoonsgegevens in evenredige verhouding staat tot de verwerkingsdoeleinden van gebruikersauthenticatie en toegangsverlening tot digitale (leer)middelen. Het is hierbij belangrijk in acht te nemen dat juist deze dienst van de Entree Federatie is opgezet om zo weinig mogelijk persoonsgegevens uit te wisselen met de leverancier van het leermiddel of dienst. Deze privacyvriendelijke toegang biedt het voordeel dat gebruikers, via een gebruiksvriendelijke ervaring met een enkele set inloggegevens, toegang kunnen verkrijgen tot diverse systemen en applicaties zonder herhaaldelijk in te loggen

Alternatieve toegangsmogelijkheden, zoals multifactor-authenticatie of token-based authenticatie, impliceren eveneens de verwerking van persoonsgegevens. Het is echter van belang op te merken dat bij deze alternatieven geen verminderde inbreuk op de privacy van de betrokkene optreedt in vergelijking met de huidige koppeling.

17. Rechten van de betrokkenen

Bij het koppelen van de eindgebruikers aan een koppeldienst worden de hiervoor te verwerken persoonsgegevens, in de vorm van de Standaard (en) Aanvullende attributenset, realtime doorgegeven. Dit betekent dat deze gegevens niet worden opgeslagen binnen Entree Federatie.

Dit beperkt in aanzienlijke mate de hierbinnen uit te oefenen rechten van betrokkenen. Na de totstandkoming van de koppeling, die in een fractie van een seconde plaatsvindt, zijn er enkel nog datasporen aan de hand van de logging die op deze koppeling heeft plaatsgevonden. De logging vindt alleen plaats voor operationele doeleinden.

Daarnaast kan er in voorkomende gevallen voor (technische) ondersteuningsdoeleinden vanuit Entree Federatie inzicht zijn in de attributen. Dit is aan de orde wanneer de koppeling van de school niet tot stand komt en er onder '*de motorkap*' gekeken moet worden. Dit verzoek tot ondersteuning wordt meestal uitgevoerd vanuit de de staffrol (welke o.a. door de ICT-beheerder van een school wordt vervuld). Entree Federatie ontvangt in dat geval een overzicht van de bij de staffrol (dus van een persoon) behorende attributen welke representatief zijn voor die ook van de school over de lijn gaan. Dit overzicht wordt gedurende 10 jaar bewaard en daarna vernietigd. Deze lange bewaartermijn is een vereiste vanuit het ministerie in verband met de subsidieverlening.

Dit betekent dat er ten aanzien van de opslag door Entree Federatie weinig tot geen persoonsgegevens beschikbaar zijn van de betrokkenen, waardoor de uitoefening van specifieke rechten beperkt aan de orde kan zijn.

Eindgebruikers gebruiken bij het inloggen op aangesloten dienstaanbieders hun "schoolaccount". De school kan in "mijn Entree Federatie" aangeven bij welke partijen hun eindgebruikers SSO kunnen inloggen. Ook zijn er in Mijn Entree Federatie gebruiksstatistieken beschikbaar. Omdat Entree Federatie alleen "realtime" gegevens doorgeeft en er (anders dan gepseudonimiseerde logging gegevens) geen gegevens worden bewaard, kunnen ze ook niet gevraagd worden om deze te verwijderen.

Kennisnet biedt de mogelijkheid aan om in voorkomende gevallen zowel het inzagerecht als het verwijderrecht te faciliteren op verzoek van een betrokkene respectievelijk een schoolbestuur.

Ten aanzien van het recht op informatie dient het schoolbestuur te kunnen verwijzen naar een openbaar gepubliceerde privacyverklaring of anders de website van Kennisnet waarop de benodigde informatie te vinden is die betrekking heeft op de gegevensverwerking ten behoeve van de koppeling.

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking*
Het recht op informatie	Bijvoorbeeld: • Openbaar gepubliceerde privacyverklaring; • Intern gepubliceerde privacyverklaring; • Versturen van een fysieke brief naar huisadres betrokkenen; • Versturen van een digitale brief naar e-mailadres betrokkenen; • Betrokkenen worden gebeld	n.v.t.

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking*
Het recht van inzage	Kan gefaciliteerd worden door Entree Federatie nadat vanuit het schoolbestuur de hierbij horende procedure wordt gevolgd.	n.v.t.
Het recht op rectificatie	Rectificatie van gegevens dient plaats te vinden binnen de IDP van de school zelf.	n.v.t.
Het recht op gegevenswissing	Kan gefaciliteerd worden door Entree Federatie nadat vanuit het schoolbestuur de hierbij horende procedure wordt gevolgd.	n.v.t.
Het recht op beperking van de verwerking	N.v.t.	n.v.t.
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	Kan gefaciliteerd worden door Entree Federatie	n.v.t.
Het recht op overdraagbaarheid van gegevens	N.v.t.	n.v.t.
Het recht van bezwaar	N.v.t.	n.v.t.
Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit	N.v.t.	n.v.t.

* *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.*

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) en daarbij gebruik maken van het daarbij horende model verwerkersovereenkomst vindt een toetsing plaats welke wordt afgezet tegen de vereisten van het convenant. Dit wordt de theoretische toets genoemd. Aanvullend hierop zal ook, aan de hand van de inzichten die deze DPIA heeft gebracht, een praktische toets plaatsvinden. Hierbij zal een vergelijk worden gemaakt tussen de in de theorie genoemde afspraken en de verwerkingen die in de praktijk plaatsvinden. De hiervoor gebruikte toetsingskaders zijn in de bijlage (verwerkersovereenkomst Toetsformulier met link) terug te vinden.

Voor leveranciers die geen deelnemer of medestander zijn van het convenant zal de verwerkersovereenkomst worden getoetst aan de vereisten van de AVG.

Na de bespreking van het verwerkersovereenkomst Toetsformulier en eventuele afspraken wordt uiteindelijk een verwerkersovereenkomst Toetsrapport met de bevindingen opgeleverd die via de Dienst Verwerkersovereenkomsten (van Kennisnet) of afgeschermd op de website van SIVON gedeeld wordt met alle schoolbesturen.

TOETSRAPPORT (o.b.v. Model VWO)	Toelichting	Risico [L/M/H]
Toets - Verwerkersovereenkomst • Betreft 'Overwegen het volgende: verwijzing onderliggende overeenkomst (naam en datum) en benoeming product/dienst'	Alleen het model is getoetst en deze kan geen datum van de ondertekende overeenkomst bevatten. Over naam onderliggende overeenkomst en benoeming product/dienst neemt Kennisnet de wijzigingen voldoende duidelijk op in Bijlage 3.	Geen
Toets - Bijlage 1: Privacybijsluiter • Betreft 'A. Contactgegevens Verwerker en Onderwijsinstelling - Functie contactpersoon'	In de Vereisten voor de bijlagen bij de model verwerkersovereenkomst is alleen opgenomen dat de functie van de contactpersoon ingevuld dient te worden. In het Model Word-document zelf wordt in de betreffende tabel ook om de naam van de contactpersoon gevraagd. Kennisnet laat dit achterwege en dat is prima, want het kan aan verandering onderhevig zijn (en dan is steeds een update noodzakelijk).	Geen
• Betreft 'C. Algemene informatie - Beknopte uitleg en werking product en/of dienst'	Hoewel netjes is voldaan aan dit vereiste, is gevraagd of het mogelijk is om de werking te visualiseren (bijv. via een dataflow). Leverancier heeft toegezegd daarmee aan de slag te gaan.	Geen
• Betreft 'F. Categorieën persoonsgegevens inclusief bewaartermijnen	In de tabel van de 'onderwijsdeelnemer' staat het vinkje bij Gebruikersgegevens, waaronder diagnostische gegevens en logging niet aangevinkt terwijl deze gegevens tijdens het proces wel worden verwerkt.	Midden
• Betreft 'G. Locatie van opslag en verwerking van persoonsgegevens	In de tabellen staat dat er tijdens de authenticatie geen persoonsgegevens	

TOETSRAPPORT (o.b.v. Model VWO)	Toelichting	Risico [L/M/H]
	worden opgeslagen. Dit klopt echter niet voor de gepseudonimiseerde logging welke wel plaatsvindt.	
Toets - Bijlage 2: Beveiligingsbijlage	Discrepantie BIV-classificatie: De Vertrouwelijkheid staat op Hoog terwijl de maatregelen Midden zijn. Dit vereist daarom aanpassing van de classificatie van Hoog naar Midden v.w.b. de Vertrouwelijkheid	Midden
Toets - Bijlage 3: Wijzigingenbijlage	Geen opmerkingen	Geen

Bij dit DPIA-rapport wordt ook een Toetsrapport verwerkersovereenkomst opgeleverd. Deze is op te vragen bij de leverancier en (op termijn) te vinden via de afgeschermde omgeving van de Dienst Verwerkersovereenkomst van Kennisnet of een afgeschermde omgeving van het Netwerk IBP.

Kennisnet is voornemens de aangepaste en door SIVON getoetste verwerkersovereenkomst in het vierde kwartaal van 2024 via de Dienst Verwerkersovereenkomsten aan te bieden aan scholen.

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

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

Beoordelingskader risico's

Alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden beschreven en afgewogen. Het gaat hierbij om de negatieve gevolgen die de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, de oorsprong van deze gevolgen, de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden: kans (waarschijnlijkheid) X impact (ernst) = risico.
De methodiek die wordt gevolgd, is beschreven door de Britse toezichthouder[24] om risico's te classificeren. Hierbij wordt een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade).

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

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

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

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.

[24] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how10

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

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

1. Risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

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

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

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 Entree Federatie (hierna ook EF) wordt ingezet of dat het risico het systeem zelf betreft (de applicatie).

Toelichting MAPGOOD-methode

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

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

Risicotabel (EF = Entree Federatie):

Risiconr.	Mapgood	Risico-omschrijving School/EF	Oorzaak	Gevolgen betrokkene
1	O	School Verwerking vindt mogelijk plaats in strijd met het uitgangspunt van dataminimalisatie. De aanbieders (leveranciers van bijvoorbeeld leermiddelen) die aanvullende attributen voorwaardelijk stellen voor hun dienstverlening motiveren onvoldoende waarom deze gegevens noodzakelijk zijn. Hierdoor is de inschatting als school moeilijk te maken of de	Aanbieder betracht zichzelf onvoldoende moeite om verantwoording af te leggen voor de noodzakelijk geachte aanvullende attributen.	Als de aanbieder onvoldoende motiveert waarom bepaalde attributen nodig zijn, kan dit leiden tot zorgen over privacy en het onnodig delen van persoonlijke informatie. Betrokkenen kunnen zich in hun belangen geschaad voelen kans op datalekken neemt toe.

Risiconr.	Mapgood	Risico-omschrijving School/EF	Oorzaak	Gevolgen betrokkene
		uitgevraagde attributen noodzakelijk en proportioneel zijn.		
2	P	EF De informatiebeveiliging op het gebied van de Integriteit voldoet niet aan de gestelde norm uit het ROSA-schema. Er wordt nog niet volledig voldaan aan de maatregelen die op basis van het ROSA-schema2 moeten zijn geïmplementeerd uitgaande van een BIV-classificatie waarbij de Integriteit op Hoog is gezet. Er wordt wel voldaan aan de maatregelen die passen bij de classificatie Midden. Hierdoor is ook onduidelijkheid bestaan ten aanzien van de classificatie welke bij Integriteit in de verwerkersovereenkomst op Hoog staat en in het ROSA-schema op Midden.	BIV-classificatie in het ROSA-schema (H-M-M) komt niet overeen met de passende normering die SIVON hieraan verbindt. Verder staat wel in de verwerkersovereenkomst (H-H-H) opgenomen.	Een verhoogd risico op ongeoorloofde toegang, wijziging of verlies van persoonlijke gegevens.
3a	D	Verwerkersovereenkomst Onjuiste informatievoorziening. • Betreft Bijlage 2 ‘Beveiligingsbijlage, onderdeel B, Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het	Onjuist opgenomen BIV-classificering in bijlage 2 van de verwerkersovereenkomst.	Ten onrechte veronderstelling dat toegepaste maatregelen op het gebied van Informatiebeveiliging hoger zijn dan feitelijk het geval.

Risiconr.	Mapgood	Risico-omschrijving School/EF	Oorzaak	Gevolgen betrokkene
		netwerk, de server en de applicatie te waarborgen'. De BIV-classificatie is voor de Vertrouwelijkheid op Hoog gezet terwijl deze voldoet aan de maatregelen passend bij Midden. Midden is ook opgenomen in het ROSA-schema.		
3b	D	Verwerkersovereenkomst Onjuiste informatievoorziening • Betreft 'F. Categorieën persoonsgegevens inclusief bewaartermijnen	In de tabel van de 'onderwijsdeelnemer' staat het vinkje bij Gebruikersgegevens, waaronder diagnostische gegevens en logging niet aangevinkt terwijl deze gegevens tijdens het proces wel worden verwerkt.	Tekortschietende naleving transparantie en informatieverplichting, hierdoor is betrokkene niet adequaat geïnformeerd over de verwerking van zijn persoonsgegevens
3c	D	Verwerkersovereenkomst, geen of niet-naleving bewaartermijn support-tickets	Kennisnet bewaart bij het leveren van support voor EF de tickets te lang en/of verwijdert deze niet (op tijd) waardoor de grondslag ontbreekt.	Gegevens blijven te lang bewaard.
3d	D	Verwerkersovereenkomst Onjuiste informatievoorziening • Betreft 'G. Locatie van opslag en verwerking van persoonsgegevens	In de tabellen staat dat er tijdens de authenticatie geen persoonsgegevens worden opgeslagen "*ook niet in de logging*". Dit klopt echter niet voor de gepseudonimiseerde logging welke wel inzichtelijk is voor EF.	Gebrek aan transparantie en controle over de verwerking van de gegevens.

Risiconr.	Mapgood	Risico-omschrijving School/EF	Oorzaak	Gevolgen betrokkene
4	O	School Onrechtmatige verwerking door dienstaanbieder bij inloggen zonder licentie. Bij het koppelen via de Entree Federatie naar serviceproviders wordt de uitwisseling van de attributen gefaciliteerd. In gevallen waar een licentie is beëindigd of er geen gebruik meer wordt gemaakt moet ook de koppeling worden beëindigd binnen Mijn Entree Federatie of intrekking van het ARP-formulier. Wanneer een leerling/medewerker na beëindiging van de licentie inlogt op deze serviceprovider, worden standaard en aanvullende attributen naar de serviceprovider verzonden, ondanks dat deze niet langer gerechtigd is tot het ontvangen van deze gegevens. Dit resulteert in het onbedoeld beschikbaar stellen van persoonsgegevens aan een onbevoegde partij.	Gebrekkig management t.a.v. het gebruik van dienstaanbieders.	Door in te loggen op een dienst waarmee geen licentie loopt worden attributen gedeeld waarover de dienstaanbieder niet zo moeten beschikken.

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

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

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

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

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

19. Maatregelen

Maatregelentabel:

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (Kennisnet/ school)	Rest risico	(datum)maatregel geïmplementeerd?
1	Motivering dienstaanbieder Aanvullende attributen onvoldoende	4	Proces aanwezig voor beheer en controle op de motivering van de door de dienstaanbieders verzochte Aanvullende attributen. Proces Kennisnet: controle aanwezigheid motivering Kennisnet heeft de dienstaanbieders medio 2024 indringender verzocht om gedetailleerd te motiveren waarom Aanvullende attributen voor de koppeling noodzakelijk zijn, zodat scholen goed kunnen inschatten of deze verwerking voldoet aan de beginselen van proportionaliteit en subsidiariteit. In dit kader zal ook een nieuwe oproep aan de dienstaanbieders worden gedaan om alsnog te voorzien in deze motivering. NB deze aanvullende attributen moeten ook in de VWO met de dienstaanbieder staan opgenomen.	School Kennisnet Kennisnet School	2 2 2	Lokale DPIA Uitgevoerd Lokale DPIA

2	Naleving ROSA maatregelen	9	NB dit vereist ook aanpassing van de VWO van EF op het gebied van toelichting maatregelen Integriteit. Verder dient de BIV bij Vertrouwelijkheid van Hoog naar Midden te worden aangepast.	EF	2	Q4 2024
3a	Verwerkersovereenkomst, BIV-kwalificatie	4	Aanpassing VWO, in overeenstemming brengen van de feitelijke BIV-kwalificatie.	EF	1	Q4 2024
3b	Verwerkersovereenkomst, diagnostische gegevens	4	Aanpassing VWO. In de tabel van de 'onderwijsdeelnemer' staat het vinkje bij Gebruikersgegevens, waaronder diagnostische gegevens en logging niet aangevinkt terwijl deze gegevens tijdens het proces wel worden verwerkt.	EF	1	Q4 2024
3c	Verwerkersovereenkomst, bewaartermijn support-tickets	4	Aanpassing proces Kennisnet: Kennisnet heeft toegezegd om gesloten support-tickets voor EF waarvoor Kennisnet verwerker is, te labelen als verwerkersinformatie en na 2 jaar te verwijderen.	EF	1	1 augustus 2025
3d	Verwerkersovereenkomst, logging authenticatie	4	Aanpassing VWO. In de tabellen staat dat er tijdens de authenticatie geen persoonsgegevens worden opgeslagen. Dit klopt echter niet voor de gepseudonimiseerde logging.	EF	1	Q4 2024
4	Koppeling met dienstaanbieders tijdig uitschakelen	4	Proces aanwezig voor beheer en controle op koppelingen.	School	1	Lokale DPIA

7. Deel E: MODEL lokale DPIA

A. Uitvoering lokale DPIA

beschrijving kenmerken gegevensverwerking;

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

Bij de beoordeling in deze lokale DPIA zijn betrokken:

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

B. Overwegingen over centrale DPIA

Het team dat betrokken is bij de lokale DPIA heeft de in de centrale DPIA benoemde gegevensverwerking, rechtmatigheid, risicobeoordeling en voorgenomen maatregelen beoordeeld en overgenomen.

Hierbij gelden de volgende uitzonderingen en/of toevoegingen: […].

C. Organisatiespecifieke- en algemene applicatierisico's

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

Risicotabel 1. Organisatie-specifieke risico's:
Veilige gegevensverwerking omvat meer dan alleen de verwerkingsomgeving van de applicatie/ het systeem. Het vergt ook dat de basis op orde is voor o.a. het besturingssysteem waarop het draait, de kennis en kunde van de gebruiker en het hebben en toepassen van relevant beleid.

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	Het bestuur heeft een eigen privacycoördinator of privacy officer.		

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

11	Ouders en medewerkers kunnen altijd en met succes de rechten van betrokkenen inroepen.		
12	Het bestuur heeft op elke schoolwebsite een pagina, dan wel een link naar de juiste pagina, over de wijze waarop de ouders (of leerlingen > 16 jaar) hun rechten kunnen uitoefenen (Privacyreglement).		

Risicotabel 2. Algemene applicatiespecifieke risico's

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

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	De verwerkersovereenkomst met verwerker is getekend.		
2	De verwerking is opgenomen in het register van verwerkingen.		
3	Het bestuur zal de DPIA van Entree Federatie minimaal eens per drie jaar herbeoordelen.		
4	Het bestuur houdt rekening met dataminimalisatie voor verwerken van persoonsgegevens in de applicatie.		
5	Het bestuur voldoet aan het transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over de toepassing van Entree Federatie		
6	Er is een functioneel beheerder aangewezen voor Entree Federatie		

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

Risico	Te nemen maatregel	Uitgevoerd?	Opmerking/toelichting
Bij het koppelen via de Entree Federatie naar serviceproviders worden poorten geopend om de benodigde attributen beschikbaar te stellen. In gevallen waar een licentie is beëindigd of er geen gebruik meer wordt gemaakt van een serviceprovider, zoals een leerapplicatie, bestaat het risico dat de toegang tot de leverancier niet tijdig wordt stopgezet, wat kan leiden tot ongeautoriseerde toegang en mogelijke inbreuk op de gegevensbescherming.	Zorg voor eigenaarschap, inzicht en beheer op de toegang die wordt verschaft tot service providers via Entree Federatie. Implementeer onder meer maatregelen om ervoor te zorgen dat er geen onnodige toegang tot data via de koppelingen plaatsvindt voor de leverancier wanneer er geen actieve afname van een product of dienst plaatsvindt. Schakel deze koppelingen dus tijdig uit. Voeg bijvoorbeeld een processtap toe aan het inkoopbeheer waarbij het stopzetten van een licentie automatisch gekoppeld wordt aan de ICT-afdeling, zodat zij de benodigde acties kunnen ondernemen om de relevante		

	koppelingen uit te schakelen.		
Er wordt toestemming verleend voor het verstrekken van aanvullende attributen aan serviceproviders, die niet strikt noodzakelijk zijn volgens de AVG voor de levering van de betreffende dienst of product, wat potentieel in strijd is met de privacyregelgeving	Serviceproviders dienen goed te motiveren waarom zij Aanvullende attributen nodig hebben voor hun dienstverlening. Indien deze motivatie onvoldoende is, dient de school als verwerkingsverantwoordelijke verdere verduidelijking te vragen over de noodzaak hiervan. Omdat deze Aanvullende attributen persoonsgegevens zijn dienen deze ook in de verwerkersovereenkomst opgenomen te zijn.		
Detectie brute force aanvallen. Detectie vanuit meermaals onjuist inloggen is enkel zichtbaar vanuit de IDP van de school, dit betekent dat risico's ten aanzien van zogenoemde brute force aanvallen vanuit de school gemitigeerd moeten worden.	implementeer een mechanisme dat het aantal mislukte inlogpogingen binnen een bepaalde tijdslimiet beperkt. Real-time monitoring van inlogactiviteiten kan helpen bij het identificeren van verdachte patronen, waardoor snel actie kan worden ondernomen tegen potentiële brute force-aanvallen.		

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

Beschrijving of de implementatie en gebruik van Entree Federatie 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 Entree Federatie kan veroorzaken. Weeg hierbij mogelijk risico's mee op het gebied van:

- beschrijving en beoordeling risico's voor de betrokkenen;
- beschrijving voorgenomen maatregelen]
- 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 Entree Federatie.]

[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]					
Risico-afweging <u>REST</u>RISICO	**kans**		**impact**		**<u>REST</u>RISICO**	
	NB: het restrisico betreft het risico indien de maatregel <u>wel</u> 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 [SYSTEEM] - na toepassing van risico-mitigerende maatregelen – in [onvoldoende/voldoende/goede] mate beheerst.

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

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

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

H. Risico-mitigerende maatregelen schoolbestuur

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

<u>Het schoolbestuur moet daarom zorgen voor:</u>

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

4. [BESCHRIJF HIER DE MAATREGELEN ZOALS OPGENOMEN BIJ HET ONDERDEEL "Overwegingen implementatie en lokale DPIA"]

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

I. Aanbevelingen

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

A. …

B. …

J. Verklaring schoolbestuur

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

I. kennis te hebben genomen van inhoud en uitkomsten van deze centrale en lokale DPIA;
II. in te stemmen met de in de rapportage genoemde beheersmaatregelen;
III. opdracht te geven voor het uitvoeren van de beheersmaatregelen 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 ENTREE FEDERATIE [WEL/NIET] TE [GEBRUIKEN/CONTINUEREN].

Naam bestuurder(s):

Plaats:

Datum:

Ondertekening: