CENTRALE DPIA

BASISPOORT

Versie 1.0 (september 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	Stefan Ridder (jurist en adviseur IBP) Job Vos (jurist en adviseur IBP) Ferdy IJsselmuiden (DPIA-projectmanager) Pascal Marcelis (jurist en adviseur IBP) Marcel de Rijke (ISO en adviseur IBP) Meindert-Jan Bol (Proominent) Paul-Jan van Goch (Kentalis) Annemieke Koreman (Prins Alexanderschool) Lily Kampers (Wonderwijs) Marcel van Harrewijen (RVKO)
Met dank aan	Edwin Kense (Basispoort) Jan Willem Besteman (Basispoort)
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

Deze DPIA heeft betrekking op Stichting Basispoort. Basispoort is een softwareapplicatie die een zogenaamde Single-Sign-On-toegangsdienst (SSO) biedt voor leerlingen, leerkrachten en onderwijsondersteunende medewerkers in het primair onderwijs om toegang te krijgen tot webbased lesmateriaal ('digitale leermiddelen') van uitgeverijen. Toegang is mogelijk direct via de inlog op www.basispoort.nl of via een technisch aan Basispoort gekoppelde netwerkomgeving van de onderwijsinstelling. Dit stelt scholen in staat om, na eenmaal op het schoolaccount ingelogd te zijn, via Basispoort toegang te krijgen tot de verschillende online lesmaterialen waar gebruik van wordt gemaakt zonder hiervoor een nieuwe inlogprocedure te doorlopen.

Uitvoering van de DPIA

In een periode van ruim een jaar is de DPIA door SIVON uitgevoerd. Dit met de enthousiaste medewerking van een aantal onderwijsinstellingen. Ook Basispoort heeft op een constructieve manier meegewerkt aan het uitvoeren van de DPIA. Basispoort heeft op een transparante wijze inzicht gegeven in de gegevensverwerkingen en de daarmee verbonden risico's voor de betrokkenen.

Conclusie

Basispoort is een samenwerkingsverband tussen vier grote educatieve uitgeverijen en drie schoolleveranciers dat sinds 2011 bestaat. Uit de DPIA is naar voren gekomen dat gedurende de afgelopen dertien jaar de onderwerpen privacy en informatiebeveiliging veel aandacht krijgen en hebben gekregen. Op het gebied van informatiebeveiliging zijn er in de DPIA geen grote risico's aangetroffen die (direct) nadere actie behoeven. Met inachtneming van onderstaande uit te voeren acties, kan er op een veilige manier gebruik worden gemaakt van Basispoort.

Basispoort heeft aangegeven dat er opnieuw gekeken zal worden naar de BIV classificatie en de daarmee verbonden maatregelen op het moment dat er ook koppelingen met systemen die doorstroomtoetsen aanbieden beschikbaar komen.

Gedurende de uitvoering van de DPIA is de door Basispoort gebruikte verwerkersovereenkomst aangepast aan de laatste versie van de standaard van het Privacyconvenant en is deze weer geheel bijgewerkt, zodat er nu een up-to-date en goede verwerkersovereenkomst beschikbaar is voor de onderwijsinstellingen. Een goede verwerkersovereenkomst komt de duidelijkheid ten goede en helpt de onderwijsinstellingen om heldere afspraken te maken met de verwerker van haar persoonsgegevens. Deze nieuwe verwerkersovereenkomst moet wel eerst geaccepteerd worden.

Voor wat betreft de aangetroffen risico's is er één onderwerp waar Basispoort mee aan de slag zal gaan. Dit betreft multi-factor-authenticatie (MFA). MFA kan sinds schooljaar 2023-2024 weliswaar in het systeem worden ingesteld voor een gehele school maar het moet aangezet worden en is niet als *default* ingericht. MFA moet in ieder geval worden toegepast bij rollen met veel rechten op het systeem om daarmee onrechtmatige toegang tot gegevens te voorkomen. Gelet op de rechten die m.n. de beheer rol heeft, zou bij die rol

MFA standaard moeten zijn ingesteld. Basispoort heeft aangegeven dit met ingang van het schooljaar 2024-2025 zo te zullen inrichten.

Om dit risico nu al te beheersen dient de onderwijsinstelling zelf nu al MFA in te schakelen. In dat geval direct voor alle medewerkers.

Daarnaast is er, naast de risico's als gevolg van het niet geaccepteerd zijn van de nieuwe verwerkersovereenkomst en het niet beheren van autorisaties, nog een aantal risico's geïdentificeerd die door de onderwijsinstelling moet worden gemitigeerd. Deze dienen te worden meegenomen in de lokale DPIA. Het betreft:

- Het risico is dat er gegevens beschikbaar worden gesteld aan onbevoegde koppelpartners.
- Het risico is dat er onrechtmatig toegang is tot persoonsgegevens en / of leerresultaten omdat de school in het LAS een niet persoonlijk account aanmaakt voor een algemene invalkracht i.p.v. de veilige door Basispoort aangeboden oplossing.
- Het risico is dat er onrechtmatig toegang is tot persoonsgegevens en / of leervoortgang bij het gebruik van thuisaccounts.
- Het risico is dat er onrechtmatig toegang is tot persoonsgegevens en / of leerresultaten omdat medewerkers wachtwoorden niet veilig genoeg zijn en MFA niet is aangezet.
- Het risico is dat (oud) medewerkers onrechtmatig toegang tot gegevens houden, als het proces bij uitdienst en rolverandering niet goed doorgevoerd wordt in het leerlingadministratiesysteem en in Basispoort.

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 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 moeten 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 die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van aan DPIA verplicht is[1]. 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 Basispoort

Tijdens de uitvoering van het authenticatieproces door Basispoort worden grootschalig en op dagelijkse basisgegevens 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[2] als de EDPB-richtsnoeren[3], 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 Basispoort zijn de volgende criteria:

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

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 Basispoort op een landelijke schaal plaatsvindt door veel leerlingen en leerkrachten/docenten is er sprake van ‘op grote schaal'. Sinds 2013 wordt de Basispoort-dienst dagelijks gebruikt door alle scholen voor Nederlands basisonderwijs. Ruim 125.000 leerkrachten/onderwijsondersteuners en 1,5 miljoen leerlingen hebben altijd single-sign-on toegang (SSO). Op school, thuis of waar dan ook. Via het persoonlijke software-overzicht in Basispoort. Of via een aan Basispoort gekoppelde schoolnetwerkomgeving.[4]

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

[4] https://info.basispoort.nl/over-basispoort/

een onevenwichtigheid in de relatie tussen de positie van de betrokkene en de verwerkingsverantwoordelijke kan worden vastgesteld.

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[5]: “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

[5] 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.

persoonsgegevens verwerken als verwerkingsverantwoordelijke. Denk hierbij aan de 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[6], aangevuld met onderwijs-specifieke informatie uit de *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*[7]. Het model is daarnaast aangepast aan specifieke informatie over 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 betrekking op Stichting Basispoort. Basispoort is een softwareapplicatie die een zogenaamde Single-Sign-On-toegangsdienst (SSO) biedt voor leerlingen, leerkrachten en onderwijsondersteunende medewerkers in het primair onderwijs om toegang te krijgen tot

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

webbased lesmateriaal (‘digitale leermiddelen’) van uitgeverijen. Toegang is mogelijk direct via de inlog op www.basispoort.nl of via een technisch aan Basispoort gekoppelde netwerkomgeving van de onderwijsinstelling. Dit stelt scholen in staat om, na eenmaal op het schoolaccount ingelogd te zijn, via Basispoort toegang te krijgen tot de verschillende online lesmaterialen waar gebruik van wordt gemaakt zonder hiervoor een nieuwe inlogprocedure te doorlopen.

De Stichting Basispoort is een pre-competitief samenwerkingsverband tussen vier grote educatieve uitgeverijen en drie schoolleveranciers. Stichting Basispoort is gestart in 2011. Inmiddels zijn de omgevingen van circa 35 uitgeverijen, netwerkaanbieders (zoals ZuluConnect, MOO, COOL, Prowise GO, RathoPortaal, Skool) en de 2 schooladministratiepakketten ParnasSys en ESIS gekoppeld aan Basispoort. Elke basisschool in Nederland logt via Basispoort in om toegang te verkrijgen tot de digitale leermiddelen. Dit maakt dat je voor de toegang tot de digitale leermiddelen niet om Basispoort heen kunt.

In de toegangsvoorziening tot digitale leermiddelen vallen de volgende producten en diensten:

- Basispoort toegang voor leerkrachten;
- Basispoort toegang voor onderwijsondersteunende medewerkers;
- Basispoort toegang voor leerlingen - op school;
- Basispoort toegang voor leerlingen – buiten school.

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 ten behoeve van het authenticatieproces, waarbij de gebruiker inlogt op de betreffende dienst.

Support & beheer: Hierbij worden contactgegevens van beheerders en hun acties (logging) vastgelegd.

De DPIA geeft daarmee een gestructureerd overzicht van de specifieke verwerkingen die plaatsvinden binnen Basispoort, en legt de focus op het waarborgen van privacy en gegevensbescherming binnen deze context.

VII. Buiten scope

Buiten scope van deze DPIA zijn de netwerkomgeving van de onderwijsinstelling, al dan niet met gebruikmaking van een netwerkleverancier met een eigen SSO-toegangsdienst, het autorisatieproces en de omgeving van het ‘digitale leermiddel'. Ook de software tool die Basispoort gebruikt om dynamische IP adressen van scholen te achterhalen is buiten scope.

De helpdesk ondersteuning die Basispoort levert en waarbij gebruik wordt gemaakt van het softwareprogramma Jira wordt genoemd in deze DPIA maar niet verder uitgewerkt.

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 in de periode mei 2023 t/m mei 2024 uitgevoerd door het in de colofon genoemde DPIA Team.

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.

Anonieme gegevens 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 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 worden 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 Autoriteit Persoonsgegevens (AP) snel inbreuk (kunnen) maken op de persoonlijke levenssfeer. Het gaat bijvoorbeeld om leerresultaten van kinderen, omdat daar conclusies aan kunnen worden verbonden met gevolgen voor het latere maatschappelijke leven. Of het gaat om grote verzamelingen van informatie van (zeer) jonge kinderen, gegevens over (problematische) gezinssituatie oftewel gegevens[8] waaraan zwaardere eisen gesteld aan de beveiliging van de gegevens.

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

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

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

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

verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.

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

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

Pseudonieme persoonsgegevens Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eisen verbonden dat de sleutels apart worden bewaard en dat maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.
Of pseudonieme gegevens door de ontvanger (verwerker) als persoonsgegevens aangemerkt moeten worden hangt af van de omstandigheden van het geval. Het uitvoeren van een toets zal kunnen uitwijzen in hoeverre deze door de leverancier te herleiden zijn tot persoonsgegevens[9].

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.

[9] 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

Basispoort is een softwareapplicatie die een zogenaamde Single-Sign-On-toegangsdienst (SSO) biedt voor leerlingen, leerkrachten en onderwijsondersteunende medewerkers in het primair onderwijs om toegang te krijgen tot webbased lesmateriaal ('digitale leermiddelen') van uitgeverijen. Dit betekent dat gebruikers slechts één keer hoeven in te loggen om toegang te krijgen tot meerdere digitale leermiddelen. Dit vermindert de complexiteit van het inlogproces voor leerlingen en leerkrachten en zorgt voor een betere gebruikerservaring. Via Basispoort worden er dus geen leer- of toetsresultaten opgeslagen en/of uitgewisseld. Basispoort maakt voor de totstandkoming van deze koppeling iedere nacht een download vanuit de LAS (Leerling Administratie Systeem) van de scholen. Dit betekent dat authenticatie door leerlingen en leerkrachten plaatsvindt vanuit de database van Basispoort welke een op een is overgenomen van die van de scholen.

2. Persoonsgegevens

In Basispoort worden persoonsgegevens verwerkt van leerlingen in de basisschool leeftijd en van medewerkers van de onderwijsinstelling.

Basispoort verwerkt GEEN bijzondere of gevoelige persoonsgegevens en geen nationale identificatienummers. Het verwerkt alleen 'gewone' persoonsgegevens. Het verwerkt gegevens van kwetsbare groepen, echter omvat dit alleen de leeftijd en gaat dit niet over inhoudelijke kwetsbaarheden zoals etniciteit.

Overzicht tabel

De volgende (categorieën) persoonsgegevens worden in Basispoort verwerkt.

Categorie betrokkene	Categorie persoonsgegevens	Persoonsgegevens	Bron/verkrijging persoonsgegeven
Minderjarigen (leerlingen)	Algemene contact-gegevens	- voornaam - achternaam, - tussenvoegsel - Voorletters	School (LAS)
	Overige contact-gegevens	- Basispoort-ID (gemaakt door Basispoort) - Basispoort school-ID - laskey - ECK-ID[10] - groepskey	School (LAS) Basispoort

[10] Educatief Content Keten Identificatie is een uniek identificatienummer dat wordt gebruikt om digitale leermiddelen te koppelen aan specifieke onderwijsdoelen en leerlingen.

		- jaargroep	
	Overige gegevens	- wachtwoordplaatje - wachtwoordpincode Bij vanuit huis inloggen - inlogcode thuis - IP-adres (thuis)	Basispoort Minderjarige (leerling)
Medewerker	Algemene contact-gegevens	- voornaam - achternaam, - tussenvoegsel - voorletters - e-mailadres	School (LAS)
	Overige contact-gegevens	- Basispoort-ID (gemaakt door Basispoort) - Basispoort school-ID - laskey - ECK-ID - groepskey	School (LAS) Basispoort
	Overige gegevens	- wachtwoord, - MFA code (optioneel). - optioneel: rol (ICT-coordinator, RT'er, IB'er, invalkracht of stagiair)	Basispoort School Medewerker

3. Gegevensverwerkingen

De verwerkingen door Stichting Basispoort vinden primair plaats om leerlingen, leerkrachten en onderwijsondersteunende medewerkers (gebruikers) in staat te stellen om toegang te verkrijgen (authenticatie van de gebruiker) tot online educatief materiaal door middel van één uniforme inlogprocedure. Voor de opsomming van de verwerkingen die binnen Basispoort plaatsvinden is aansluiting gezocht bij de referentiearchitectuur (FORA[11] voor het primair en voortgezet onderwijs) en de verwerkersovereenkomst.

Verwerkingen bij het gebruik van SSO-toegangsvoorziening van Basispoort vinden plaats ten behoeve van de volgende FORA processen:

- ICT ondersteuning;
- Onderwijsuitvoering;
- Informatiebeveiliging en privacy.

Deze FORA-processen behelzen standaard de volgende feitelijke gegevensverwerkingen:

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

a) het handmatig of geautomatiseerd ontvangen en opslaan van een gegevensbestand uit het leerling administratie systeem (LAS) van de onderwijsinstelling, dat in Basispoort niet muteerbaar is;
b) het aanmaken en muteren van accountgegevens van onderwijsondersteunende gebruikers;
c) het verlenen van toegang (authenticatie) aan gebruiker tot digitale leermiddelen door een single-sign-on;
d) het verzorgen van backups van accountgegevens;
e) het verzorgen van backups van mutatie van en toegang tot persoonsgegevens (logging-informatie)
f) het verlenen van inzage aan de Verwerkingsverantwoordelijke in de accountgegevens;
g) het verlenen van inzage aan de Verwerkingsverantwoordelijke in de accountgegevens op verzoek van de onderwijsinstelling;
h) het verlenen van inzage aan de Verwerkingsverantwoordelijke in de logging-informatie;
i) het verlenen van inzage aan de Verwerkingsverantwoordelijke en of gebruiker in de logging-informatie op verzoek van de Verwerkingsverantwoordelijke;
j) het op eerste verzoek van de Verwerkingsverantwoordelijke verwijderen van persoonsgegevens van gebruiker;
k) het verlenen van inzage in een overzicht via het beheerscherm van door de onderwijsinstelling geactiveerde licenties;
l) het doorgeven van persoonsgegevens aan leveranciers van digitale leermiddelen of netwerkomgevingen van de onderwijsinstelling waarvoor door de onderwijsinstelling in Basispoort toestemming is verleend, waarbij door Verwerker in geen geval gegevens worden doorgegeven aan leveranciers van leermiddelen of netwerkomgevingen van de onderwijsinstelling waarvoor de onderwijsinstelling in Basispoort geen toestemming heeft gegeven;
m) het beheren en uitvoeren van een licentiekantoor (Basispoort Hosted Lika) namens de leveranciers van leermiddelen, t.b.v. de toewijzing van leermiddelen aan gebruikers, waarbij de onderwijsinstelling in de Basispoort-applicatie aan de Verwerker toestemming heeft verleend, persoonsgegevens te mogen verwerken.

De onderwijsinstelling kan de doorgifte van persoonsgegevens als bedoeld onder l en m aan iedere Participant via de Basispoortdienst activeren en deactiveren. Door Verwerker worden geen leer- of toetsresultaten opgeslagen en/of uitgewisseld.

<u>Optionele verwerkingen</u>

Bij het gebruik van SSO-toegangsvoorziening van Basispoort kunnen met specifieke toestemming van de onderwijstelling ook andere verwerkingen plaatsvinden. Onderwijsinstellingen hebben voor deze verwerkingen een actieve keuzeoptie en gaan in Basispoort expliciet akkoord met de verwerkingen voordat deze plaatsvinden. Het betreft verwerkingen in het kader van:

a) Het verlenen van toegang aan gebruiker tot leermiddelen buiten de schoolomgeving (thuis) door een single-sign-on. De verwerkersverantwoordelijke kan deze optionele dienstverlening zelf activeren en deactiveren.
b) Het verlenen van toegang aan gebruikers tot leermiddelen vanuit een door de onderwijsinstelling gekozen en technisch aan Basispoort gekoppelde schoolnetwerkomgeving door een single-sign-on. De verwerkersverantwoordelijke kan deze optionele dienstverlening zelf activeren en deactiveren.

Helpdesk

In overeenstemming met de verwerkersovereenkomst en de daarin besloten opdracht tot gegevensverwerking biedt Basispoort, in de rol van verwerker, ondersteuning aan de (eind)gebruikers. Voor ondersteuning aan scholen worden in een speciale helpdesk omgeving, naast genoemde informatie beschikbaar in de Basispoort applicatie, aanvullende contactgegevens opgeslagen. Dit betreft dan de opslag van telefoonnummers van schoolmedewerkers en soms ook gegevens van ouders. Hiervoor gebruikt Basispoort Jira als ticketregistratieprogramma. 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. Deze ondersteuning aan de (eind)gebruikers wordt verzorgd door (medewerkers van) Uitgeverij Malmberg.

Het indienen van ondersteuningsverzoeken en de eventueel in dat kader verwerkte persoonsgegevens is buiten scope en verder niet onderzocht in deze DPIA.

Applicatielandschap

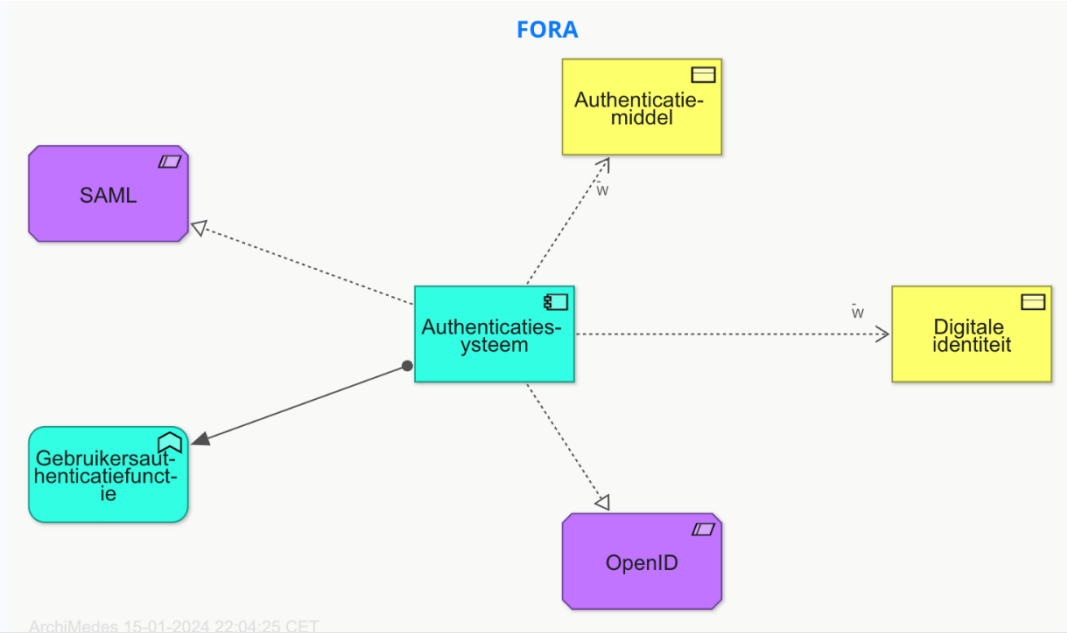
In de toegangsvoorziening tot digitale leermiddelen vallen de volgende producten en diensten:

- Basispoort toegang voor leerkrachten;
- Basispoort toegang voor onderwijsondersteunende medewerkers;
- Basispoort toegang voor leerlingen - op school;
- Basispoort toegang voor leerlingen - buiten school.

De verwerking van persoonsgegevens binnen deze producten en diensten heeft betrekking op: Het gepersonaliseerd toegang krijgen tot ‘digitale leermiddelen’ van uitgeverijen, d.m.v. een inlogprocedure op www.basispoort.nl of via een technisch aan Basispoort gekoppelde netwerkomgeving van de onderwijsinstelling.

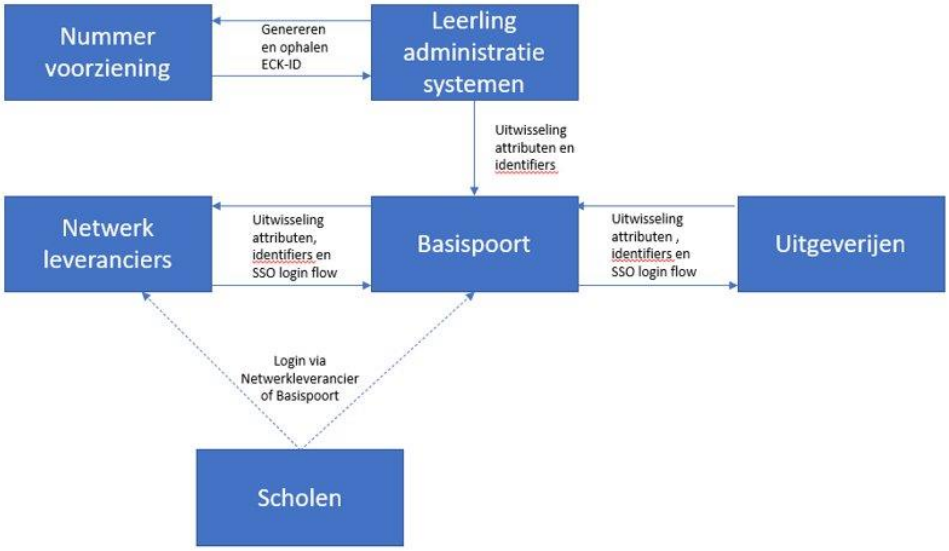
In referentie architectuur termen is Basispoort een Authenticatiesysteem. De FORA omschrijft dit als een systeem of geheel van systemen en modules dat Authenticatie van gebruikers uitvoert aan de hand van een Authenticatiemiddel. Een authenticatiemiddel is dan een middel waarmee met (een bepaalde mate van) zekerheid de digitale identiteit van een individu wordt vastgesteld. Dit met als doel het recht van een geauthentiseerde

identiteit vast te stellen om gebruik te maken van bepaalde functionaliteit. In dit specifieke geval het gebruik maken van leermiddelen.[12]

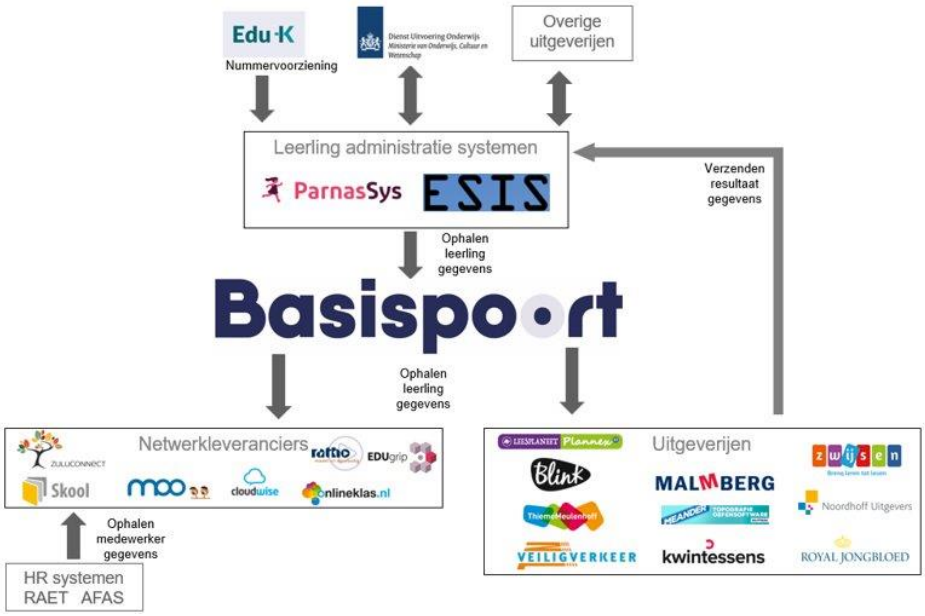


Koppelingen en gegevensstromen

In de onderstaande afbeeldingen is weergegeven welke koppelingen en er zijn en hoe de gegevensstromen plaatsvinden.



[12] https://fora.wikixl.nl/index.php/FORA/id-16ae32a3-0d2b-49f7-b994-f21fbea6b160



De volgende gegevens worden uitgewisseld via deze koppelingen

Leerling gegevens. De gegevens van leerlingen zijn afkomstig uit het Leerling Administratie Systeem (LAS). Basispoort heeft een automatische koppeling met een LAS (ParnasSys of Esis) en gebruikt voor uitwisseling van gegevens de UWLR 2.3 standaard.

Resultaatgegevens worden direct verzonden door de uitgever naar het LAS en gaan dus niet via Basispoort.

Medewerker gegevens. De gegevens van medewerkers zijn afkomstig uit het Leerling Administratie Systeem (LAS) nadat deze zijn opgehaald uit het Personeel Informatie Systeem van de onderwijsinstelling.

Koppelpartner (uitgevers van digitale leermiddelen): er is een koppeling met de verschillende uitgeverijen van digitale leermiddelen. Basispoort is niet verantwoordelijk voor partijen die aansluiten, maar stelt wel als eis dat ze lid zijn van het privacyconvenant, het ROSA certificeringsschema gebruiken en een security test laten uitvoeren, waarbij de hoge risico's opgelost zijn 'voordat de knop wordt' omgezet en de risico's met classificatie 'midden', middels pas toe of leg uit binnen twee maanden zijn opgelost. De (licentie) informatie flow loopt als volgt:

Gebruikers willen en mogen alleen licenties zien waarop zij recht hebben. Dit geldt binnen de Basispoort omgeving, maar ook vanuit een netwerkomgeving. Om dit mogelijk te maken zijn er verschillende licentieprocessen beschikbaar. Licenties zijn persoonsgebonden. Een licentie moet gekoppeld worden aan een gebruiker. Dit gebeurt via het ECK-iD en School-iD en/of via het Basispoort-iD.

Basispoort heeft een koppeling met een licentiekantoor (LIKA of Hosted-LIKA). De uitgever is verantwoordelijk voor de licentietoewijzing aan de juiste leerling. Koppelingen lopen via TLS

encrypted verbindingen. Gegevens uitwisselingen met Uitgeverijen/ Netwerkleveranciers alleen via mTLS (dus inlog via een client certificaat).

Licentie kantoor (LIKA)
Basispoort haalt real-time de licentiegegevens op uit een uitgeverij-LIKA (Licentie Kantoor). Daarvoor bestaan er twee flows:
o De LIKA-flow:
Hierbij wordt het licentiekantoor van de uitgeverij rechtstreeks benaderd.
o De Hosted-LIKA-flow:
Hierbij schrijft de uitgeverij de koppeling tussen leerling en licentie weg in de database van Basispoort.

Omdat voor iedere gebruiker die inlogt een vraag gesteld wordt aan het LIKA, wordt van het licentie kantoor een zeer goede performance geëist: maximaal 1 seconde; ook tijdens piekmomenten. Onder meer om die reden wordt deze flow ook alleen door de grotere uitgeverijen (met materiaal voor alle vakken) gebruikt. De meeste uitgeverijen maken gebruik van de Hosted-LIKA-omgeving. Voor de performance van deze Hosted-LIKA omgeving, is Basispoort zelf verantwoordelijk.

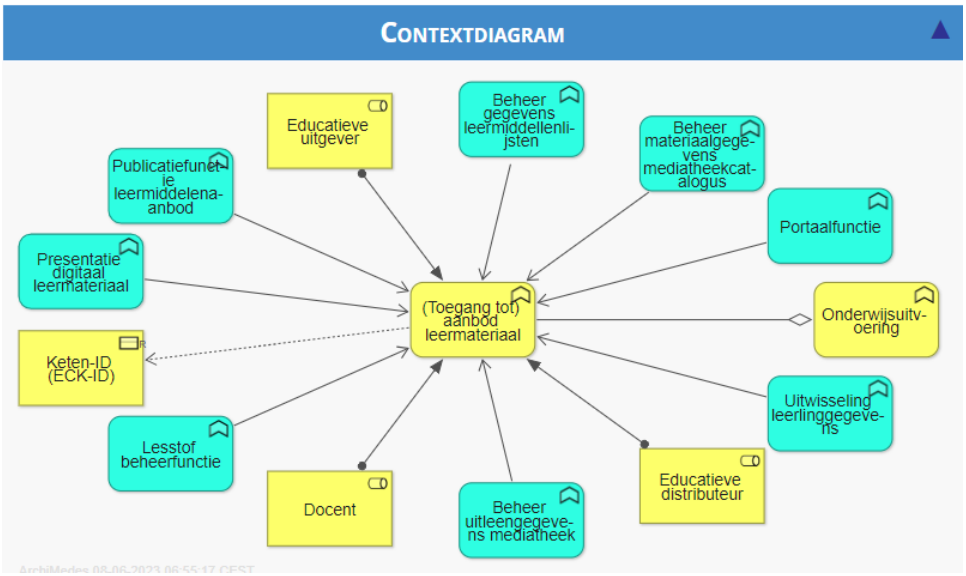
Alleen relevante licenties
Basispoort is een pre-competitieve samenwerking. Het portaal mag door de participanten en partners niet gebruikt worden voor commerciële doelstellingen. Het is daarom ook niet toegestaan om ongevraagd licenties aan een gebruiker toe te kennen. Uitgeverijen dienen er ook voor te zorgen dat licentietoewijzing plaatsvindt aan de juiste leerlingen. Voorkomen moet worden dat leerlingen licenties zien, die zij niet behoren te zien. Het is aan de uitgeverijen hoe zij dit proces inrichten. Veel gebruikt is:
1. licenties toekennen op basis van het leerjaar van de leerling;
2. licenties toekennen op basis van de stamgroep;
3. licenties individueel toekennen;
4. een combinatie van de bovenstaande mogelijkheden.
Het toekenningsproces (welke optie dan ook) vindt altijd plaats in het domein van de uitgeverij.

Consent management
Consent management in Basispoort regelt de toegang tot data per koppelpartner. Er vindt dataminimalisatie plaats, daar waar mogelijk met een jaarlijkse analyse.

4. Verwerkingsdoeleinden

Basispoort heeft als applicatie een ‘portaalfunctie’. Dit betekent dat Basispoort als "toegangspoort" fungeert wat uit diverse bronnen geselecteerde informatie biedt en/of toegang geeft tot verschillende informatiebronnen. De meest gebruikte toegang ziet op de leermiddelen waartoe zowel leerling als leerkracht toegang krijgen via Basispoort.

Vanuit een FORA-perspectief is het doel van de verwerking het geven van toegang tot aanbod leermateriaal (bedrijfsfunctie) als onderdeel van het proces onderwijsuitvoering (hoofd bedrijfsfunctie).



Afbeelding: context diagram bedrijfsfunctie [(Toegang tot) aanbod leermateriaal - Funderend Onderwijs Referentie Architectuur (wikixl.nl).]

De verwerkingsdoeleinden sluiten aan bij de in het Privacyconvenant[13] opgenomen verwerkingsdoeleinden:

a) het geleverd krijgen / in gebruik kunnen nemen van digitale onderwijsmiddelen conform de afspraken die zijn gemaakt tussen het schoolbestuur en de leverancier;
b) het verkrijgen van toegang tot de aangeboden digitale onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;
c) 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 verwerkingsdoeleinden zijn schematisch weergegeven en gekoppeld aan de verwerking

Gegevensverwerking (par.3 Gegevensverwerkingen)	Doeleinde verwerking (par.4. Verwerkingsdoeleinden)	Toelichting
• het handmatig of geautomatiseerd ontvangen en opslaan van een gegevensbestand uit het leerling administratie systeem (LAS) van de onderwijsinstelling, dat in Basispoort niet muteerbaar is; • het aanmaken en muteren van accountgegevens van	• het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen het schoolbestuur en de Leverancier.	

[13] https://www.privacyconvenant.nl/downloads

onderwijsondersteunende gebruikers; • het verlenen van toegang (authenticatie) aan gebruiker tot digitale leermiddelen door een single-sign-on;		
• het verzorgen van backups van accountgegevens; • het verzorgen van backups van mutatie van en toegang tot persoonsgegevens (logging-informatie) • het verlenen van inzage aan de Verwerkingsverantwoordelijke in de accountgegevens; • het verlenen van inzage aan de Verwerkingsverantwoordelijke in de accountgegevens op verzoek van de onderwijsinstelling; • het verlenen van inzage aan de Verwerkingsverantwoordelijke in de logging-informatie; • het verlenen van inzage aan de Verwerkingsverantwoordelijke en of gebruiker in de logging-informatie op verzoek van de Verwerkingsverantwoordelijke; • het op eerste verzoek van de Verwerkingsverantwoordelijke verwijderen van persoonsgegevens van gebruiker; • het verlenen van inzage in een overzicht via het beheerscherm van door de onderwijsinstelling geactiveerde licenties;	• 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.	
• het doorgeven van persoonsgegevens aan leveranciers van digitale leermiddelen of netwerkomgevingen van de onderwijsinstelling waarvoor door de onderwijsinstelling in Basispoort toestemming is verleend, waarbij door Verwerker in geen geval gegevens worden doorgegeven aan leveranciers van leermiddelen of netwerkomgevingen van de onderwijsinstelling waarvoor de onderwijsinstelling in Basispoort	• het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie.	

geen toestemming heeft gegeven;; • het beheren en uitvoeren van een licentiekantoor (Basispoort Hosted Lika) namens de leveranciers van leermiddelen, t.b.v. de toewijzing van leermiddelen aan gebruikers, waarbij de onderwijsinstelling in de Basispoort-applicatie aan de Verwerker toestemming heeft verleend, persoonsgegevens te mogen verwerken.		

5. Betrokken partijen

De volgende organisaties zijn betrokken bij de gegevensverwerkingen:

Naam partij	**AVG-rol**	**Functie/taak**	**Betrokken persoonsgegevens**	**Verstrekker of ontvanger**
Schoolbestuur	Verwerkingsverantwoordelijke	Beschikbaar stellen leermiddelen	Alle genoemde persoonsgegevens	Verstrekker
Leerlingen en medewerkers	Betrokkenen	Eindgebruiker	Alle genoemde persoonsgegevens	Verstrekker
IO Digital, Marconilaan 16, 5621 AA, Eindhoven	Subverwerker	Beheer van de Basispoort-dienst. Ontwikkeling van de Basispoort applicatie.	Alle genoemde persoonsgegevens	Ontvanger
Microsoft Ireland Operations Limited, Dublin, Ierland	Subverwerker	Aanbieder van Microsoft Azure, serverinfrastructuur voor cloudopslag.	Alle genoemde persoonsgegevens	Ontvanger
Atlassian, Sydney, Australië	Subverwerker	Jira Service management applicatie voor het registreren van helpdesk meldingen.	Contactgegevens	Ontvanger
SendGrid, divisie van: Twilio Inc., 375 Beale Street, Suite 300, San	Subverwerker	Cloud-based mail verzend service die het mogelijk maakt mails (met name	Contactgegevens, Gebruikersgegevens, Overige gegevens – correspondentiegegevens	Ontvanger

Francisco, CA 94105 USA		wachtwoordmail) vanuit de Basispoort applicatie naar schoolmedewerkers te verzenden		
Malmberg Magistratenlaan 138 5223 MB 's-Hertogenbosch	Subverwerker	Helpdesk/landelijk beheer: ondersteuning van Gebruikers.	Alle genoemde persoonsgegevens	Ontvanger
Kense Informatie Management B.V. Brede steeg 20 5062KH Oisterwijk	Subverwerker	Technische coördinatie, ondersteuning 1e lijns helpdesk en databeheer in de 2e lijn.	Alle genoemde persoonsgegevens	Ontvanger
NextBest Marketing Communicatie Management	Subverwerker	Algemene coördinatie, ondersteuning 1e lijns helpdesk en databeheer in de 2e lijn.	Alle genoemde persoonsgegevens	Ontvanger
Koppelpartner (zie Partners & koppelingen - Basispoort)	Verwerker	Aanbieden digitale (leer)middelen	ECK-iD en School-iD en/of het Basispoort-iD	Ontvanger

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.

Basispoort in de rol van verwerker ziet heeft als taak het aanbieden van een betrouwbare SSO-dienst ten behoeve van het koppelen tussen het schoolbestuur en de aanbieders van digitale (leer)middelen.

Het belang van de door Basispoort ingeschakelde subverwerkers is het zorgen voor een zo goed mogelijk werking van het systeem.

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
IO Digital	Nederland	Beheer van de Basispoort-dienst. Ontwikkeling van de Basispoort applicatie.	Nederland: Microsoft Azure, Middenmeer
Microsoft	Verenigde Staten	Aanbieder van Microsoft Azure, serverinfrastructuur voor cloudopslag.	Nederland: Microsoft Azure, Middenmeer
Atlassian	Australië	Jira Service management applicatie voor het registreren van helpdesk meldingen.	Amazon (AWS) Frankfurt of AWS Dublin.
Sendgrid (Twilio)	Verenigde Staten	Cloud-based mail verzend service die het mogelijk maakt mails (met name wachtwoordmail) vanuit de Basispoort applicatie naar schoolmedewerkers te verzenden	Zie hiervoor: https://www.twilio.com/en-us/legal/sub-processors
Uitgeverij Malmberg	Nederland	Helpdesk/landelijk beheer: ondersteuning van Gebruikers.	Den Bosch
Kense Informatie	Nederland	Technische coördinatie,	Oisterwijk

Management B.V.		ondersteuning 1e lijns helpdesk en databeheer in de 2e lijn.	
NextBest Marketing Communicatie Management	Nederland	Algemene coördinatie, ondersteuning 1e lijns helpdesk en databeheer in de 2e lijn.	Udenhout

8. Data Transfer Impact Assessment (DTIA)

De AVG bevat specifieke regels voor de doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER). In beginsel mogen persoonsgegevens alleen worden overgedragen aan landen buiten de EER als het land een 'passend beschermingsniveau' heeft. Dat niveau kan op verschillende manieren worden bepaald: een multinational kan bindende bedrijfsvoorschriften vaststellen (BCR's), de EU-standaardcontractbepalingen (SCC) toepassen of alleen overdragen aan landen waarvoor de Europese Commissie een zogeheten adequaatheidsbesluit[11] heeft genomen.

Basispoort verwerkt de persoonsgegevens in Europese datacenters van het Amerikaanse bedrijf Microsoft. Buiten Europa worden persoonsgegevens verwerkt t.b.v. e-mails.

Op 10 juli 2023 heeft de EC (Europese Commissie) het adequaatheidsbesluit voor het nieuwe Data Privacy Framework (DPF) tussen de EU en Verenigde Staten (VS) aangenomen. Het Framework is de opvolger van het eerdere EU-VS Privacy Shield dat door het Europese Hof van Justitie met haar Schrems II-uitspraak in 2020 ongeldig werd verklaard, omdat de rechten van Europese burgers onvoldoende beschermd waren. De Europese Commissie heeft bepaald dat dit met het nieuwe Framework is opgelost. Dat betekent dat organisaties binnen de EER op basis van het nieuwe besluit veilig persoonsgegevens kunnen doorgeven aan bedrijven in de VS die deelnemen aan het nieuwe Framework.

Microsoft en Sendgrid (Twilio) zijn aangesloten bij het nieuwe DPF. Zie: https://www.dataprivacyframework.gov/s/participant-search.

Bij Atlassian, de leverancier van het helpdesksysteem Jira, die de gegevens verwerkt bij AWS in Frankfurt of Dublin, geldt dat er voor Australië geen adequaatheidsbesluit van toepassing is. Atlassian heeft hiervoor een DTIA[14] uitgevoerd. Daaruit zijn grote risico's naar voren gekomen.

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

[14] https://www.atlassian.com/legal/data-transfer-impact-assessment#intro

abstracte formulering wordt gebruik gemaakt van de voor de verwerkers opgestelde standaard DPIA-vragenlijst. Deze vragenlijst wordt door de verwerker gevuld en zal voor een belangrijk deel inzicht geven in o.a. de genomen technische beheersmaatregelen en informatiebeveiliging.

Technische analyse en cookies

Tijdens het verkrijgen van technische inzichten in Basispoort is gebruik gemaakt van een netwerkanalyse en een inlogsessie op de omgeving van Basispoort.

In de ontwikkelaars weergave van de browser is gekeken naar de cookies die Basispoort plaatst. Er worden geen 3rd party cookies geplaatst.

Bij problemen kan door de eindgebruiker client logging ingeschakeld worden, alleen dan wordt een speciale cookie geplaatst. Deze is actief voor een periode van maximaal 7 dagen.

Basispoort gebruikt een software tool om dynamische IP adressen van scholen te achterhalen. Deze software moet op een lokale PC draaien. We hebben deze software niet geïnstalleerd en is daarmee buiten scope van deze DPIA. Stichting Basispoort geeft aan dat deze tool door minder dan 10 scholen geïnstalleerd en gebruikt wordt.

Bij automatische ophalen van gebruikersgegevens uit de LAS systemen ParnasSys en ESIS komt de koppeling tot stand waarbij een autorisatiesleutel wordt gebruikt. Hiermee is geborgd dat de school in het LAS systeem expliciet toestemming heeft gegeven dat de leerling, leerkracht en groepsgegevens van die school met Basispoort mag worden gedeeld. De verbinding is op basis van minimaal TLS 1.2.[15.]

Indien de school gebruik maakt van een gekoppelde netwerkleverancier wordt er via een SAML[16]-request en een SAML-response de identiteit vastgesteld. Basispoort ondersteunt geen rechtstreekse koppelingen met Google Workspace of Microsoft 365. Basispoort accepteert alleen koppelingen vanuit de netwerkleveranciers.

Het loggen van ongebruikelijke activiteiten wordt door Basispoort gedocumenteerd, geanalyseerd en opgevolgd met gepaste maatregelen.

Mailmogelijkheden

Basispoort maakt gebruik van Sendgrid. Dit is een cloud-based mail verzend service die het mogelijk maakt mails (met name wachtwoordmail) vanuit de Basispoort applicatie naar schoolmedewerkers te verzenden. Scholen kunnen niet mailen via dit systeem en ontvangen ook geen e-mails.

[15] Bron: https://www.edustandaard.nl/app/uploads/2017/05/ECK_Distributie_en_Toegang_2.1_-Technische_Voorschriften_Services.pdf en https://www.edustandaard.nl/standaard_afspraken/uniforme-beveiligingsvoorschriften/uniforme-beveiligingsvoorschriften-1-0/

16Security Assertion Markup Language (SAML) is een op XML gebaseerde standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

Invalkrachten

Basispoort kent ‘standaard’ voor iedere groep een ‘anoniem’ account voor een ‘invalleerkracht’. Op de dag van invallen, kan dit account worden geactiveerd door de ICT-coördinator. Hierbij wordt het e-mail adres van de invalkracht gebruikt. Er moet worden aangevinkt of dit account 1, 2 of 5 dagen actief moet blijven. Ook de naam van de invalleerkracht kan worden ingevuld (niet verplicht). De invalkracht heeft toegang tot het groepsoverzicht van zijn of haar invalgroep en tot alle gekoppelde methodesoftware (voor de ingestelde periode van 1,2 of 5 dagen). De ICT-coördinator kan het account op ieder moment deactiveren. Is toegang voor de invalkracht langer dan 5 dagen gewenst, dan kan de periode worden verlengd. Staat een invalkracht langer dan 10 dagen voor de groep, dan is het aan te bevelen deze (tijdelijk) als groepsleerkracht aan te maken in het LAS. Dan krijgt de invaller (tijdelijk) een Basispoort-account ‘als reguliere leerkracht’. In het scherm staat de einddatum voor een invalkracht ‘default’ op 2026. Deze datum wordt specifiek (er verschijnt een ‘echte’ datum), zodra een invalkracht wordt geactiveerd voor 1, 2 of 5 dagen.

Onderzoek Informatiebeveiliging

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

Voor dit onderzoek is de volgende informatie verstrekt:

- Basispoort is niet ISO27001 gecertificeerd maar conformeert zich aan de NCSC richtlijnen voor veilig ontwikkelen van applicaties[17].
- Basispoort voert jaarlijks een pentest uit. Een TPM verklaring van een pentest uit 2023 over de testresultaten is verstrekt.
- Basispoort geeft aan te voldoen aan de gestelde vereisten van het ROSA certificeringsschema (voor de niveaus hoog-medium-medium voor resp. Betrouwbaarheid, Integriteit en Vertrouwelijkheid).
- Toelichting is verstrekt van het IB beveiligingsbeleid en de PDCA cyclus van hun ISMS. Er is inzage verstrekt in het IB beleid en jaarplan. De status wordt regelmatig besproken met het bestuur en jaarlijks wordt een IB jaarverslag opgesteld. Er zijn geen bijzonderheden geconstateerd.

Er zijn geen aanbevelingen ten aanzien van informatiebeveiliging.

IAMA: mensenrechten in beeld bij algoritmes

Omdat uit voornoemde DPIA-vragenlijst, interviews met Basispoort 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.

[17] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties

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	**Normenkader IBP**	**Hoofdstuk 10, Identity & Access Management**
Logging	**Normenkader IBP**	**Hoofdstuk 11.4 Security Management**

11. Bewaartermijnen

Stichting Basispoort verwijdert de verkregen persoonsgegevens uit de database ten behoeve van het uitvoeren van de SSO-toegangsvoorziening op periodieke basis, gebaseerd op de werking van het schooljaar. Basispoort verwijdert de gegevens die door de onderwijsinstelling inactief zijn gemaakt. Gebruikers worden inactief indien:

- deze niet meer (tijdens de dagelijkse nachtelijke download) uit het LAS-bestand meekomen naar Basispoort;
- deze in Basispoort handmatig zijn aangemaakt en daarna door de school weer handmatig worden verwijderd;
- de onderwijsinstelling aan Basispoort vraagt om de voorwaarden in te trekken (de onderwijsinstelling in Basispoort op te heffen).
- Basispoort erachter komt dat een onderwijsinstelling en daarmee de verwerkersverantwoordelijke niet meer bestaat. Dan trekt Basispoort de voorwaarden in.

Basispoort kan de gegevens eerder wissen, maar de verwerkersverantwoordelijke moet deze binnen een redelijke termijn kunnen opvragen. Maandelijks worden gegevens van

accounts in Basispoort die al 3 maanden niet meer de status ‘actief’ hebben, verwijderd uit de database.

Gegevensverwerking	Verwerkingsdoeleinde	Categorie persoonsgegevens	Bewaartermijn en grondslag
• Gegevens van scholen • Gegevens van leerkrachten en onderwijsondersteunende medewerkers • Gegevens van leerlingen • Optionele persoonsgegevens	• Het geleverd krijgen / in gebruik kunnen nemen van digitale onderwijsmiddelen conform de afspraken die zijn gemaakt tussen het schoolbestuur en de leverancier; • Het verkrijgen van toegang tot de aangeboden digitale onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie.	Algemene en overige contactgegevens	Max 1,5 jaar. Maandelijks worden gegevens van accounts in Basispoort die al 3 maanden niet meer de status ‘actief’ hebben, verwijderd uit de database.
Inlogs: bevat tijdstip, Basispoort id en ip-nummer	• 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.	Algemene en overige contactgegevens	Max 1,5 jaar. Basispoort verwijdert maandelijks reguliere logging-gegevens die ouder zijn dan 18 maanden.
Auditlog: bevat privacyrelevante beheersactiviteiten door ICT coördinator en/of beheerder	• 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.	Algemene en overige contactgegevens	Max 1,5 jaar. Audit log wordt bewaard tot een school wordt verwijderd.

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[18]

d) Vitaal belang van de betrokkene

e) Taak van algemeen belang[19] (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 Basispoort, wordt in het onderstaande uiteengezet wat de regels zijn omtrent het aanbieden van leermiddelen in het primair onderwijs (hierna: po) 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.

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

[18] 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.

[19] 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.

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.

De wetgever heeft hiermee een rechtsgrond voor de gegevensverwerking in het leven geroepen. Dit geeft (indirect) aan dat een onderwijsinstelling in het kader van haar taken zoals bedoeld in de WPO, namelijk het geven van onderwijs, digitale leermiddelen mag inzetten en daarbij gebruik kan maken van ondersteunende digitale diensten (zoals Basispoort). De AVG schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. Het is voldoende dat de hoofdlijnen uit de WPO kenbaar zijn. Er kan dus worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen waaronder een SSO-dienst.

Het is de verantwoordelijkheid van de school om te waarborgen dat leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen. Het implementeren van een SSO-dienst ondersteunt dit proces.

Technische maatregelen

De AVG[20] 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.

Basispoort 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 bieden van veilige inlogmethoden vormgegeven aan de vereisten van artikel 32 AVG.

13. Bijzondere persoonsgegevens

Binnen de SSO-dienst van Basispoort 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.

[20] Artikel 32 AVG, beveiliging van de verwerking

Basispoort 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 Basispoort is er na een eerste beoordeling geen noodzaak voor een nadere analyse met betrekking tot de kinderrechten. Dit komt voort uit het feit dat Basispoort 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

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

Uit de gegevensverwerkingsanalyse, blijkt dat de door Basispoort te verwerken persoonsgegevens noodzakelijk zijn in relatie tot het doel van de gegevensverwerking, te weten het via het toepassen van de SSO-oplossing kunnen waarborgen van een ononderbroken ontwikkelingsproces[21] voor de leerling.

16. b. Proportionaliteit en subsidiariteit

Bij het gebruik van de SSO-dienst worden uitsluitend noodzakelijke gegevens veilig via de SAML-procedure 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 Basispoort is opgezet om zo weinig

[21] Zie artikel 8 WPO.

mogelijk persoonsgegevens uit te wisselen met de leverancier van het leermiddel of dienst. Deze privacy vriendelijke toegang biedt het voordeel dat gebruikers 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

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

Van iedere onderwijsinstelling die gebruik maakt van Basispoort wordt verondersteld dat deze op haar website een duidelijke privacyverklaring en/of privacyreglement heeft opgenomen. Hierin staat voldoende beschreven welke rechten betrokkenen hebben betreffende de verwerking van hun persoonsgegevens en hoe men hun rechten kan uitoefenen.

De onderwijsinstelling kan via de applicatie van Basispoort in beginsel zelf de informatie vinden die van belang is voor het voldoen aan een verzoek van een betrokkene (leerling/ouder/medewerker) om inzicht te hebben in welke persoonsgegevens voor welke doeleinden worden verwerkt.

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking*
Het recht op informatie	Bijvoorbeeld: • Openbaar gepubliceerde privacyverklaring; • Intern gepubliceerde privacyverklaring; • Versturen van een digitale brief naar e-mailadres betrokkenen.	n.v.t.
Het recht van inzage	Basispoort kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Het recht op rectificatie	Basispoort kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Het recht op gegevenswissing	Basispoort kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Het recht op beperking van de verwerking	Basispoort kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	Basispoort kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.

Het recht op overdraagbaarheid van gegevens	n.v.t.	n.v.t.
Het recht van bezwaar	Basispoort kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit	N.vt	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 heeft ook een praktische toets plaatsgevonden. Hierbij is een vergelijking gemaakt tussen de in de theorie genoemde afspraken en de verwerkingen die in de praktijk plaatsvinden.

De verwerkersovereenkomst van Basispoort is getoetst. De verwerkersovereenkomst voldoet, na diverse aanpassingen gedurende het gehele DPIA traject, aan de eisen. Er zijn na aanpassing geen risico's meer over die aan ondertekening in de weg staan. De verwerkersovereenkomst en het Toetsrapport zijn beschikbaar via de Dienst Verwerkersovereenkomsten van Kennisnet. NB. Deze nieuwe versie van de verwerkersovereenkomst moet wel door de school geaccepteerd worden.

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 rechtmatig (Deel B) worden afgewogen tegen de rechten en vrijheden van betrokkenen. De risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden beschreven en beoordeeld. Hierbij wegen de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen mee.

Beoordelingskader risico's

Alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden 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.
Negatieve gevolgen van de gegevensverwerking zijn bijvoorbeeld:

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

De methodiek die wordt gevolgd, is beschreven door de Britse toezichthouder[22] 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.

[22] 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

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

Hulpmiddel beoordelen score laag, midden en hoog

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

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

De in deze centrale DPIA geconstateerde risico's betreffen:

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 Basispoort 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:

Risico nr.	Mapgood	Risico-omschrijving	Oorzaak	Kans	Impact	Risico	Proces en/of systeem-risico?
1	O	Het risico is dat de verwerkingsverantwoordelijke geen toereikende afspraken	Er is geen getekende verwerkersovereenkomst. Als er geen goede afspraken met de	2	2	4	Proces (school)

		met de verwerker heeft gemaakt over de verwerking van de persoonsgegevens.	verwerker zijn gemaakt kan dat tot gevolg hebben dat de verwerking niet aan de vereisten van de AVG voldoet en dat de bescherming van de rechten van betrokkenen daardoor onvoldoende is gewaarborgd.				
2	O	Het risico is dat er gegevens beschikbaar worden gesteld aan onbevoegde koppelpartners.	De ICT coördinator kan in Basispoort aangeven welke partijen gegevens mogen ophalen uit Basispoort. In principe kan dan ook een partij die geen leverancier (meer) is gegevens ophalen.	2	2	4	Proces (school)
3	O	Het risico is dat er bij accounts (met veel rechten) onregelmatigheden plaatsvinden doordat de toegang tot de applicatie onvoldoende is beveiligd.	Onderwijsinstellingen stellen het gebruik van MFA (bij beheerders) niet verplicht (omdat het alleen voor de gehele school is in te stellen). De kans is groter dat onbevoegde gebruikers toegang krijgen tot persoonsgegevens en/of gegevens worden gemuteerd.	3	3	9	Proces en Systeem (Basispoort en school)
4	O	Het risico is dat er onrechtmatig toegang is tot persoonsgegevens en / of leerresultaten omdat de school in het LAS een niet persoonlijk account aanmaakt voor een algemene invalkracht i.p.v. de veilige door Basispoort aangeboden oplossing.	Basispoort heeft standaard voor iedere school, per groep in het LAS van de school, een ‘anoniem’ account voor een invalleerkracht aangemaakt. Op de dag van invallen kan dit zogenaamde ‘invalaccount’ worden geactiveerd door de ICT-coördinator. De invalkracht heeft dan direct toegang (en hoeft geen dag meer te wachten).	2	3	6	Proces (school)
5	O	Het risico is dat er onrechtmatig toegang is tot	De uitgegeven sleutels en wachtwoorden van de thuisgebruik accounts	2	2	4	Proces (school)

		persoonsgegevens en / of leervoortgang bij het gebruik van thuisaccounts.	worden niet periodiek door de leerkracht gewijzigd.				
6	O	Het risico is dat er onrechtmatig toegang is tot persoonsgegevens en / of leerresultaten omdat wachtwoorden niet veilig genoeg zijn.	Periodiek wijzigen wachtwoord bij medewerkers wordt niet afgedwongen en ook niet periodiek aangegeven door de ICT-coördinator.	2	2	4	Proces (school)
7	O	Het risico is dat er onrechtmatig toegang is tot persoonsgegevens en / of leerresultaten omdat medewerkers onterecht beschikken over de beheer rol.	De ICT-coördinator heeft brede bevoegdheden. Indien er geen strikt autorisatiebeheer zit op de rol van ICT-coördinator in Basispoort kan het zijn dat er teveel medewerkers niet noodzakelijke toegang hebben tot persoonsgegeven en / of leerresultaten.	2	3	6	Proces (school)
8	O	Het risico is dat (oud) medewerkers onrechtmatig toegang tot gegevens houden, als het proces bij uitdienst en rolverandering niet goed doorgevoerd wordt in het leerlingadministratiesysteem en in Basispoort.	Scholen moeten in- en uitdienst procedures goed opzetten en daarin ook de handmatig aangemaakte accounts in Basispoort in meenemen.	3	3	9	Proces (school)

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.

20. Maatregelen

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

Maatregelentabel:

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (Basispoort /school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum)maatregel geïmplementeerd?
1	Geen up-to-date verwerkersovereenkomst	4	Onderwijsinstelling moet de nieuwe verwerkersovereenkomst accepteren.	School	2		
2	Toegang door onbevoegde koppelpartners	4	Volg de instructies uit de CHECKLIST PROBLEEMLOZE OVERGANG NAAR SCHOOLJAAR en controleer minimaal één keer per jaar alle koppelingen.	School	2		
3	Geen MFA	9	1. Basispoort zal MFA voor beheerders default instellen en zal overwegen dit ook voor andere medewerkers te laten gelden. 2. Onderwijsinstelling moet gebruik van MFA (voor beheerders) verplichten.	Basispoort en school	3		Basispoort zal MFA by default voor beheerders in het schooljaar 2024-2025 hebben gerealiseerd.
4	Geen persoonlijk account invalkracht	6	Onderwijsinstelling moet gebruik maken van invalkracht account van Basispoort.	School	2		
5	Onrechtmatige toegang door thuisaccounts	4	Vraag periodiek aan leerkrachten om langdurig gebruikte of niet meer gebruikte login gegevens voor thuis te wijzigen.	School	2		

6	Onrechtmatige toegang door onveilige wachtwoorden	4	Volg de instructies uit de CHECKLIST PROBLEEMLOZE OVERGANG NAAR SCHOOLJAAR en vraag periodiek wachtwoorden te wijzigen.	School	2		
7	Onrechtmatige toegang door ontoereikend autorisatiebeheer	6	School moet goed autorisatiebeheer op Basispoort inrichten en toepassen.	School	3		
8	Onrechtmatige toegang door geen goed proces bij in- en uit dienst	9	Volg de instructies uit de CHECKLIST PROBLEEMLOZE OVERGANG NAAR SCHOOLJAAR en verwijder medewerkers bij uitdiensttreding (ook handmatig In Basispoort aangemaakte accounts).	School	2		

7. Deel E: MODEL lokale DPIA

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

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

A. Uitvoering lokale DPIA

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

Bij de beoordeling in deze lokale DPIA zijn betrokken:

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

B. Overwegingen over centrale DPIA

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

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

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

C. Organisatiespecifieke- en algemene applicatierisico's

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

12	Het bestuur heeft op elke schoolwebsite een pagina, dan wel een link naar de juiste pagina, over de wijze waarop de ouders (of leerlingen > 16 jaar) hun rechten kunnen uitoefenen (Privacyreglement).		

Risicotabel 2. Algemene applicatie specifieke 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. Zie ook onder risico's.		
2	De verwerking is opgenomen in het register van verwerkingen.		
3	Het bestuur zal de DPIA van Basispoort minimaal eens per drie jaar herbeoordelen.		
4	Er zijn duidelijke afspraken over de invoer bij open velden. Dit kan bijvoorbeeld aan de hand van vastgesteld beleid of protocollen zijn geïmplementeerd. Hierin is vastgesteld of het gebruik van vrije invulvelden noodzakelijk is en zo ja voor welke informatie. Over deze uitgangspunten is duidelijk gecommuniceerd met alle medewerkers die gebruik maken van de applicatie.		
5	Het bestuur houdt rekening met dataminimalisatie voor verwerken van persoonsgegevens in de applicatie.		
6	Het bestuur hanteert de wettelijke bewaartermijnen. De bewaartermijnen zijn vastgesteld en beschreven.		
7	Het bestuur zorgt ervoor dat persoonsgegevens na afloop van de bewaartermijn daadwerkelijk worden geschoond en heeft een procedure voor.		
8	Het bestuur voldoet aan het transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de		

	privacyverklaring over de (optionele) toepassing van Basispoort.		
9	Het bestuur heeft autorisaties ingericht op basis van 'need to know' (role based access). Zie ook onder risico's.		
10	Afstemming met betrokkenen. Het bestuur heeft bij het uitvoeren van de lokale DPIA de betrokkenen om hun mening gevraagd over de verwerking en deze meegenomen in de DPIA (artikel 35 lid 9 AVG). Dit kan bijvoorbeeld via de medezeggenschapsraad.		
11	Gebruikers van de applicatie zijn/worden afdoende getraind in het gebruik ervan.		
12	Persoonsgegevens worden niet op verkeerde plekken opgeslagen omdat regels en/of bekendheid met Basispoort dit voorkomt. Er is daarom geen sprake van een schaduwadministratie op verschillende schijven en mappen van medewerkers.		
13	Er is een functioneel beheerder aangewezen voor Basispoort en dit is tevens gedocumenteerd.		
14	De onderwijsinstelling neemt verantwoordelijkheid voor het veilig koppelen van het Basispoort met een ander systeem zoals een leerlingadministratiesysteem.		

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

Risico	Te nemen maatregel	Uitgevoerd?	Opmerking/toelichting
Het risico is dat er gegevens beschikbaar worden gesteld aan onbevoegde koppelpartners.	Volg de instructies uit de CHECKLIST PROBLEEMLOZE OVERGANG NAAR SCHOOLJAAR en controleer minimaal één keer per jaar alle koppelingen.		
Het risico is dat er bij accounts (met veel rechten) onregelmatigheden plaatsvinden doordat de toegang tot de applicatie onvoldoende is beveiligd.	Onderwijsinstelling moet gebruik van MFA (voor beheerders) verplichten.		
Het risico is dat er onrechtmatig toegang is tot persoonsgegevens en / of leerresultaten omdat de school een niet persoonlijk account gebruikt voor een invalkracht i.p.v. de veilige door Basispoort aangeboden oplossing.	Onderwijsinstelling moet gebruik maken van invalkracht account van Basispoort.		
Het risico is dat er onrechtmatig toegang is tot persoonsgegevens en / of leerresultaten bij het gebruik van thuisaccounts.	Vraag periodiek aan leerkrachten om langdurig gebruikte of niet meer gebruikte login gegevens voor thuis te wijzigen.		
Het risico is dat er onrechtmatig toegang is tot persoonsgegevens en / of leerresultaten omdat wachtwoorden niet veilig genoeg zijn.	Volg de instructies uit de CHECKLIST PROBLEEMLOZE OVERGANG NAAR SCHOOLJAAR en vraag periodiek wachtwoorden te wijzigen.		

[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 RESTRISICO	**kans**		**impact**		**RESTRISICO**	
	NB: het restrisico betreft het risico indien de maatregel wel wordt uitgevoerd. Zonder maatregel resteert het oorspronkelijke risico.					

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

D. 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 […].

E. 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.

F. 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.

G. Risico-mitigerende maatregelen schoolbestuur

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

Het schoolbestuur moet daarom zorgen voor:

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

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

H. Aanbevelingen

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

A. …

B. …

I. 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 [SYSTEEM] [WEL/NIET] TE [GEBRUIKEN/CONTINUEREN].

Naam bestuurder(s):

Plaats:

Datum:

Ondertekening: