CENTRALE DPIA

Versie 1.2 (juni 2023)

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) Ferdy IJsselmuiden (DPIA-projectmanager) Pascal Marcelis (adviseur IBP) Marcel de Rijke (ISO) Hans-Peter Ligthart (portfoliomanager IBP) Rynk van der Togt (Lucas Onderwijs) I.Berger (Viviani onderwijs) R. Lubbers (Viviani onderwijs)
Met dank aan	Klaas Waslander (Snappet) Meindert Boon (Snappet)
Auteurs model DPIA (v.1.2)	Hans-Peter Ligthart (portfoliomanager IBP) Job Vos (jurist en adviseur IBP) Ferdy IJsselmuiden (DPIA-projectmanager)

Versie beheer

Datum	Versie	Wijziging
Oktober 2023 t/m april 2024	1.0	Centrale DPIA Snappet

Inhoudsopgave

1. Samenvatting

Snappet is een online lesplatform dat toegang geeft tot complete lesmethoden voor rekenen, taal en spelling. Snappet wordt gebruikt in het basisonderwijs en is actief in meerdere landen. Met de applicatie van Snappet, beschikbaar op apparaten zoals laptops en tablets, kunnen leerlingen toegang krijgen tot Snappet waaronder de leerstof en verwerkingsopgaven. Leerkrachten kunnen in het Snappet-platform de leerinhoud bepalen en de leerresultaten zien. Snappet is een zogenaamd adaptieve leermethode. De lesstof is afgestemd op de individuele behoefte, het tempo en de mogelijkheden van de leerling.

Uitvoering van de DPIA

In een periode van een half jaar is de DPIA door SIVON uitgevoerd. Dit met de enthousiaste medewerking van een aantal onderwijsinstellingen en ook Snappet heeft op een constructieve en plezierige manier meegewerkt aan het uitvoeren van de DPIA. Snappet heeft op een transparante wijze inzicht gegeven in de gegevensverwerkingen en de daarmee verbonden risico's voor de betrokkenen. Snappet heeft aangegeven een aantal verbeteringen te zullen doorvoeren, die het met name voor de onderwijsinstelling eenvoudiger maken om haar rol als verwerkingsverantwoordelijke goed uit te kunnen oefenen.

Conclusie

Snappet is een online lesplatform dat inmiddels ruim 10 jaar bestaat. Uit de DPIA is naar voren gekomen dat gedurende deze periode de onderwerpen privacy en informatiebeveiliging veel aandacht krijgen en hebben gekregen. Met inachtneming van onderstaande, door zowel Snappet als de onderwijsinstelling uit te voeren acties, kan er op een veilige manier gebruik worden gemaakt van Snappet.

Op het gebied van informatiebeveiliging zijn er in de DPIA geen grote risico's aangetroffen die (direct) nadere actie behoeven. Snappet heeft wel aangegeven dat zij – onder andere omwille van de aantoonbaarheid - een traject zal starten wat tegen de zomer van 2025 zal moeten leiden tot een ISO 27001 certificaat[1].

De door Snappet gebruikte verwerkersovereenkomst wijkt op een aantal onderdelen af van de standaard van het Privacyconvenant. Snappet heeft aangegeven dat zij voor de zomer van 2024 een nieuwe versie zal gaan gebruiken die in lijn zal zijn met de standaard. Dit zal de duidelijkheid ten goede komen en helpt de onderwijsinstellingen om heldere afspraken te maken met de verwerker van haar persoonsgegevens.

Voor wat betreft de overige aangetroffen risico's is er een aantal zaken dat door Snappet zal worden opgelost, waarmee onderwijsinstellingen deze risico’s beter kunnen beheersen. Dit betreft:

[1] https://nl.wikipedia.org/wiki/ISO/IEC_27001

- Het risico beperken op verlies van data als gevolg van ongecontroleerde exports of downloads: er komt een nieuwe optie om te kunnen zien welke exports er door wie zijn gemaakt vanuit het Snappet dashboard;
- Het risico beperken dat gegevens onbevoegd worden ingezien of gewijzigd: de huidige werkwijze wordt vereenvoudigd door directer inzicht in logs (zonder tussenkomst helpdesk);
- Het risico dat gegevens langer worden bewaard dan noodzakelijk is: de huidige werkwijze wordt vereenvoudigd door bewaartermijnen in te kunnen stellen (zonder tussenkomst helpdesk).

Om deze risico's te beheersen zal overigens ook de onderwijsinstelling zelf een aantal maatregelen moeten treffen. Daarnaast is er 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 dat dataverkeer onvoldoende veilig is omdat onderwijsinstellingen gebruik maken van verouderde devices die niet de gangbare protocollen ondersteunen;
- Het risico dat er bij accounts (met veel rechten) onregelmatigheden plaatsvinden doordat geen gebruik wordt gemaakt van MFA;
- Het risico dat onderwijsinstellingen de werking van Snappet en het algoritme / adaptiviteit niet transparant maken, waardoor betrokkenen hun recht op informatie niet kunnen uitoefenen;
- Het risico dat de leerkracht een beoordeling of een besluit enkel op één leermiddel op beperkte informatie baseert zonder voldoende zicht op de algemene prestaties van een leerling.

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 n 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[2]. 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.

De verplichting om een DPIA uit te voeren doet zich voor in het geval van een digitaal leermiddel zoals Snappet waarbij de verwerking wordt aangemerkt als profilering, alsook bij grootschalige verwerking van bijzondere persoonsgegevens volgens artikel 35(3)(b) van de AVG en het Besluit DPIA. Bij het onderzoek naar Snappet is het uitvoeren van een DPIA verplicht omdat er volgens het overzicht van de European Data Protection Board[3] aan twee criteria wordt voldaan. Hierdoor spreken we van een 'hoog risicoverwerking'.

Er is namelijk sprake van een verwerking van 'gevoelige gegevens' die kunnen leiden tot 'evaluatie of scoretoekenning', omdat er binnen Snappet leer- en testresultaten worden verwerkt en zichtbaar zijn voor gebruikers (leerkrachten). Daarnaast heeft deze verwerking van persoonsgegevens betrekking op kinderen onder de 16 jaar. Deze vorm van gegevensverwerking vereist een extra bescherming omdat het hier kwetsbare personen betreft. Daarom zijn er twee criteria van de WP29-lijst waaraan voldaan wordt, op basis waarvan de verwerkingsverantwoordelijke verplicht is een DPIA uit te voeren bij het gebruik van deze applicatie.

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

[3] De 'WP29 werkgroep' (vanaf mei 2018: European Data Protection Board – EDPB): zie de WP29-richtlijn voor DPIA's (WP 248 rev.01 zoals vastgesteld op 4 april 2017, en laatstelijk gewijzigd op 4 oktober 2017).

Volgens de lijst van de Autoriteit Persoonsgegevens[4] is er sprake van '15. Profilering'. Dit gaat om een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op automatische verwerking, zoals bijvoorbeeld prestaties van leerlingen. Ook het voldoen aan dit criterium stelt het uitvoeren van een DPIA verplicht.

III. Toetsing rolverdeling verwerkingsverantwoordelijke en verwerker

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

In alle gevallen is het uitgangspunt dat de leverancier verwerker is en dat verwerking van persoonsgegevens beperkt is tot legitieme doeleinden. Een leverancier kan ook persoonsgegevens verwerken als verwerkingsverantwoordelijke. Denk hierbij aan de 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] Zie Staatscourant 2019, nummer 64418 van 27 november 2019.

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[5], aangevuld met onderwijs-specifieke informatie uit de *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*[6]. 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

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

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:

1. Het Snappet-platform en het hierbij horende dashboard waarmee onder andere leerresultaten kunnen worden ingezien en per leerling de leerinhoud kan worden bepaald;
2. De Snappet-applicatie. Dit is de applicatie op een device waarmee leerstof, verwerkingsopgaven en andere educatieve componenten kunnen worden benaderd.

VII. Buiten scope

Buiten de scope van de DPIA zijn:

- De devices van Snappet en aanverwante hardware en/of producten (die dienen om de devices te laten functioneren).
- De uitwisseling van leer- en testresultaten met leerling administratiesystemen van de Onderwijsinstelling;
- De uitwisseling van leer- en testresultaten met dashboards (B.I) die de onderwijsinstelling in gebruik heeft;
- Het door de Onderwijsinstelling beschikbaar stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek.

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

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 (inclusief uitoefenen recht op inzage etc.);
- Beoordeling van de default settings (privacy by design);
- Analyse van de wijze waarop het systeem voorziet in logging en de wijze waarop dit door de onderwijsinstelling gemonitord kan worden;
- Opstellen rapportage;
- Overleg met leverancier over (aanvullende) maatregelen.

De centrale DPIA is uitgevoerd in de periode juli 2023 tot en met maart 2024 door het in de colofon genoemde DPIA Team. Tijdens het uitvoeren van de DPIA heeft een analyse van de tussentijdse resultaten van de DPIA met de leverancier plaatsgevonden en zijn er nadere vragen gesteld aan de leverancier. Op basis van de verkregen antwoorden is invulling gegeven aan dit DPIA-rapport.

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

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

Bijzondere persoonsgegevens mogen alleen verwerkt worden als je een beroep kunt doen op een uitzondering. Voor het onderwijs geldt bijvoorbeeld dat gezondheidsgegevens alleen gebruikt mogen worden als dat noodzakelijk is voor het geven van onderwijs en het begeleiden van een leerling. Ze zijn bijzonder omdat het gebruik van deze gegevens iemands

privacy ernstig kan beïnvloeden. Voorbeelden zijn gezondheidsgegevens, levensovertuiging, lidmaatschap van de vakbond, ras of etnische afkomst.

Diagnostische gegevens zijn gegevens over het individuele gebruik van de diensten. Bijvoorbeeld: hoe vaak je inlogt, welk soort documenten je opslaat, leest etc.. Deze gegevens komen in logbestanden terecht van de clouddienst. [Deze data wordt ook soms servicegegevens genoemd.]

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

Gevoelige persoonsgegevens gaan over gegevens die volgens de Autoriteit Persoonsgegevens (AP) snel inbreuk (kunnen) maken op de persoonlijke levenssfeer. Het gaat bijvoorbeeld om leerresultaten van kinderen, omdat daar conclusies aan kunnen worden verbonden met gevolgen voor het latere maatschappelijke leven. Of het gaat om grote verzamelingen van informatie van (zeer) jonge kinderen, gegevens over (problematische) gezinssituatie of[7] 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’

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

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

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

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

Pseudonieme persoonsgegevens Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eisen verbonden dat de sleutels apart worden bewaard en dat maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.
Of pseudonieme gegevens door de ontvanger (verwerker) als persoonsgegevens aangemerkt moeten worden hangt af van de omstandigheden van het geval. Het uitvoeren van een toets zal kunnen uitwijzen in hoeverre deze door de leverancier te herleiden zijn tot persoonsgegevens[8].

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

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

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.

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

Snappet is een digitale aanbieder van lesmethoden waar schoolbesturen gebruik van kunnen maken bij het onderwijzen van hun leerlingen. Leerlingen kunnen hun opdrachten online maken of in werkboeken. Scholen kunnen zelf kiezen voor welke onderdelen van de les- en oefenstof online of werkboek effectiever of beter passend is binnen het curriculum dat de school hanteert. Met Snappet kun je, al dan niet aan de hand van de adaptieve leermethoden, leerprestaties van leerlingen vaststellen waarbij de docent door middel van het dashboard inzicht verkrijgt in de leerresultaten van de individuele leerlingen van zijn groep. Hierbij wordt gebruik gemaakt van een grote hoeveelheid opgaven per leerdoel waarbij het niveau van de leerling per leerdoel wordt bepaald.

2. Persoonsgegevens

In dit onderdeel wordt beschreven welke categorieën persoonsgegevens van welke betrokkenen worden verwerkt binnen Snappet. Zie ook de definitiebepalingen onder IX.

In Snappet worden persoonsgegevens verwerkt van leerlingen in de basisschool leeftijd (<13jr.) en van medewerkers van de onderwijsinstelling.

De volgende categorieën persoonsgegevens en betrokkenen worden in Snappet verwerkt.

Persoonsgegevens	Medewerker	Stagiair / LIO	Vrijwilligers	Externen	Sollicitant	Minder-jarigen
Algemene contact-gegevens	X					X
Feiten en waarderingen over iemand zijn gedragingen, eigenschappen of opmerkingen						
Overige contact-gegevens						
Personeelsnummer						
Nationaliteit en geboorteplaats						
Gezondheidsgegevens (op eigen verzoek t.b.v. beheersmaatregel)						

Godsdienst (op eigen verzoek t.b.v. beheersmaatregel)						
Gesprekscyclus (documenten)						
Ervaringen (werkervaring en opleidingen)						
Gegevens met betrekking tot financiën						
Beeldmateriaal						
Verzuimregistratie						
BSN						
Overige gegevens: Diagnostische gegevens Logging gegevens	X					X
Overige gegevens: (Leer)resultaten en niveaubepaling						X

Overzicht tabel

De hiervoor genoemde informatie wordt verder uitgewerkt in de volgende tabel:

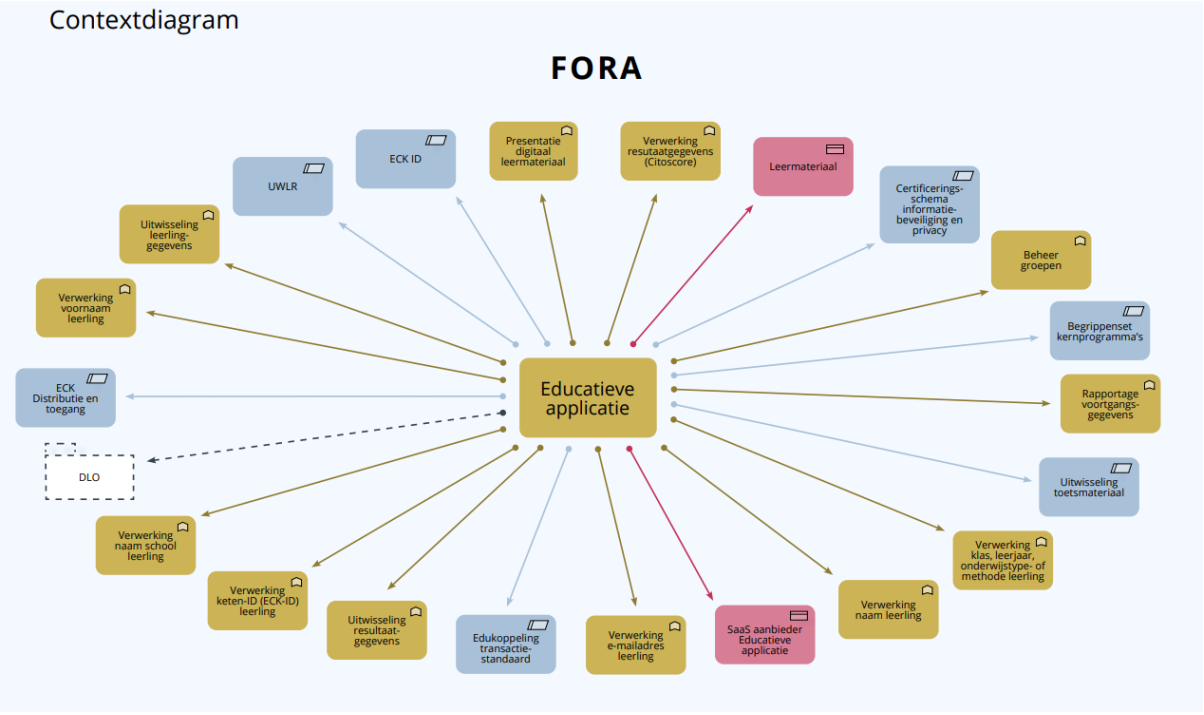
Categorie betrokkene	Categorie persoonsgegevens	Persoonsgegeven	Bron/verkrijging persoonsgegeven
Minderjarigen (leerlingen)	Algemene contact-gegevens	– voornaam – achternaam, – tussenvoegsel – e-mail adres (school)	School
Minderjarigen (leerlingen)	Overige contact-gegevens	- pupil ID - klas / leerjaar - ILT code	Snappet School
Minderjarigen (leerlingen)	Overige gegevens	- studievoortgang of studietraject - diagnostische gegevens - loggegevens - metadata - IP-adres - correspondentie gegevens - gepseudonimiseerde gegevens	Leerling Snappet
Medewerker	Algemene contact-gegevens	– voornaam – achternaam, – tussenvoegsel	School

		– e-mail adres (school)	
Medewerker	Overige contact-gegevens	- zakelijk adres	School
Medewerker	Overige gegevens	- diagnostische gegevens - loggegevens - metadata - IP-adres - correspondentie gegevens	Snappet Medewerker

3. Gegevensverwerkingen

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

Voor het schetsen van de scope van de gegevensverwerkingsanalyse wordt gebruik gemaakt van de referentiearchitectuur. Snappet kan in termen van FORA[9] worden geduid als 'Educatieve applicatie'.



Voor de opsomming van de verwerkingen die binnen Snappet plaatsvinden is aansluiting gezocht bij de verwerkersovereenkomst van Snappet en de FORA.

In de verwerkersovereenkomst staan de verwerkingen opgesomd. Deze staat ook aan de basis van de scope bepaling van deze DPIA, zie onderdeel 2. VI van deze DPIA. Raadpleging van de FORA (zie hierboven weergegeven afbeelding 'Contextdiagram') heeft geen aanleiding gegeven tot het verder uitbreiden van de scope.

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

Standaard verwerkingen

Verwerking van Persoonsgegevens met behulp van Snappet vindt plaats ten behoeve van het verzorgen van onderwijs, waaronder het voorbereiden, uitvoeren, evalueren en ondersteunen van het onderwijs(proces), het begeleiden en volgen van Onderwijsdeelnemers (in hun leerproces) en het zorgen voor een veilige leeromgeving.

Deze aan FORA ontleende processen behelzen de volgende feitelijke gegevensverwerkingen:

1. Het verwerken van persoonsgegevens waaronder de leerresultaten van individuele leerlingen (betrokkene) voor de leerling zelf.
2. Het via het dashboard beschikbaar stellen van de persoonsgegevens, waaronder de leerresultaten, aan de leerkrachten van de individuele leerlingen.
3. Het maken van een back-up.

Optionele verwerkingen

Bij het gebruik van Snappet kunnen met specifieke toestemming van de Onderwijsinstelling, ter verdieping en ondersteuning aan voornoemde verwerkingen, ook optionele verwerkingen plaatsvinden. Deze optionele verwerkingen vinden plaats voor inzicht en bijsturing door de Onderwijsinstelling en/of leerkracht op individueel plus en groepsniveau.

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

Als een bevoegd iemand binnen de onderwijsinstelling een opt-in geeft voor optionele dataverwerkingen, dan mag Snappet in de rol van verwerker de data van de leerlingen gebruiken om anonieme statistische datasets af te leiden ten behoeve van de volgende 3 doeleinden:

1. Het maken en zelfstandig gebruiken van overzichten van, door leerlingen behaalde, resultaten per opgave, bijvoorbeeld om de moeilijkheid van die opgaven nauwkeurig te bepalen. Niet direct identificerende overzichten met resultaten per opgave worden door de Onderwijsinstellingen, op basis van de Verwerkersovereenkomst, ter beschikking gesteld aan Snappet voor beperkt zelfstandig gebruik.
2. Het maken van niet direct identificerende overzichten met betrekking tot vaardigheden, bijvoorbeeld om op verschillende momenten het vaardigheidsniveau van een leerling of een groep leerlingen te classificeren naar een percentielscore. Niet direct identificerende overzichten met percentielscores worden door de Onderwijsinstellingen ter beschikking gesteld aan Snappet voor beperkt zelfstandig gebruik.
3. Het maken van identificerende overzichten voor Onderwijsinstelling en/of leerkracht op basis van actuele vaardigheden van individuele leerlingen, die gecombineerd worden met data, die wordt afgeleid uit anonieme historische bestanden van leerplannen, leerdoelen en actuele resultaten. Deze identificerende overzichten

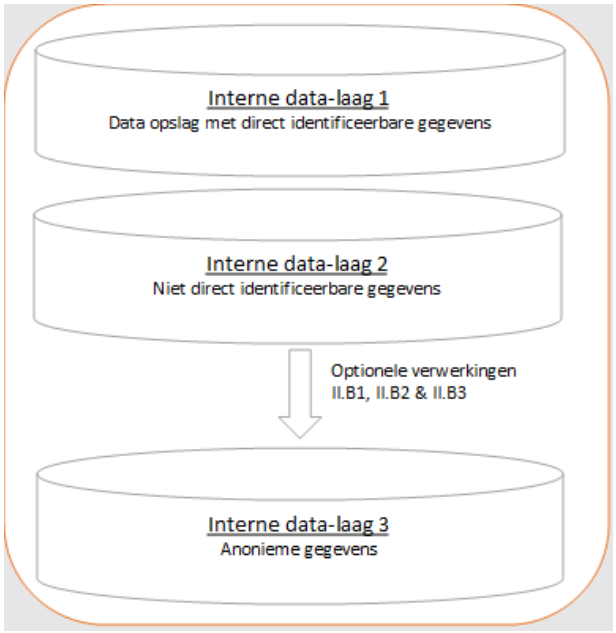
worden door de Onderwijsinstelling en/of leerkracht gebruikt bij het bijsturen van de resultaten van de individuele leerlingen en/of het bijstellen van leerplannen en/of leerdoelen. Tevens is het mogelijk dat de Onderwijsinstelling en/of leerkracht de inhoud en de aard van leermiddelen kan personaliseren. Een anonieme versie van het historische bestand van leerplannen, leerdoelen en resultaten worden door de onderwijsinstelling ter beschikking gesteld aan Snappet voor beperkt zelfstandig gebruik.

Daarnaast kunnen er na voorafgaande additionele opdracht van de Onderwijsinstelling gegevens worden verwerkt t.b.v. (i) het adviseren door consulenten van Snappet met betrekking tot het verbeteren van leerprestaties van leerlingen en/of (ii) het vaststellen van een curriculum en/of (iii) het beschikbaar stellen, na instructie van de Onderwijsinstelling, van een set (persoons)gegevens aan onderzoeksinstellingen.

Overzicht data stromen binnen Snappet

De bovenstaande standaard en optionele verwerkingen vinden binnen Snappet plaats binnen drie lagen teneinde zo goed mogelijk de privacy van betrokkenen te waarborgen. Door deze gelaagdheid kan Snappet privacy risico's beter beperken: door zoveel mogelijk laag 2 en 3 te gebruiken, worden gegevens in laag 2 minder gemakkelijk herleidbaar en in laag 3 niet herleidbaar naar individuele personen.

In de onderstaande cilo-afbeelding wordt weergegeven hoe de data zich tussen drie lagen beweegt, welke verwerking er in welke laag plaatsvindt en of data t.b.v. die verwerking wordt gepseudonimiseerd of geanonimiseerd.



In het Snappet-platform zijn de gegevens aldus onderverdeeld in drie gegevenslagen.

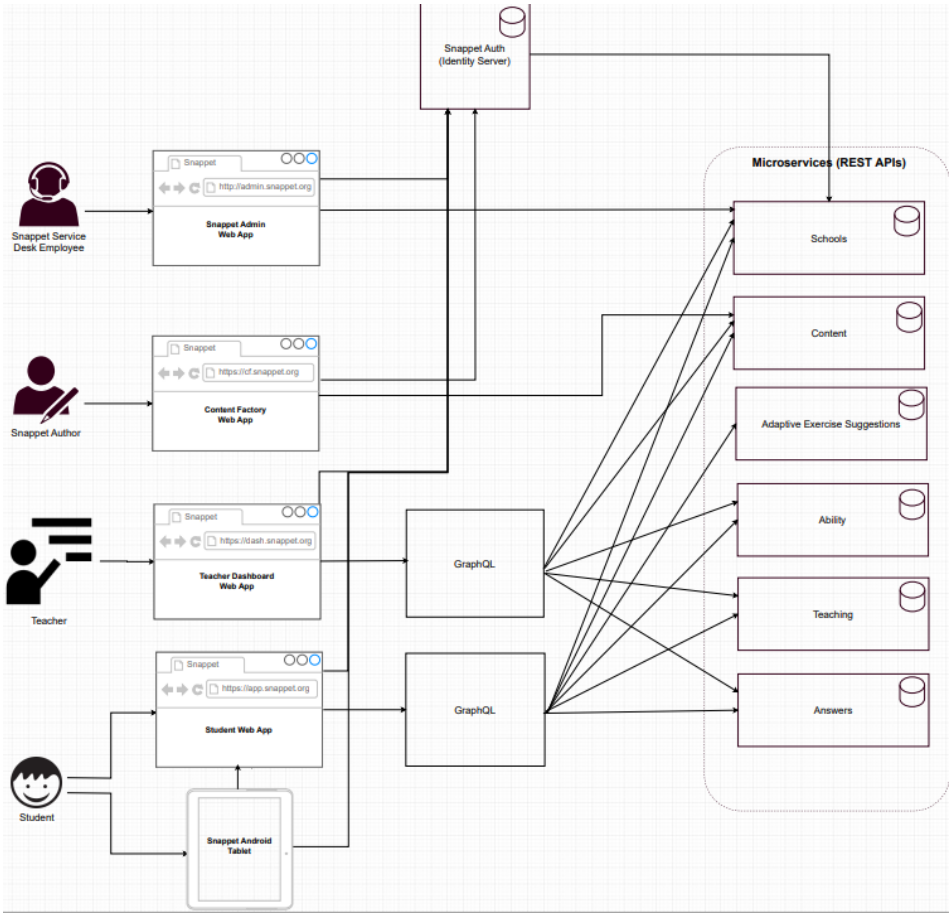
Laag 1 - direct identificeerbare gegevensopslag: bevat persoonlijk identificeerbare informatie (zoals namen, e-mailadressen, interne ID's).

Laag 2 - niet direct identificeerbare gegevensopslag: (zoals antwoorden van leerlingen): de opgeslagen gegevens zijn gepseudonimiseerd en kunnen alleen worden geïdentificeerd door het interne ID te combineren met de gegevensopslag van laag 1.

Laag 3 - anonieme gegevensopslag: de gegevens kunnen niet meer worden herleid naar een persoon (zoals de percentielgrenzen van de vaardigheden van leerlingen in de loop van de tijd). Snappet slaat geen ID's of individuele gegevensreeksen (zoals antwoorden) op. De anonieme dataset als uitkomst van de berekeningen met behulp van laag 2-gegevens worden getransporteerd naar laag 3.

Architectuur

Onderstaand schema geeft op hoog niveau de architectuur weer van Snappet.



Koppelingen

Het Snappet Platform heeft standaard de volgende koppelingen:

- Met Readspeaker: voorlezen van content, student web app roept ReadSpeaker endpoint aan, alleen opgaven dus geen persoonlijke data.
- Met New Relic en Raygun: op server/infrastructuur niveau verzamelt deze infrastructuur informatie waaronder browser informatie en IP adressen t.b.v. security monitoring.

- Met Sendgrid: e-mails worden door het Snappet platform aan leerkrachten/scholen via beveiligde koppeling via Sendgrid verstuurd. Denk aan welcome email nieuwe leerkracht, signup/reset password, invoices etc.

Het Snappet Platform heeft de volgende door de Onderwijsinstelling zelf te activeren koppelingen:

- Met ParnasSys of ESIS voor de uitwisseling van groepen/gebruikers en examenresultaten activeren. Dit loopt via de school service en de uitwisseling vindt plaats via beveiligde verbindingen met een unieke autorisatiesleutel per school. Deze koppeling is niet standaard actief.

4. Verwerkingsdoeleinden

De verwerkingsdoeleinden ten behoeve waarvan de gegevensverwerkingen binnen Snappet plaatsvinden sluiten aan bij de in het Privacyconvenant[10] opgenomen verwerkingsdoeleinden.

De verwerkingsdoeleinden zijn schematisch weergegeven en gekoppeld aan de verwerking.

Gegevensverwerking (par.3 Gegevensverwerkingen)	Doeleinde verwerking (par.4. Verwerkingsdoeleinden)	Toelichting
Onderwijsevaluatie	De opslag van leer- en toetsresultaten.	Resultatenregistratie Beoordeling
Onderwijsevaluatie	Het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten.	Resultatenregistratie
Leerlingbegeleiding	De beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer.	Monitoring en begeleiding voortgang leerroute en leerproces Onderwijsbegeleiding Voortgang- en resultatenweergave
Leerlingbegeleiding	Analyse en interpretatie van leer- en toetsresultaten.	Monitoring en begeleiding voortgang leerroute en leerproces
Onderwijsevaluatie Leerlingbegeleiding	Het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen.	Resultatenregistratie Monitoring en begeleiding voortgang leerroute en leerproces
Onderwijsuitvoering	Het begeleiden en ondersteunen van leerkrachten/docenten en andere medewerkers binnen de Onderwijsinstelling.	
Onderwijsuitvoering	De communicatie met Onderwijsdeelnemers en ouders en met medewerkers van de Onderwijsinstelling.	
Onderwijsuitvoering	Monitoring en verantwoording, met name ten behoeve van: (prestatie)metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs(vormen) of de geboden	

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

	ondersteuning van Onderwijsdeelnemers bij passend onderwijs.	
Onderwijsuitvoering	Het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier.	Inkoop Beheer ict-middelen (Toegang tot) aanbod leermateriaal
Onderwijsuitvoering	Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie.	(Toegang tot) aanbod leermateriaal Beheer identiteiten Authenticatie en autorisatie
Informatiebeveiliging en privacy	De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens.	
Onderwijsuitvoering	De continuïteit, verbetering en goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning.	Beheer ict-middelen (Contractbeheer)
Onderwijsuitvoering	Het door de Onderwijsinstelling beschikbaar kunnen stellen van (geanonimiseerde of gepseudonimiseerde) Persoonsgegevens voor wetenschappelijk onderzoek of statistische doeleinden ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling, dat wordt uitgevoerd op basis van strikte voorwaarden vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek.	Opleidingontwikkeling Materiaalontwikkeling
Onderwijsuitvoering	Het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.	Inschrijving en leerlinggegevensbeheer
Onderwijsuitvoering	Het behandelen van geschillen.	Registratie klachten en bezwaren Klachtbehandeling
Onderwijsevaluatie	Onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling.	
Onderwijsuitvoering – en evaluatie	Vaststellen van leerplannen en leerdoelen, vakken naar behoefte toe voegen en personaliseren van de inhoud en de aard van de leermiddelen door de Onderwijsinstellingen en/of leerkracht of op verzoek van de Onderwijsinstelling en/of Leerkracht door Snappet.	

5. Betrokken partijen

De hieronder genoemde organisaties zijn betrokken bij de gegevensverwerkingen.

Naam partij	AVG-rol	Functie/taak	Betrokken persoons-gegevens	Verstrekker of ontvanger	De volgende personen/ rollen hebben toegang deze pgg
Onderwijs-instelling	Verwerkings-verantwoordelijke	Beheer en toepassing van het digitaal leermateriaal	Alle genoemde persoonsgegevens	Verstrekker	Beheerder, leerkrachten, ICT-er, leerlingen
Snappet	Verwerker	Aanbieder digitaal leermateriaal	Alle genoemde persoonsgegevens	Ontvanger	Beheerder, Support medewerkers, Trainers
Amazon Web Services EMEA SARL (Luxemburg, Luxemburg)	Subverwerker	Hosting vragen, antwoorden, resultaten en basisgegevens van de leerlingen en leerkrachten	Contactgegevens, Studievoortgang, Gebruikersgegevens, Overige gegevens	Ontvanger	Overeenkomstig de subverwerkersovereenkomst
New Relic Inc, (VS, EER)	Subverwerker	Hosting security controls (monitoring)	Gebruikersgegevens	Ontvanger	Overeenkomstig de subverwerkersovereenkomst
Raygun limited (Nieuw Zeeland - Wellington, VS – Northern Virginia)	Subverwerker	Hosting security controls (monitoring)	Gebruikersgegevens	Ontvanger	Overeenkomstig de subverwerkers-overeenkomst
Sendgrid Inc. (VS, Denver)	Subverwerker	E-mail functionaliteiten	Contactgegevens, Gebruikersgegevens, Overige gegevens – correspondentiegegevens	Ontvanger	Overeenkomstig de subverwerker-sovereenkomst
Zendesk Inc (VS, San Francisco)	Subverwerker	Support functie	Contactgegevens, Gebruikersgegevens, Overige gegevens – correspondentiegegevens	Ontvanger	Overeenkomstig de subverwerkers-overeenkomst

6. Belangen bij de gegevensverwerking

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

De belangen die Snappet en haar subverwerkers hebben, is het leveren van een goed werkende digitale omgeving waarin de leermiddelen en toetsen kunnen worden aangeboden, waarbij tevens een adaptieve functionaliteit wordt verstrekt.

De belangen van de geïdentificeerde subverwerkers zijn alle ondersteunend aan het hierboven genoemde hoofddoel: een goed werkende digitale leer-en toetsapplicatie.

7. Verwerkingslocaties

De gegevensverwerking vindt plaats in de volgende landen.

Partijnaam	Statutaire vestigings-plaats (sub-) verwerker	Beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt verwerkt door deze (sub)verwerker	Plaats/land van opslag en verwerking persoonsgegevens en doorgifte mechanisme indien buiten de EER
Snappet AWS EMEA SARL	Utrecht Luxemburg, Luxemburg	Platform en applicatie	AVG / DPF
New Relic Inc Raygun limited	VS – San Francisco VS – Nothern Virginia Nieuw Zeeland - Wellington	Security controls (hosting)	VS - DPF en SCC overeenkomst, geen gevoelige persoonsgegevens (Leerresultaten) Nieuw Zeeland - adequaatheidsbesluit
Sendgrid Inc.	VS, Denver	E-mail functionaliteiten	VS - DPF (Twilio) en SCC overeenkomst.
Zendesk Inc	VS, San Francisco	Support functie	VS - DPF en BCR goedgekeurd door de Nederlandse en Engelse Autoriteit + een SCC overeenkomst

8. Passend beschermingsniveau

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.

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

Snappet verwerkt de persoonsgegevens en leerresultaten in Europese datacenters van AWS Europe gevestigd te Luxemburg (een dochteronderneming van het Amerikaanse Amazon). Buiten Europa worden persoonsgegevens verwerkt t.b.v. security controls (gepseudonimiseerd), e-mails en supportverzoeken.

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.

Amazon Webservices, New Relic, Sendgrid en Zendesk zijn aangesloten bij het nieuwe DPF. Zie: https://www.dataprivacyframework.gov/s/participant-search.

Raygun is een bedrijf dat is gevestigd in Nieuw-Zeeland. Voor Nieuw-Zeeland is er ook een adequaatheidsbesluit.

Als extra waarborg om te voorkomen dat de Amerikaanse overheid toch toegang zou krijgen tot de persoonsgegevens die Snappet verwerkt bij AWS in Luxemburg heeft Snappet de volgende maatregelen getroffen:

- Data-at-rest wordt *altijd* encrypted als het persoonlijke details bevat (zoals naam of e-mailadres), of als het betrokken is bij data uitwisseling met externe systemen;
- Snappet gebruikt geen AWS Owned keys, maar AWS Managed keys die binnen de eigen hosting omgeving secure opgeslagen zijn, waardoor AWS geen toegang heeft tot de sleutels. Alle toegang tot de keys gelogd wordt (m.b.v. CloudTrail)

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. Daarnaast wordt er in Snappet gebruik gemaakt van adaptiviteit (algoritmes/AI) en wordt de wijze waarop hierin persoonsgegevens worden verwerkt beschreven. Tot slot wordt komen enkele andere meer technische aspecten, welke samenhangen met de applicatie Snappet, aan bod.

Status van informatiebeveiliging

Er is globaal onderzoek verricht naar de status van informatiebeveiliging van de applicatie Snappet. Dit onderzoek is gebaseerd op informatie welke door Snappet is verstrekt en een compliance check op het ROSA classificatieschema. Er is geen technisch onderzoek uitgevoerd naar het implementatieniveau van beveiliging.

Uit dit onderzoek is de volgende informatie verkregen:

- Er worden verschillende classificatieniveaus voor de applicatie gebruikt afhankelijk van het soort gebruik. Voor de classificaties Beschikbaarheid en Integriteit staan deze altijd op Midden. Voor Vertrouwelijkheid staat deze op Laag voor de omgeving van leerlingen, Midden voor Leerkrachten en Hoog voor de centrale applicatie.
- Snappet is niet ISO27001 gecertificeerd maar geeft wel aan conform deze richtlijnen te werken. In het Informatiebeveiligings- en ISMS-beleid van Snappet is de werking van hun ISMS beschreven inclusief PDCA-cyclus. De werking is aangetoond door het in Spanje verstrekte ENS certificaat. Snappet heeft aangegeven per 01.07.2025 ISO gecertificeerd te willen zijn.
- Jaarlijks wordt de omgeving van Snappet aan een pentest onderworpen. De meest recente is van december 2022. Het rapport is besproken en bevindingen zijn correct door Snappet opgepakt en verholpen.
- Snappet geeft aan compliant te zijn aan het ROSA schema. Voor de categorieën Beschikbaarheid en Integriteit wordt volledig aan het ROSA schema voldaan. Voor de categorie Vertrouwelijkheid wordt bij 3 normen niet aan de vereisten voldaan maar zijn alternatieve implementaties voorhanden. Deze zijn beargumenteerd en voldoen.

Een bevinding is dat een verouderde encryptie methode wordt ondersteund (TLS 1.0 en 1.1). Snappet geeft aan dat deze variant alleen gebruikt wordt voor oudere tablets of oude devices die scholen nog in gebruik hebben en dat deze ondersteuning eind schooljaar 2023/24 beëindigd wordt.

Werking adaptiviteit / training modellen (algoritme/AI)

Snappet maakt gebruik van een algoritme ten behoeve van de inzet van adaptieve opdrachten. Deze adaptieve opdrachten passen zich aan aan het niveau van de leerling. Afhankelijk van de gegeven antwoorden zullen er moeilijkere of minder moeilijke vragen worden voorgelegd. Dit beoogt het laten groeien van de leerling op eigen niveau en tempo. Tijdens de DPIA heeft SIVON gekeken naar de werking van het adaptieve leersysteem, de persoonsgegevens die hierbinnen worden verzameld en hoe hier mee wordt omgegaan, maar ook de uitwerking van het adaptieve op het onderwijs in het geheel. In welke mate de uitkomst bijvoorbeeld doorslaggevend is voor impactvolle besluiten zoals of een leerling blijft zitten of de niveaubepaling voor het vervolgonderwijs.

SIVON heeft gekeken naar belangrijke AVG pijlers die van invloed zijn op de inzet van een adaptief leersysteem binnen een onderwijsapplicatie. Er is echter geen sprake geweest van een audit of Impact Assessment mensenrechten en Algoritmes[12].

Snappet gebruikt in haar platform verschillende modellen. De eerste is het ability model, wat gebruikt wordt om een leraar en de leerling te informeren over vaardigheid en daarmee in staat te stellen om keuzes te maken. Het tweede domein is adaptieve, waarmee Snappet de (volgorde van) opgaven in de adaptieve werkmodus bepaalt.

[12] Impact Assessment Mensenrechten en Algoritmes | Rapport | Rijksoverheid.nl

Snappet kent twee varianten van het trainen van de modellen. Dit betreft Machine learning en Deep learning.

Machine learning

Aan de hand van machine learning wordt het model op zo'n manier getraind dat naarmate er meer data (waaronder antwoorden) worden verzameld de machine learning beter in staat is om patronen en informatie te extraheren uit de beschikbare gegevens. Tijdens het leerproces past het systeem de parameters van het model aan om de prestaties te optimaliseren. Dit heeft tot gevolg dat het model steeds beter in staat is om de juiste opdrachten voor te leggen. Binnen dit model berekent Snappet automatisch wat de best passende volgende opdracht voor de leerling is.

Deep learning

Deze variant kenmerkt zich doordat het systeem zelf in staat is om kenmerken en patronen te ontdekken en hierdoor een zelflerend karakter heeft. De diepere inzichten en het begrijpen van complexere taken vindt hierbinnen plaats. Het deep learning model wordt door Snappet's data-wetenschappers voorzien van data uit data-laag 2 (zie pagina 21) van die scholen die hiermee hebben ingestemd. Met deze data wordt het model getraind, daarna wordt de data verwijderd zodat het getrainde model is geschoond van persoonsgegevens.

Monitoring en controle van de werking van het algoritme

Er zijn technische methoden om de betrouwbaarheid van algoritmes en AI te waarborgen. Deze kunnen zowel worden geïntegreerd in de ontwerp-, ontwikkelings- en gebruikersfases van een systeem zoals het adaptieve leersysteem van Snappet. Tijdens de ontwikkelfase van Snappet wordt breed besproken wat de effecten van een model zouden zijn. Hier wordt ook de pedagogische kennis binnen de organisatie bij betrokken, zodat er vanuit diverse invalshoeken gevalideerd wordt dat nieuwe ideeën geen onwelkome bijeffecten zouden kunnen hebben. Hier maakt Snappet ook de ethische afwegingen en ‘vangrails’ (beperkingen) voor een model.

Allereerst wordt er gekeken in hoeverre modellen voorspellen op een ongeziene validatie dataset (dus leerlingen die niet in de data zaten waarop ze zijn getraind). Snappet vergelijkt dan de voorspelde kans op goed gegeven antwoorden met het vastgestelde percentage correct. Dit doet Snappet niet alleen over alle datapunten heen, maar ook per subcategorie (bijvoorbeeld het begin van adaptief).

Als een algoritme voor deze test slaagt, vergelijkt Snappet adaptieve algoritmes door middel van A/B tests. Er wordt hier beoordeeld wat het model toevoegt t.o.v. eerdere modellen en hoe dit effect zich verspreid over verschillende subgroepen (leerjaar, level). Hierbij wordt ook gecorrigeerd voor school en klas effecten.

De algoritmes binnen Snappet krijgen als input beperkte antwoordeigenschappen, waaronder of het antwoord correct was of niet. Er wordt dus, met opzet, in geen van de

modellen expliciete karakteristieken van de leerling meegegeven. Denk dan bijvoorbeeld aan geslacht of naam, maar ook aan klas en school. Dit sluit directe bias uit.

Er vindt een validatie plaats of er bias aanwezig is op basis van leeftijd of leerprestatie. Om dat uit te sluiten heeft Snappet in A/B tests expliciet het effect van elk adaptief algoritme gesplitst per vaardigheid, percentielgroep en per leerjaar (groep 3 t/m 8). Hiermee controleert Snappet dat verbeteringen aan algoritmes een positief effect hebben voor elke subgroep van leerlingen.

Snappet monitort voortdurend de hoeveelheid antwoorden en groei in het platform. Hierdoor kan zij ingrijpen wanneer er afwijkingen plaatsvinden.

Bijsturen op resultaten

Er zijn diverse mogelijkheden voor de leerkracht om bij te sturen op de resultaten. Allereerst corrigeert de vakvaardigheid (bijvoorbeeld voor “rekenen”) zich vrij snel: bij benadering kun je stellen dat de 25 laatste opgaven de vaardigheid op leerdoel niveau grotendeels kunnen bepalen, en dat de laatste 500 antwoorden op vak niveau de vakvaardigheid bepalen.

Daarbij kan de leerkracht bijsturen op welke leerdoelen wordt gewerkt door leerlingen en wanneer door bepaalde leerlingen er niet meer geoefend hoeft te worden aan leerdoelen. Als blijkt dat een groep leerlingen een leerdoel nog niet beheerst kan in Snappet een extra instructie gegeven worden door de docent aan deze leerlingen.

Met bovenstaande is het eigenlijk nooit nodig om opnieuw te beginnen, het systeem corrigeert zich over het algemeen snel genoeg om weer een goed representatief beeld te geven van de vaardigheid van de leerling.

Mocht opnieuw beginnen alsnog nodig zijn, dan is er in het uiterste geval de mogelijkheid om een nieuwe leerling aan te maken waarbij de vakvaardigheid dus vrij snel weer een accuraat beeld geeft.

Verwerking persoonsgegevens

Snappet maakt voor de training van de algoritmes gebruik van persoonsgegevens van leerlingen. Dit betreft een beperkte dataset van niet direct identificeerbare gegevens van leerlingen bestaande uit:

- Snappet student ID[13];
- Exercise hierarchy ;
- Context van het antwoord (bijv. Gegeven binnen een lesopdracht, examen of adaptief);
- Uitkomst (correct/incorrect).

Snappet heeft kenbaar gemaakt op de roadmap aanvullende features te gebruiken voor toekomstig gebruik en verbetering van het algoritme. Deze zijn tijdens deze DPIA inzichtelijk

[13] Zodra het model afdoende getraind en getest is, wordt in het model de link met het Snappet student ID verwijderd. Zodra die link is verwijderd, is het model een pure statistische aggregatie waarmee het geanonimiseerde data wordt.

gemaakt en geven, mits dezelfde zorgvuldigheidseisen worden gehanteerd als in deze DPIA onder de aandacht worden gebracht, geen reden tot zorgen over de privacy.

Data verzameling

Bij het implementeren van adaptieve leersystemen is het cruciaal dat de verwerking van persoonsgegevens proportioneel is en niet meer inbreuk maakt op de privacy van leerlingen dan strikt noodzakelijk. Uit het onderzoek in deze DPIA is gebleken dat er geen gedragsgegevens, sociaal-economische informatie en andere persoonlijke details worden gebruikt of verzameld tijdens het trainen van het model. In het geval dat dit wel gebeurt, kan dit leiden tot gedetailleerde en mogelijk onnauwkeurige profielen van individuele leerlingen, met bijbehorende risico's zoals discriminatie, onrechtvaardige behandeling, of foutieve aannames en beslissingen. Bovendien kunnen gebruikers door hun dataprofiel in een specifieke richting worden gestuurd, wat afwijkt van hun eigen voorkeuren en invloed kan hebben op hun vrije persoonlijke ontwikkeling. Dit is in het huidige geval niet aan de orde. De inzichtelijk gemaakte data die gebruikt wordt ten behoeve van het trainen van de modellen heeft een proportioneel karakter hetgeen de inbreuk rechtvaardigt.

Transparantie

Het recht op informatie is een wezenlijk onderdeel uit de AVG waar verwerkingsverantwoordelijken aan moeten voldoen. Hierbij dient duidelijk te worden aangegeven welke persoonsgegevens worden verzameld, met welk doel dit gebeurt en onder welke voorwaarden deze verwerking plaatsvindt. Wanneer een schoolbestuur gebruik maakt van een digitaal leermiddel die voor een groot gedeelte draait en output geeft aan de hand van een adaptief leersysteem is het des te belangrijker om de werking hiervan op een begrijpelijke manier te over het voetlicht te brengen. Snappet heeft hiervoor een informatieve pagina op de website[14] waarin de werking en kwaliteitscontrole van de adaptiviteit wordt uitgelegd.

Overige technische bevindingen

Snappet is een webapplicatie (software-as-a-service) en maakt gebruik van verschillende (sub)domeinen. Snappet.org is voor de US website, de sub-domeinen van snappet.org worden gebruikt door het Snappet platform. De landextensies zijn vooral voor de websites. Snappet is langzaam bezig om delen van het platform ook via landextensies aan te gaan bieden (zoals .nl / .es).

Voor wat betreft het gebruik van cookies kan worden volstaan met de constatering dat er alleen *1st party cookies* worden geplaatst en dat er geen sprake is van *third party tracking*.

[14] Hoe werkt de adaptiviteit van Snappet? – Stichting Snappet

10. Juridisch en beleidsmatig kader

In dit hoofdstuk wordt aandacht gegeven aan de voor het verwerkingsproces van toepassing zijnde wet- en regelgeving, niet zijnde de (U)AVG. De verder uitwerking van de grondslag komt in hoofdstuk 12 aan de orde.

In deze 'Juridische paragraaf' wordt uiteengezet wat de wettelijke basis is in relatie tot de doelen in het kader van het basisonderwijs voor wat betreft het aanbieden van leermiddelen.

Wet op het primair onderwijs (WPO)

In de sectorspecifieke wetgeving die op de schoolbesturen van toepassing is bij het uitvoeren van de processen die in deze DPIA centraal staan, zijn de hoofdlijnen van de hierbij gepaard gaande verwerkingen van persoonsgegevens voldoende kenbaar. Zo behoort het tot de verantwoordelijkheid van de school om er voor zorg te dragen dat de leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen[15].

Voor wat betreft de inzet van digitale middelen ten behoeve van dit doel impliceert de WPO evengoed dat scholen deze mogelijkheid hebben. Dit kan door middel van het aanmaken en gebruiken van het pseudoniem[16] van de leerling voor het toegang geven tot een digitaal leermiddel of het digitaal afnemen van toetsen[17]. Onder deze categorie valt ook het gebruik van Snappet.

De inhoud van het onderwijs omvat, al dan niet in samenhang, de drie kernvakken die ook het lespakket van Snappet behelzen te weten rekenen, taal en spelling. Het aanbod vanuit Snappet sluit daarmee aan op de wettelijk vastgestelde[18] inhoud van het basisonderwijs.

Normenkader IBP

Digitaal veilig onderwijs voor leerling en leerkracht is het doel geweest bij de ontwikkeling van het Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs (IBP FO). Met dit hulpmiddel kunnen schoolbesturen toewerken naar sterkere informatiebeveiliging en betere bescherming van persoonsgegevens. Dit normenkader wordt op termijn wettelijk verankerd hetgeen betekent dat scholen binnenkort moeten voldoen aan deze normen. Leveranciers krijgen ook te maken met de effecten van het normenkader, denk hierbij aan het managen van leveranciers in de keten en het stellen van bepaalde eisen op het gebied van IBP zoals in hoofdstuk 15 van IBP FO nader is uitgewerkt.

Wet- en regelgeving

Onderstaande wet- en regelgeving is op de verwerking van persoonsgegeven door Snappet van toepassing.

---

[15] Artikel 8, eerste lid, WPO wetten.nl - Regeling - Wet op het primair onderwijs - BWBR0003420 (overheid.nl)
[16] Het pseudoniem wordt gegenereerd uit het persoonsgebonden nummer van een leerling en kan worden gebruikt t.b.v. het bieden van onderwijsvoorzieningen en begeleiding. Artikel 178a, lid 11, WPO.
[17] Gebruik persoonsgebonden nummer door bevoegd gezag, Artikel 178a, twaalfde lid, WPO.
[18] Artikel 9, eerste lid, sub b en c, WPO, wetten.nl - Regeling - Wet op het primair onderwijs - BWBR0003420 (overheid.nl)

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
Leermiddelen (inzet van)	Wet op het primair onderwijs (WPO)	Artikel 8, eerste lid WPO Artikel 9 WPO
Digitaal afnemen van toetsen	Wet op het primair onderwijs (WPO)	Artikel 182 lid 12 WPO
Inzet van leermiddelen en het digitaal afnemen van toetsen via een externe leverancier (als ketenpartner)	Normenkader IBP	Hoofdstuk 15, Ketenbeheer

11. Bewaartermijnen

De volgende bewaartermijnen zijn op de verwerking van Persoonsgegevens binnen Snappet van toepassing.

Gegevensverwerking	Verwerkingsdoeleinde	Categorie persoonsgegevens	Bewaartermijn en grondslag
Onderwijsevaluatie Onderwijsuitvoering Leerlingbegeleiding	Onderwijs geven en leerlingen kunnen volgen en begeleiden	*Algemene en overige contactgegevens*	Verwijderd na instructie van de onderwijsinstelling
Onderwijsevaluatie Onderwijsuitvoering Leerlingbegeleiding	Onderwijs geven en leerlingen kunnen volgen en begeleiden	*Gegevens m.b.t. studievoortgang of studietraject*	Verwijderd na instructie van de onderwijsinstelling
ICT-ondersteuning Informatiebeveiliging & privacy	Het verkrijgen van toegang en de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid	*Diagnostische en loggegevens*	Gegevens worden na 6 maanden verwijderd door Snappet
Onderwijsevaluatie Onderwijsuitvoering	Vaststellen van leerplannen en leerdoelen, vakken naar behoefte toe	*Trainingsdata*	Data wordt geanonimiseerd

	voegen en personaliseren van de inhoud en de aard van de leermiddelen door de Onderwijsinstellingen en/of leerkracht of op verzoek van de Onderwijsinstelling en/of Leerkracht door Snappet.		
Personeel en organisatie	Optioneel (adviseren leerkrachten)	*Algemene en overige contactgegevens*	Verwijderd na instructie van de onderwijsinstelling

Vanuit Kennisnet[14] zijn op de persoonsgegevens die binnen Snappet worden verwerkt de volgende bewaartermijnen van toepassing. Deze termijnen kunnen door de onderwijsinstelling op verzoek worden doorgevoerd in Snappet.

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

Snappet biedt hiervoor de mogelijkheid om gegevens op verzoek te laten verwijderen (via de helpdesk), en biedt (nog) geen handmatige instelling en er is geen sprake van standaard ingestelde verwijdertermijnen. Snappet heeft aangegeven hier een oplossing voor te realiseren (zie ook onder risico's en maatregelen).

De AVG schrijft voor dat persoonsgegevens niet langer mogen worden bewaard dan nodig. In sommige gevallen kan worden aangesloten bij wettelijke bewaartermijnen. Voor de verwerkingen die binnen een leerapplicatie plaatsvinden (zoals de gemaakte opdrachten en toetsen) zijn er geen wettelijke bewaartermijnen maar wél voor de resultaten daarvan die binnen het Leerlingadministratiesysteem (LAS) worden opgeslagen. Binnen het LAS krijgt het onderwijskundig rapport[1] vorm waarin, naast de uit de leerapplicatie afkomstige resultaten, ook andere persoonlijke informatie wordt opgeslagen zoals verslagen van oudergesprekken. Voor het onderwijskundig rapport geldt een wettelijke bewaartermijn van 5 jaar na uitschrijving van de leerling.

Nadat de relevante leerresultaten uit de leerapplicatie zijn opgenomen in het LAS is het in de regel niet langer nodig om deze ook nog in de leerapplicatie te bewaren. Dit betekent dat de bewaartermijn beperkt kan worden tot het (jaarlijkse) moment waarop de relevante leerresultaten in het LAS zijn opgenomen. Mocht het voor de school van waarde zijn om de

gegevens langer te bewaren, bijvoorbeeld omdat de leerapplicatie voorziet in een gedetailleerde ontwikkeling van de leer- en ontwikkelprestaties en/of de leerling zelf toegang heeft tot de ontwikkelingen en resultaten van de afgelopen jaren, dan dient hiervoor een afzonderlijke onderbouwing en termijn voor te worden vastgesteld. Een dergelijke onderbouwing kan bijvoorbeeld in het bewaartermijnenbeleid worden opgenomen of bij gebrek daaraan in een ander daarvoor bestemd document of structuur. Dit lijkt aan de orde bij Snappet.

Wanneer na het overzetten van de resultaten/cijfers naar het LAS, van deze gegevens binnen de leerapplicatie geen gebruik meer wordt gemaakt kunnen deze gegevens worden verwijderd. Hiervoor hoeft niet gewacht te worden totdat de leerling de school heeft verlaten. Een verwijdertermijn van bijvoorbeeld 1 jaar na afronding van het betreffende schooljaar kan in acht worden genomen. Controleer voor verwijdering of de mutatie naar het LAS volledig heeft plaatsgevonden.

4. Deel B: Beoordeling rechtmatigheid gegevensverwerkingen

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

12. Rechtsgrond

Een belangrijk onderdeel van de verantwoordingsplicht is dat kan 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.

AVG

Artikel 6 van de AVG geeft een zestal verwerkingsgrondslagen welke gebruikt kunnen worden om persoonsgegevens te mogen verwerken. Schoolbesturen maken in de uitoefening van de onderwijstaken zoals in deze DPIA beschreven gebruik van de bij formele wet voorgeschreven Wet op het primair onderwijs (WPO).

Dit brengt met zich mee dat schoolbesturen de verwerking kunnen baseren op artikel 6, eerste lid onder e van de AVG. De verwerkingen zijn noodzakelijk voor de vervulling van een taak van algemeen belang welke aan de verwerkingsverantwoordelijke is opgedragen. Deze verwerkingsgrondslag is niet uitsluitend voor overheidsinstellingen en bestuursorganen maar kan ook worden gebruikt door organisaties die persoonsgegevens verwerken ten behoeve van een publieke taak.

De AVG eist dat de rechtsgronden voor het verwerken van persoonsgegevens bij lidstatelijk recht zijn vastgelegd. Met andere woorden, de door de Nederlandse overheid opgelegde taak waarvoor het verwerken van persoonsgegevens onvermijdelijk is, moet specifiek zijn vastgelegd in een wet. De verwerkingsverantwoordelijke (de onderwijsinstelling) is als zodanig in de WPO aangewezen om deze taak uit te voeren.

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

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

De verwerking van persoonsgegevens in Snappet is gebaseerd op de volgende grondslagen en dekt alle in paragraaf 4 opgesomde verwerkingsdoeleinden.

Verwerking/doeleinde	Grondslag AVG	Toelichting
• Leermiddelen (inzet van) • Digitaal afnemen van toetsen • De opslag van leer- en toetsresultaten. • Het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten. • De beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een Onderwijsdeelnemer. • De beoordeling van de leer- en testresultaten van één leerling ten opzichte van de resultaten van een normgroep, om inzicht te krijgen hoe een leerling presteert ten opzichte van deze groep. • Analyse en interpretatie van leer- en toetsresultaten. • Het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier. • Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie. • De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens. • De continuïteit, verbetering en goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning. • Het beschikbaar stellen van gegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan digitale onderwijsmiddelen.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 182 lid 12 WPO. Taak van algemeen belang (of openbaar gezag)[20].	Het inzetten van een leermethode zoals Snappet is toegestaan op grond van artikel 6 lid 1 sub e AVG (*algemeen belang, o.b.v. een wettelijke verplichting, zijnde de WPO.*

De conclusie is dat de verwerking van persoonsgegevens bij het inzetten van een leermethode zoals Snappet door de onderwijsinstelling plaatsvindt op grond van artikel 6 lid 1 sub e AVG (algemeen belang, o.b.v. de WPO).

13. Bijzondere persoonsgegevens

In Snappet worden geen bijzondere of strafrechtelijke persoonsgegevens verwerkt.

14. Doelbinding

In Snappet worden er geen persoonsgegevens verwerkt voor een ander doel dan waarvoor ze oorspronkelijk verzameld zijn. Alle verwerkingen vinden uitdrukkelijk in opdracht van de verwerkingsverantwoordelijke plaats.

Voor optionele verwerkingen wordt expliciet toestemming gevraagd aan het schoolbestuur.

15. Kinderrechten-afweging (Best Interests Assessment Children)

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

Met schoolbesturen als leden van SIVON in het primair en voortgezet onderwijs, betekent dit dat SIVON in haar DPIA's rekening houdt met o.a. gebruikers (betrokkenen) in de leeftijd van 4 tot 18 jaar (of ouder). Kinderen hebben recht op specifieke bescherming van hun persoonsgegevens. Dit volgt uit het feit dat zij zich minder bewust zijn van de risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van hun persoonsgegevens.

SIVON geeft hier in deze DPIA invulling aan door af te wegen of het gebruik van Snappet en/of de gegevensverwerking(en) die daarmee samenhangen, in het belang zijn van de betrokkenen (kind/leerling als betrokkene). SIVON maakt hierbij gebruik van de systematiek van de best interests assessment children van de Britse ICO[19]. De afweging bestaat uit 4 stappen:

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

Hieronder wordt beschreven welke rechten[20] van en voor kinderen relevant zijn in het kader van deze DPIA. Van belang is de leeftijd van de kinderen (leeftijdsadequaat). Hierbij wordt

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

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

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

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

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

2. Identificeer het effect van de gegevensverwerking en gebruik van Snappet op deze rechten

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

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

3. Beoordeel of dit effect wenselijk is

De impact en de ernst van deze mogelijke gevolgen voor het kind kunnen groot zijn. Snappet heeft echter verschillende maatregelen getroffen waardoor de waarschijnlijkheid dat de gevolgen, zoals het aanbieden van niet bij het niveau van de leerling aansluitende opdrachten, op zullen treden zeer laag is. Derhalve wordt het risico als laag ingeschat.

Snappet wordt altijd ingezet via het onderwijskundige proces van de onderwijsinstelling, waarbij de onderwijsinstelling bepaalt wie verantwoordelijk is en er dus geen sprake is van willekeurigheid of onrechtmatigheid.

Binnen Snappet is de enige verwerking waar geen leerkracht tussen zit, het adaptief aanbieden van de volgende opgave. Bij alle andere geautomatiseerde verwerkingen blijft het de keuze van de leerkracht wat ermee gebeurt. Bij het adaptief aanbieden van de volgende opgave blijft het de keuze van de leerkracht of de leerlingen in de klas het gaan gebruiken.

Als de leerkracht adaptieve opgaven inzet, dan gebeurt dat op basis van een algoritme waarbij maatregelen zijn genomen om de gelijke kansen van alle kinderen (ongeacht achtergrond of context) te beschermen. Deze maatregelen bestaan eruit dat het algoritme en de bijbehorende data geen enkele kenmerken van personen bevat die iets zeggen over de achtergrond, in combinatie met A/B tests waarbij expliciet wordt getest dat verbeteringen aan het algoritme een positief effect hebben op subgroepen van leerlingen.

Snappet heeft ervoor gezorgd dat onderwijsinstellingen de mogelijkheid hebben om in te grijpen. Als kinderen het niet eens zijn met iets, dan kunnen ze dit in de klas bespreken met de leerkracht en heeft deze de mogelijkheid hier iets mee te doen want de leerkracht houdt de regie binnen Snappet. Als ouders/voogden het niet eens zijn met een beslissing of standpunt, kunnen ze dat met de school bespreken. In al deze gevallen levert Snappet informatie en suggesties, waarbij de leerkracht en de school de regie houden en hun eigen keuzes maken. Aanvullend kan de leerkracht op onderdelen zelf antwoorden van leerlingen verwijderen en als er meer opgeschoond moet worden kan de onderwijsinstelling dit aanvragen bij de Snappet servicedesk.

Correcties Snappet

Bij het geven van onjuiste antwoorden op de voorgelegde opdrachten ziet de leerling zich geconfronteerd met een duidelijk zichtbare rode streep door het onjuist gegeven antwoord in combinatie met puntenaftrek. Dit geautomatiseerde proces wordt ook wel ‘Optimale Feedback (hierna: feedback) genoemd'[21]. Snappet heeft aangegeven dat de effecten van deze corrigerende handelingen een licht positief effect laten zien op de uiteindelijke resultaten. Snappet heeft hierop veel getest en daarbij gekeken naar de leerresultaten waarbij voor onjuiste antwoorden een grote rode streep wordt gezet. Het idee daarbij is dat een dergelijke correctie tot effect zal hebben dat de leerling de benodigde concentratie zal herpakken voor het geven van het juist antwoord. Voor de beantwoording van een

[21] https://snappet.nl/oplossingen/de-beste-feedback-voor-elke-leerling/#:~:text=De%20huidige%2C%20optimale%20feedback%20blijft,huidige%20feedback%20minder%20vooruitgang%20maken.

moeilijke vraag kunnen evenredig veel punten verkregen worden als bij de onjuiste beantwoording van een makkelijke vraag.

Voor zover scholen van mening zijn dat dergelijke feedback een onwenselijk effect heeft op een specifieke leerling of klas dan kan deze worden uitgeschakeld door 'minimale feedback' te activeren. Leerlingen zien dan geen rode streep meer na een fout antwoord en ook de minpunten zijn verborgen.

Ten aanzien van deze kinderrechten afweging is het van belang om stil te staan bij het effect van een dergelijke feedback op de leerlingen. Van belang is dat deze functionaliteit niet in strijd mag zijn met de vrijheid van de leerling om zich te ontwikkelen en te ontplooien. Hierbij wordt opgemerkt dat het al dan niet gebruik maken van deze manier van corrigeren zich meer afspeelt in het didactische domein. De wenselijkheid ervan dient daarom vanuit dat domein beoordeeld te worden. Vanuit het onderzoek binnen deze DPIA is echter bij het gebruik van deze feedback niet gebleken van een inperking van de rechten en vrijheden van de leerling om vrij te kunnen leren.

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

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

16 a. Noodzakelijkheid

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

Uit de analyse van de gegevensverwerking (zie deel A: de gegevensverwerkingsanalyse) blijkt dat de door Snappet te verwerken persoonsgegevens noodzakelijk zijn in relatie tot het doel van de gegevensverwerking, te weten het via het toepassen van leermiddelen en toets applicatie kunnen waarborgen van een ononderbroken ontwikkelingsproces[22] voor de leerling.

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

16. b. Proportionaliteit en subsidiariteit

De Onderwijsinstelling is verantwoordelijk voor de uitvoering van goed onderwijs volgens de bepalingen van de Wet op het primair onderwijs. Hierbij staat de inbreuk op de persoonlijke

[22] Zie artikel 8 WPO.

levenssfeer in evenredige verhouding tot de verwerkingsdoelen, namelijk het waarborgen van een ononderbroken ontwikkelingsproces met behulp van (digitale) leermiddelen. Vanwege het feit dat via een prudent toegangsbeleid alleen medewerkers van de onderwijsinstelling op een 'need to know' basis bij de leerlingen van hun groep kunnen, is de 'inbreuk' beperkt tot professionals die leerlingen ondersteunen in hun ontwikkelingsproces. De minimale gegevens zijn noodzakelijk om de vakken en toetsen op het oefen- en toets platform Snappet aan leerlingen aan te kunnen bieden.

Het online leer- en toetsplatform Snappet is een complete en op het onderwijs toegepaste leermethodiek. Het (digitaal) behandelen van les- en oefenstof en het afleggen van toetsen – met als doel het gewenste referentieniveaus te behalen - is noodzakelijk in het kader van de WPO. Het gebruik van potlood/papier is een alternatief, maar deze optie is niet per definitie makkelijker en veiliger. Het gebruik van een digitaal leerplatform is niet meer belastend om hetzelfde doel te behalen.

17. Rechten van de betrokkenen

In het volgende overzicht wordt weer gegeven hoe betrokkenen hun rechten kunnen uitoefenen.

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking*
Het recht op informatie	• De onderwijsinstelling dient als verwerkingsverantwoordelijke te zorgen voor een openbaar gepubliceerde privacyverklaring; • Daarnaast is op de website van Snappet informatie voorhanden over de gegevensverwerking en over het adaptieve model.	n.v.t.
Het recht van inzage	Snappet kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Het recht op rectificatie	Snappet kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Het recht op gegevenswissing	Snappet kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Het recht op beperking van de verwerking	Snappet kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	Snappet kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.
Het recht op overdraagbaarheid van gegevens	Snappet kan op verzoek van de onderwijsinstelling dit recht waarborgen.	n.v.t.

Het recht van bezwaar	Snappet 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	Dit is niet aan de orde. De Onderwijsinstelling neemt de uitkomsten van de leer- en toetsresultaten mee in de eigen beoordeling van de leerling.	n.v.t.

18. Beoordeling verwerkersovereenkomst

Voor leveranciers die deelnemer of medestander zijn van het Convenant digitale onderwijsmiddelen en privacy 4.0 (ook wel: Privacyconvenant Onderwijs, hierna: Convenant) en daarbij gebruik maken van het daarbij horende model verwerkersovereenkomst vindt een toetsing plaats welke wordt afgezet tegen de vereisten van het convenant. Dit wordt de theoretische toets genoemd. Aanvullend hierop zal ook, aan de hand van de inzichten die deze DPIA heeft gebracht, een praktische toets plaatsvinden. Hierbij zal een vergelijk worden gemaakt tussen de in de theorie genoemde afspraken en de verwerkingen die in de praktijk plaatsvinden. De hiervoor gebruikte toetsingskaders zijn in de bijlage (verwerkersovereenkomst Toetsformulier met link) terug te vinden.

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

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

Toets - Verwerkersovereenkomst	**OPMERKING VOOR TOETSRAPPORT**
Ondergetekende - Verwerker: naam, juridische entiteit, KvK-nummer, tekenbevoegde	KvK-nummer ontbreekt: Is een van de vereisten uit Model VWO van het PrivacyConvenant Onderwijs, en nodig om als unieke waarde (naam kan vaker voorkomen/is aan meer wijziging onderhevig) te kunnen controleren of de overeenkomst vanuit welke/juiste juridische entiteit is/wordt aangegaan (er is voldoende praktijkervaring dat de juridische entiteit/naam niet klopt). Voor de volledigheid en transparantie graag opnemen.
Toets - Bijlage 1: Privacybijsluiter	**OPMERKING VOOR TOETSRAPPORT**
F. Categorieën Persoonsgegevens inclusief bewaartermijnen **Dit onderdeel bestaat uit: ***	

1. een omschrijving van de categorieën Betrokkenen (o.a. Onderwijsdeelnemers, ouders/verzorgers, medewerkers) over wie Persoonsgegevens worden verwerkt, en de te verwerken categorieën Persoonsgegevens van deze Betrokkenen, en	Categorieën betrokkenen worden niet uitgesplitst: In het Model worden persoonsgegevens uitgesplitst per betrokkene-categorie. Graag het Model volgen. Indien Betrokkene-categorieën en Gebruikers consistent en conform Model worden doorgevoerd, hoeft dit alleen een plek te krijgen bij Medewerker. ID en pseudonieme gegevens ontbreken: Wanneer het internal ID/pupil ID of security ID direct of indirect te herleiden is tot een persoon is het een persoonsgegeven en dient het opgenomen te worden in de verwerkersovereenkomst.
2. door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen).	Bewaartermijnen zijn onvoldoende duidelijk opgenomen: Het zou goed zijn om de beschikbare informatie (o.a. onderscheid Audit-logging en technische logging) bij dit onderdeel in de verwerkersovereenkomst op te nemen, inclusief termijn van verwijdering/teruggave na einde onderliggende overeenkomst.
G. Locatie van opslag en Verwerking Persoonsgegevens	
Onder G. wordt vastgelegd wat de plaats(en)/land(en) van opslag en Verwerking van de Persoonsgegevens zijn.	Er wordt geen verbinding gemaakt met Doeleinden: Graag opnemen conform Model.
Toets - Bijlage 2: Beveiligingsbijlage	**OPMERKING VOOR TOETSRAPPORT**
Toets - Bijlage 3: Wijzigingenbijlage (indien van toepassing)	**OPMERKING VOOR TOETSRAPPORT**
1. Beschrijving noodzakelijke afwijkingen Model Verwerkersovereenkomst incl. Bijlagen	Er wordt niet geheel conform Model gewerkt of niet alle wijzigingen zijn opgenomen in de Wijzigingenbijlage: Graag conform vereisten van Model verwerken of anders ook alle andere wijzigingen opnemen in de Wijzigingenbijlage.

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:

De methodiek die wordt gevolgd, is beschreven door de Britse toezichthouder[23] om risico's te classificeren. Hierbij wordt een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade).

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

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

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

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

[23] 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

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

In onderstaande risicotabel worden de risico's beschreven. Per risico worden de mogelijke oorzaken en gevolgen aangegeven met daarbij de kans dat het zich voordoet en de impact. Tevens is aangegeven of het risico betrekking heeft op een proces waarbij Snappet wordt ingezet of dat het risico het systeem zelf betreft (de applicatie).

Risicotabel:

Risico nr.	Mapgood	Risico-omschrijving	Oorzaak / toelichting	Kans	Impact	Risico	Proces en/of systeem -risico?
1	A	Het risico is dat dataverkeer onvoldoende veilig is omdat onderwijsinstellingen gebruik maken van verouderde devices die niet de gangbare protocollen ondersteunen.	Onderwijsinstellingen gebruiken verouderde devices. Persoonsgegevens kunnen daardoor in verkeerde handen vallen.	2	2	4	Systeem (school)
2	O	Het risico is dat de verwerkingsverantwoordelijke geen toereikende afspraken met de verwerker heeft gemaakt over de verwerking van de persoonsgegevens.	De verwerkersovereenkomst voldoet niet aan alle eisen (Zie uitwerking paragraaf 18). Als er geen goede afspraken met de 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	2	4	Proces (Snappet en school)
3	O	Het risico is dat er bij accounts (met veel rechten) onregelmatigheden plaatsvinden doordat de	Onderwijsinstellingen stellen het gebruik van MFA (bij beheerders) niet verplicht. De kans is groter dat onbevoegde gebruikers toegang	3	3	9	Proces (school)

		toegang tot de applicatie onvoldoende is beveiligd.	krijgen tot persoonsgegevens en/of gegevens worden gemuteerd.				
4	P	Het risico is dat er door het gebruik van de export en/of download functie mogelijk gevoelige persoonsgegevens buiten de applicatie terecht komen wat verlies van controle over deze data tot gevolg heeft.	Het maken van exports en downloads is een ongecontroleerd proces. Het is mogelijk dat onbevoegde gebruikers toegang krijgen tot persoonsgegevens en dat persoonsgegevens op allerlei plekken worden bewaard en niet tijdig worden vernietigd.	2	3	6	Systeem (Snappet) en Proces (school)
5	G	Het risico is dat de onderwijsinstelling geen of onvoldoende zicht heeft op onregelmatigheden m.b.t. de verwerking hetgeen de mogelijke controle op de gegevensverwerkingen beperkt.	Toegang tot logging informatie is alleen via de helpdesk te verkrijgen. De gegevens van de betrokkenen kunnen door onbevoegden worden ingezien of gewijzigd zonder dat de school daar rechtstreeks controle op kan uitoefenen of onregelmatigheden kan achterhalen.	2	3	6	Systeem (Snappet) en Proces (School)
6	O	Het risico is dat de werking van Snappet en het algoritme / adaptiviteit niet transparant is waardoor betrokkenen hun recht op informatie niet kunnen uitoefenen.	Onderwijsinstellingen stellen gebruikers (en hun ouders) onvoldoende op de hoogte van de werking van het leermiddel. Betrokkenen zijn onvoldoende geïnformeerd over de verwerking van hun persoonsgegevens.	2	2	4	Proces (School)

7	P	Het risico is dat persoonsgegevens te lang worden bewaard, hetgeen risico's met zich meebrengt voor de rechten en vrijheden van betrokkenen.	Onderwijsinstelling moet zelf opdracht geven tot verwijdering. Er is geen mogelijkheid om (in activatie tool) bewaartermijnen in te stellen. Verwijderen van gegevens na einde contract is een handmatig proces. Dit vergroot het risico dat persoonsgegevens langer worden bewaard dan noodzakelijk is (met het risico op ongewenste openbaarmaking).	2	2	4	Systeem (Snappet) en Proces (School)
8	O	Het risico is dat een beoordeling of een besluit op beperkte informatie wordt gebaseerd zonder voldoende zicht op de algemene prestaties van een leerling.	Onderwijsinstelling gebruikt alleen inzichten Snappet voor oordeels- en besluitvorming over bijvoorbeeld doubleren of niveaubepaling vervolgonderwijs. De leerling ondervindt mogelijke nadelige (psychische) gevolgen.	2	2	4	Proces (School)

6. Deel D: Beschrijving voorgenomen maatregelen

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

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

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

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

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

19. Maatregelen

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 (Snappet /school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum)maatregel geïmplementeerd?
1	Niet veilige dataverbindingen.	4	Onderwijsinstelling moet afscheid nemen van verouderde devices.	School	2		
2	Verwerker gebruikt het model in de verwerkersovereenkomst niet (goed).	4	1. Snappet moet de verwerkersovereenkomst aanpassen aan Model verwerkersovereenkomst privacy convenant 4.0 toepassen. 2. Onderwijsinstelling moet Verwerkersovereenkomst sluiten cnf. model.	Snappet en school	2		1. Snappet: 01.07.2024
3	Geen gebruik MFA	9	Onderwijsinstelling moet gebruik van MFA (voor beheerders) verplichten.	School	3		
4	Export en download van leerlingresultaten,	6	1. Snappet moet voor de Onderwijsinstelling direct zichtbare logging maken zodat achterhaald kan worden welke exports er door wie zijn gemaakt. 2. Onderwijsinstelling moet afspraken maken over het maken en gebruiken van exports en hier controle op uitoefenen.	Snappet en School	3		1. Snappet: 01.09.2024
5	Geen of onvoldoende toegang tot logging informatie.	6	1. Snappet moet audit logging toegankelijk maken zonder dat de helpdesk daarvoor nodig is, zodat Onderwijsinstelling zelf toegang heeft tot foutieve inlog pogingen en mutaties van resultaten. 2. Onderwijsinstelling moet afspraken maken over controle op de login.	Snappet	3		1. Snappet: 01.03.2025
6	Werking Snappet niet transparant.	4	Onderwijsinstelling moet informatie verstrekken. De school kan verwijzen naar informatiepagina's van	School	2		

			Snappet of voorzien in een eigen informatievoorziening.				
7	Gegevens worden te lang bewaard.	6	1. Snappet moet mogelijkheid bieden om bewaartermijnen in te stellen. 2. Onderwijsinstelling moet bewaartermijnenbeleid opstellen en toepassen.	Snappet en school	2		1. Snappet: 01.12.2024
8	Onjuiste oordeels- of besluitvorming	4	Onderwijsinstelling moet in beleid opnemen dat zij meerdere elementen meeneemt in oordeels- en besluitvorming.	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 privacyvereisten binnen het schoolbestuur. Onderstaande tabellen bieden een kader om inzicht te krijgen op de aan- of afwezigheid van belangrijke basismaatregelen. Betrek de bevindingen bij de risicobeoordeling en voer maatregelen door waar nodig.

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

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

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

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

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	De verwerkersovereenkomst met verwerker is getekend.		
2	De verwerking is opgenomen in het register van verwerkingen.		
3	Het bestuur zal de DPIA van Snappet 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 Snappet.		

9	Het bestuur heeft autorisaties ingericht op basis van ‘need to know’ (role based access).		
10	Afstemming met betrokkenen. Het bestuur heeft bij het uitvoeren van de lokale DPIA de betrokkenen om hun mening gevraagd over de verwerking en deze meegenomen in de DPIA (artikel 35 lid 9 AVG). Dit kan bijvoorbeeld via de medezeggenschapsraad.		
11	Gebruikers van de applicatie zijn/worden afdoende getraind in het gebruik ervan.		
12	Persoonsgegevens worden niet op verkeerde plekken opgeslagen omdat regels en/of bekendheid met Snappet 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 Snappet en dit is tevens gedocumenteerd.		
14	De onderwijsinstelling neemt verantwoordelijkheid voor het veilig koppelen van het Snappet 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 een beoordeling of een besluit op uitsluitend de vanuit Snappet verkregen inzichten wordt gebaseerd zonder voldoende zicht op de algemene prestaties van een leerling.	De onderwijsinstelling neemt in haar beleid op dat zij meerdere elementen meeneemt in oordeels- en besluitvorming.		
Het risico is dat de werking van Snappet en het algoritme / adaptiviteit niet transparant is waardoor betrokkenen hun recht op informatie niet kunnen uitoefenen.	De onderwijsinstelling verstrekt informatie. De school kan verwijzen naar informatiepagina's van Snappet of voorzien in een eigen informatievoorziening.		
Het risico is dat er bij accounts (met veel rechten) onregelmatigheden plaatsvinden doordat de toegang tot de applicatie onvoldoende is beveiligd.	De onderwijsinstelling verplicht het gebruik van MFA (voor beheerders).		
Het risico is dat er door het gebruik van de export en/of download functie mogelijk gevoelige persoonsgegevens buiten de applicatie terecht komen wat verlies van controle over deze data tot gevolg heeft.	De onderwijsinstelling maakt afspraken over het maken en gebruiken van exports en hier controle op uitoefenen.		

Het risico is dat persoonsgegevens te lang worden bewaard, hetgeen risico's met zich meebrengt voor de rechten en vrijheden van betrokkenen.	De onderwijsinstelling stelt een bewaartermijnenbeleid op en past dit toe.		
Het risico is dat dataverkeer onvoldoende veilig is omdat onderwijsinstellingen gebruik maken van verouderde devices die niet de gangbare protocollen ondersteunen.	De onderwijsinstelling neemt afscheid van verouderde devices die TLS1.2 e.v. niet ondersteunen.		

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

kans (waarschijnlijkheid) X impact (ernst) = risico

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

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

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

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

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

De in de lokale DPIA geconstateerde risico's betreffen:

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

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

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

Het schoolbestuur moet daarom zorgen voor:

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

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

H. Aanbevelingen

Naast de hiervoor genoemde bevindingen en maatregelen, zijn er een aantal aanbevelingen die buiten scope van deze DPIA vallen omdat zij nietbinnen 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: