CENTRALE DPIA

Studiemeter voor het Voortgezet Onderwijs

(Leverancier: Uitgeverij Deviant)

Centrale DPIA sjabloon: Versie 1.2 (juni 2023)

DPIA Studiemeter: Versie 1.0

Colofon

DPIA uitgevoerd door	Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A. (SIVON) www.sivon.nl info@sivon.nl
Betrokkenen bij uitvoering DPIA	Sander van de Molen (jurist en adviseur IBP) Ferdy IJsselmuiden (DPIA-projectmanager) Ashley Hoogendoorn (DPIA-projectmanager) Pascal Marcelis (jurist en adviseur IBP) Marcel de Rijke (ISO en adviseur IBP) René de Wolf (Quadraam) Hans-Peter Ligthart (portfoliomanager IBP)
Met dank aan	Team van Studiemeter (Leverancier Uitgeverij Deviant), te weten: Anne Boon (CISO) en Jelle Pol (Directie)

Deze DPIA is gebaseerd op het model van SIVON (*welke het Model DPIA Rijksdienst versie 2.0 volgt*), *Handreiking DPIA in het mbo*, *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (1.0)*. De gebruiker mag deze publicatie kopiëren, verspreiden, doorgeven, remixen en afgeleide werken maken onder de voorwaarde van het vermelden van de “Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A., [de naam van de betrokken schrijvers van de DPIA]” en link/bron/vindplaats van dit document (Creative Commons CC-BY 4.0).

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

Versie beheer DPIA Studiemeter

Datum	Versie	Wijziging
December 2023	0.1	Concept (SvdM)
December 2023	0.2	Tegenlezen (FIJ)
Januari – Maart 2024	0.3-18	Concept (SvdM), afstemmen geconstateerde risico's met Uitgeverij Deviant en onderzoek diverse onderwerpen
Maart – Mei 2024	0.91	Tegenlezen Uitgeverij Deviant en SIVON
Juni 2024	*1.0*	*Publicatie*

Inhoudsopgave

1. Samenvatting

Deze DPIA heeft betrekking op de digitale leeromgeving 'Studiemeter' voor het Voortgezet Onderwijs (VO), die door Uitgeverij Deviant als leverancier wordt geleverd aan scholen voor het VO. Studiemeter is een leerplatform voor het aanleren van basisvaardigheden voor taal en rekenen.

Kinderen, leerlingen in het VO, maken gebruik van deze leermethode. De risico's die het gebruik van dit digitale leermiddel met zich meebrengen worden in deze DPIA geïnventariseerd. Op basis van de risico's wordt nagegaan of de juiste maatregelen worden toegepast om deze risico's te minimaliseren, zodat een veilig gebruik van Studiemeter mogelijk is. De DPIA bevat alle wettelijk verplichte elementen van de AVG: een systematische beschrijving van de verwerkingen en de verwerkingsdoelen, de beoordeling van de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden, alsmede een beoordeling van de risico's voor betrokkenen en de getroffen maatregelen. Met het uitvoeren van een DPIA kan de verwerkingsverantwoordelijke aantoonbaar maken dat aan de verplichtingen van de AVG is voldaan.

Via Studiemeter hebben leerlingen en docenten van de onderwijsinstelling, toegang tot al het door hen bestelde lesmateriaal. Dit omvat *Nederlands en Rekenen*, als mogelijk ook aanvullend digitaal lesmateriaal bij alle methodes van Uitgeverij Deviant.

Samenwerking

De samenwerking tijdens het DPIA-proces met Uitgeverij Deviant als leverancier van het leermiddel Studiemeter was ronduit positief te noemen. De open werkwijze, goede gesprekken en gemotiveerde houding om verbetervoorstellen door te voeren hebben bijgedragen aan het onderzoek en identificatie van de risico's. Een belangrijke verbetering van de dienst op het gebied van informatiebeveiliging is het verhogen van de BIV-classificatie op het gebied van de Vertrouwelijkheid van Midden naar Hoog. Nadat SIVON en Uitgeverij Deviant hier inhoudelijk overeenstemming hadden bereikt is er vlot toegewerkt naar acties en deadlines om dit ook in de praktijk te realiseren. De gedane toezeggingen op dit gebied zorgen ervoor dat de dienst nog een stuk veiliger en robuuster wordt.

Ook de deelnemende school heeft belangrijke praktijkinzichten gebracht die wezenlijk waren voor het begrip van de werking van de dienst.

Conclusie

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

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

1. De verwerking van persoonsgegevens rechtmatig kan plaatsvinden en ook noodzakelijk is om het doel te bereiken;
2. De inbreuk op de persoonlijke levenssfeer in verhouding staat tot het doel en er geen minder belastende manier is om hetzelfde doel te bereiken;
3. Er adequate maatregelen zijn en worden getroffen om de verwerking te beschermen.

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

Risico's en maatregelen:
De volgende risico's zijn uit het DPIA-onderzoek naar voren gekomen

1. Risico: Dataminimalisatie: er worden te veel persoonsgegevens verwerkt. Binnen Studiemeter wordt per leerling vastgelegd of er sprake is van '*dyslexie*' of een '*auditieve beperking*'. Dit is een verwerking van bijzondere persoonsgegevens en leidt tot het risico op discriminatie van een individu.
Maatregel: (Uitgeverij Deviant) Technisch: Verwijderen/aanpassen vragen over dyslexie en auditieve beperking. Voorgesteld alternatief: Andere omschrijving Bijvoorbeeld '*extra tijd'*, of '*ondertiteling gewenst ja/nee*'. Deze maatregel is per 1 september 2024 ingeregeld.

2. Risico: Betrokkenen worden onjuist geïnformeerd over de cookies die worden geplaatst. Er worden meer of andere cookies geplaatst dan waarvoor toestemming is gegeven dan wel de mogelijkheid om per cookiesoort toestemming te geven ontbreekt. Dit leidt tot (mogelijke) niet toegestane profilering.
Maatregel: Uitgeverij Deviant verwijdert de '*toestemming pop up'* wanneer de betrokkene de leeromgeving bezoekt. Hierdoor wordt geen toestemming meer gevraagd die niet nodig was. Deze maatregel is per 1 september 2024 ingeregeld.

3. Risico: Doordat de 'Vertrouwelijkheid' van de BIV-classificatie op 'Midden' is geselecteerd i.p.v. 'Hoog' is er een aantal maatregelen die (nog) niet goed worden toegepast. Dit betreft: De MFA op de toegang voor docenten. Dit risico kan leiden tot reputatieschade of nadeel voor de betrokkene.
Maatregel: Uitgeverij Deviant bouwt de mogelijkheid in om vanuit de beheerder MFA '*by default'* aan te zetten voor gebruikers. Voor studenten: geen MFA (*inloggen vindt uitsluitend plaats via Entree Federatie*). Hiermee is het risico op onrechtmatige toegang tot een acceptabel niveau gemitigeerd. Deze maatregel is per 1 september 2024 ingeregeld.

4. Risico: Doordat de 'Vertrouwelijkheid' van de BIV-classificatie op 'Midden' is geselecteerd i.p.v. 'Hoog' is er een aantal maatregelen die (nog) niet goed worden toegepast. Dit risico kan leiden tot reputatieschade of nadeel voor de betrokkene. Dit betreft: Het ontbreken van encryptie van de database.

Maatregel: Uitgeverij Deviant zal de dubbele encryptie toepassen op de database. Hiermee is de kans gemitigeerd. Deze maatregel is per 1 januari 2025 ingeregeld.

5. Risico: Logging tot toegang tot persoonsgegevens is ontoereikend.
Maatregel: Uitgeverij Deviant zal een schoolspecifieke functionaliteit aanbieden, bestaande uit de laatste activiteitdatum van een gebruiker voor scholen op de bestaande gebruikersoverzichten. Daarnaast wordt de logging met betrekking tot exports uitgebreid; hierbij wordt zichtbaar wie een export heeft gedownload. Deze gegevens kunnen worden opgevraagd bij de servicedesk. Overige logging is via de servicedesk opvraagbaar en wordt altijd gehonoreerd. Deze maatregel is per 1 september 2024 ingeregeld.

6. Risico: Onrechtmatige toegang tot persoonsgegevens, en beperkte controle over de persoonsgegevens. Exports worden automatisch gedownload. Persoonsgegevens kunnen mogelijk worden ingezien door onbevoegden. Dit risico kan leiden tot reputatieschade of nadeel voor de betrokkene.
Maatregel: Uitgeverij Deviant zal de optie '*automatisch downloaden*' uitzetten. Technisch wordt het mogelijk om dergelijk exportbestand in de browser te openen. Het vereist een extra handeling vanuit school om deze dan in de downloadmap op te nemen. Restrisico op ongestructureerde data blijft aanwezig wanneer er sprake is van onvoldoende uitgedragen beleid en bewustwording binnen school waardoor onzorgvuldig met downloads wordt omgegaan. Deze maatregel is per 1 september 2024 ingeregeld.

7. Risico: Bewaartermijnen worden niet nageleefd. Persoonsgegevens worden te lang bewaard, hetgeen een risico inhoudt voor de rechten en vrijheden van betrokkenen. Bewaartermijnen zijn standaard in de applicatie ingesteld op vier (4) jaar, dit is langer dan noodzakelijk en niet in overeenstemming met de bewaartermijnen zoals gepresenteerd door Kennisnet (2 jaar).
Maatregel: (School) Indien de school zelf de bewaartermijnen bijhoudt en persoonsgegevens op tijd verwijderd uit de applicatie, dan is het restrisico acceptabel. Hiermee is het risico voldoende gemitigeerd.

8. Risico: Privacy-juridische rollen onduidelijk van verwerkingsverantwoordelijke of verwerker. Voor Studiemeter is Uitgeverij Deviant verwerker, zodat er geen toestemming van de betrokkene nodig is. De privacy-juridische rollen van Uitgeverij Deviant lopen door elkaar. Bij het voor de eerste keer inloggen moet je als leerling/docent toestemming geven voor de algemene voorwaarden.
Maatregel: Uitgeverij Deviant verwijdert het 'tussenscherm' akkoord gaan met de Algemene Voorwaarden (AV). Vanaf 1 september 2024 wordt dit gewijzigd en zullen de AV niet meer worden getoond. Hiermee is het risico voldoende gemitigeerd. Deze maatregel is per 1 september 2024 ingeregeld.

9. Risico: Toegangsrechten te ruim ingericht. Het risico is aanwezig dat gebruikers (docenten) gegevens kunnen inzien van leerlingen die niet tot hun kerngroep behoren. Dit heeft als oorzaak dat de bevoegdheden van docenten te ruim kunnen worden ingesteld.
Maatregel: Uitgeverij Deviant kan losse scholen aanmaken t.b.v. het scheiden van de toegang. Uitgeverij Deviant zal hiervoor een duidelijke instructie maken. Deze maatregel is per 1 september 2024 ingeregeld.

10. Risico: Google Analytics 4 (GA4) en een eigen analysetool van Uitgeverij Deviant worden ingezet om gebruikersgegevens te analyseren. Het risico bestaat dat er te veel persoonsgegevens worden verwerkt, zonder dat dit voor de gebruiker duidelijk is, hetgeen leidt tot het aantasten van rechten en vrijheden van betrokkenen.
Maatregel: De privacy-juridische rol van Uitgeverij Deviant bij het gebruik van deze analyticsmethode is die van verwerker. Google heeft de rol van subverwerker. Vanwege deze reden zal Uitgeverij Deviant daarom GA4 en de eigen analytictool en de wijze van gebruik (*en welke gegevens worden gebruikt op een gegranuleerd niveau*) in de lijst van subverwerkers toevoegen. Deze maatregel is per 1 september 2024 ingeregeld.

11. Risico: Ontbreken van een register van verwerkingsactiviteiten bij Uitgeverij Deviant. Kans op het niet goed kunnen uitoefenen van de rechten van betrokkenen omdat onvoldoende inzichtelijk is welke persoonsgegevens verwerker precies voor de verwerkingsverantwoordelijke verwerkt.
Maatregel: Uitgeverij Deviant stelt een register van verwerkingsactiviteiten op. Deze maatregel is per 1 september 2024 ingeregeld.

12. Risico: Onbevoegde toegang tot persoonsgegevens. Hetgeen tot nadeel kan leiden voor de betrokkene. Accounts blijven mogelijk open staan, waardoor onbevoegden toegang kunnen krijgen tot de persoonsgegevens.
Maatregel: (Uitgeverij Deviant) Uitgeverij Deviant gaat aan het gebruikersoverzicht voor beheerders de informatie toevoegen wanneer een gebruiker voor het laatst actief is geweest. (School) De beheerder kan een overzicht van de docenten maken en deze kan gematcht worden met een *‘HR – in dienst – uit dienst lijst’*, zodat er een schoning kan worden doorgevoerd. De uitvoering van de beheersmaatregel ligt dus bij de school voor wat betreft het beheer van autorisaties en handmatige verwijdering.

13. Risico: Risico’s verwerkersovereenkomst. Via de toets verwerkersovereenkomsten is een aantal risico’s gesignaleerd, die in hoofdstuk 18 worden samengevat.
Maatregel: Uitgeverij Deviant zal deze risico’s verder mitigeren en de aanbevelingen doorvoeren. Deze zullen per 1 november 2024 zijn doorgevoerd.

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 (DPIA). In de AVG wordt dit een gegevensbeschermingseffectbeoordeling (GEB) genoemd. Deze DPIA wordt uitgevoerd op een applicatie of verwerking van persoonsgegevens door een leverancier (verwerker). De DPIA wordt uitgevoerd conform de eisen van artikel 35 lid 7 AVG. Bij een DPIA wordt het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens onderzocht. Vastgesteld wordt of het gebruik van persoonsgegevens (verwerking) een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen (leerlingen, hun ouders en medewerkers). De uitkomst van de DPIA is o.a. een rapportage met daarin een overzicht van geclassificeerde risico’s voor de rechten en vrijheden van betrokkenen en mitigerende maatregelen. Mitigerende maatregelen zijn maatregelen die het risico beperken. Alleen indien de hoge risico's voldoende worden beheerst door mitigerende maatregelen, is een gegevensverwerking toegestaan.

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

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

II. Verplichting DPIA

Een DPIA is verplicht als de verwerking van persoonsgegevens - gelet op de aard, de omvang, de context en de doeleinden van die verwerking - waarschijnlijk een hoog risico inhoudt voor de privacy van onderwijsdeelnemers en medewerkers. Ook is het mogelijk dat het uitvoeren van een DPIA verplicht is volgens de regels van de privacytoezichthouder Autoriteit Persoonsgegevens die een lijst gepubliceerd heeft bij welke verwerkingen het uitvoeren van aan DPIA verplicht is[1]. Het schoolbestuur voert door middel van een DPIA voorafgaand aan de verwerking van persoonsgegevens een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

Bij het onderzoek naar het leerplatform Studiemeter (*van de leverancier: Uitgeverij Deviant, makers van online leermiddelen voor het aanleren van basisvaardigheden taal en rekenen*) is gebleken dat het uitvoeren van een DPIA verplicht is om de volgende reden.

Volgens het overzicht van de European Data Protection Board[2] wordt aan twee criteria 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 Studiemeter leer- en testresultaten worden verwerkt over een langere periode en deze resultaten zichtbaar zijn voor gebruikers (*leerkrachten en leerlingen*). Daarnaast heeft deze verwerking van persoonsgegevens betrekking op kinderen onder de 16 jaar. Deze vorm van gegevensverwerking vereist een

---

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

[2] 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).

extra bescherming omdat het hier *kwetsbare personen* betreft. Aldus is er sprake van twee criteria uit de lijst van de WP29 op basis waarvan een DPIA verplicht is om uit te voeren voor de verwerkingsverantwoordelijke bij gebruikmaking van deze applicatie.

Volgens de lijst van de Autoriteit Persoonsgegevens[3] is er tevens sprake van *'15. Profilering'*. Dit gaat om een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op automatische verwerking, zoals bijvoorbeeld *prestaties van leerlingen*. Ook het voldoen aan dit criteria 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 heeft 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?

---

[3] Zie Staatscourant 2019, nummer 64418 van 27 november 2019.

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

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

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

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

In de centrale DPIA worden de punten 1, 2 en 3 uitgevoerd door SIVON. Het schoolbestuur krijgt aanbevelingen voor punt 4 in hoofdstuk 7, Deel E van deze DPIA. 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[4], aangevuld met onderwijsspecifieke informatie uit de *Handleiding uitvoeren data protection impact assessment (DPIA) voor het po en vo (versie 1.0)*[5]. Het model is daarnaast aangepast aan specifieke informatie over het systeem en aangevuld met een model lokale DPIA.

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

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

Deze DPIA bestaat derhalve uit 5 delen:

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

VI. Scope van deze DPIA

Deze DPIA heeft betrekking op de digitale leeromgeving 'Studiemeter', die door Uitgeverij Deviant als leverancier wordt geleverd aan scholen voor het voorgezet onderwijs. Kinderen, leerlingen in het voortgezet onderwijs, maken gebruik van deze leermethode. De risico’s die het gebruik van dit digitale leermiddel met zich meebrengen worden in deze DPIA geïnventariseerd. Op basis van de risico’s wordt nagegaan of de juiste maatregelen worden toegepast om deze risico’s te minimaliseren, zodat een veilig gebruik van Studiemeter mogelijk is.

Studiemeter is een leerplatform voor het aanleren van basisvaardigheden voor taal en rekenen.

---

[4] rapportagemodel-dpia-rijksdienst-v2-0-aangepast-cf-toegangscontrole.docx (live.com)

[5] https://aanpakibp.kennisnet.nl/app/uploads/Handreiking-DPIA-v1.0-1.pdf

Via Studiemeter hebben leerlingen en docenten van de onderwijsinstelling, toegang tot al het door hen bestelde lesmateriaal. Dit omvat *Nederlands en Rekenen*, als ook aanvullend digitaal lesmateriaal bij alle methodes van Uitgeverij Deviant. Dit aanvullend lesmateriaal bestaat uit extra oefeningen, toetsen, methodeonafhankelijke niveautesten, examentrainingsprogramma's en educatieve games. Studiemeter biedt een online oefen- en toetsplatform aan voor leerlingen die hierbinnen opdrachten (individueel) en het aanvullend digitaal lesmateriaal kunnen uitvoeren.

Studiemeter beoogt hiermee om bij te dragen aan de verbetering van de studieresultaten en het bevorderen van zelfstandig leren. Daarnaast kunnen leerlingen behaalde resultaten direct inzien. En ook heeft de leraar inzicht in de voortgang en resultaten van leerlingen. Op basis van de resultaten van het gebruik van digitale leermiddelen kan de onderwijsinstelling zelf conclusies trekken over de leerontwikkeling van leerlingen.

Link naar uitgever en/of productpagina: www.uitgeverij-deviant.nl.

Doelgroep: Middelbaar beroepsonderwijs, primair- en voortgezet onderwijs. Deze DPIA gaat over het Voortgezet Onderwijs (VO).

Gebruikers: leerlingen, leraren en intern begeleiders.

De scope van deze DPIA beperkt zich tot de verwerking van persoonsgegevens in het kader van het gebruik van het online oefen- en toetsplatform Studiemeter voor het VO.

VII. Buiten scope

De scope is beperkt tot de diensten van Uitgeverij Deviant in het kader van het programma 'Studiemeter'.

Buiten scope is:

- Het kunnen uitwisselen van leer- en testresultaten met leerling administratiesystemen van de onderwijsinstelling;
    - *NB: Ten tijde van het uitvoeren van deze DPIA zijn er vanuit Studiemeter geen technische mogelijkheden om te koppelen met leerling administratiesystemen.*
- Het kunnen uitwisselen van leer- en testresultaten met dashboards die de onderwijsinstelling in gebruik heeft;
    - *NB: Ten tijde van het uitvoeren van deze DPIA zijn er vanuit Studiemeter geen technische mogelijkheden om te koppelen met eigen dashboards van onderwijsinstellingen.*
- 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.

  - *NB: Hier is ten tijde van het uitvoeren van deze DPIA niet eerder door een schoolinstelling gebruik van gemaakt.*

- Het aankoopproces van schoolboeken en andere producten in de rol van docent of leerling.

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

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 en 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;
- Uitvoeren van testscript bij leverancier;
- Opstellen rapportage;
- Overleg met leverancier over (aanvullende) maatregelen.

De centrale DPIA is uitgevoerd in de periode oktober 2023 t/m januari 2024 door SIVON, in samenwerking en afstemming met vertegenwoordigers van Uitgeverij Deviant. Na deze periode heeft een analyse van de resultaten van de DPIA-sessies met de leverancier plaatsgevonden en zijn er nadere vragen gesteld aan de leverancier. Op basis van de verkregen antwoorden is verdere invulling gegeven aan de DPIA. De samenwerking met Uitgeverij Deviant is zeer goed verlopen. Er is sprake geweest van constructieve besprekingen. Gesignaleerde verbeteringen zijn goed opgepakt en daar zijn afspraken over gemaakt. Zie hiervoor hoofdstuk 6, maatregelen.

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 worden ook soms servicegegevens genoemd.]

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

Gevoelige persoonsgegevens gaan over gegevens die volgens de Autoriteit Persoonsgegevens (AP) snel inbreuk (kunnen) maken op de persoonlijke levenssfeer. Het gaat bijvoorbeeld om leerresultaten van kinderen, omdat daar conclusies aan kunnen worden verbonden met gevolgen voor het latere maatschappelijke leven. Of het gaat om grote verzamelingen van informatie van (zeer) jonge kinderen, gegevens over (problematische) gezinssituatie of[6] 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

---

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

wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere betrokkenen. Denk hierbij aan minderjarigen en etnische minderheden. De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader.

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

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

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

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

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

Pseudonieme persoonsgegevens Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eisen verbonden dat de sleutels apart worden bewaard en dat maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.
Of pseudonieme gegevens door de ontvanger (verwerker) als persoonsgegevens aangemerkt moeten worden hangt af van de omstandigheden van het geval. Het uitvoeren van een toets zal kunnen uitwijzen in hoeverre deze door de leverancier te herleiden zijn tot persoonsgegevens[7].

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

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

Via Studiemeter hebben leerlingen en docenten van de onderwijsinstelling toegang tot al het door hen bestelde lesmateriaal (*Nederlands en Rekenen*), alsmede aanvullend digitaal lesmateriaal bij alle methodes van Uitgeverij Deviant. In dit online oefen- en toetsplatform vinden leerlingen de te maken opdrachten (individueel) en extra oefeningen, toetsen, methodeonafhankelijke niveautesten, examentrainingsprogramma’s en educatieve games.

Daarnaast kunnen leerlingen behaalde resultaten direct inzien. Ook heeft de leraar eenvoudig inzicht in de voortgang en resultaten van leerlingen.

Via een inlog via Entree kunnen leerlingen en docenten via een combinatie van inlognaam en wachtwoord (eventueel via Single Sign On/2FA/MFA) de leeromgeving van Studiemeter

---

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

bereiken. Nadat de gebruiker is ingelogd kan deze gebruik maken van de functionaliteit van het online oefen- en toetsplatform. Hierbij worden persoonsgegevens verwerkt, zoals in deze DPIA weergegeven.

2. Persoonsgegevens

Betrokkenen

In Studiemeter worden persoonsgegevens verwerkt van leerlingen van de onderwijsinstelling en van medewerkers (docenten en begeleiders) van de onderwijsinstelling.

Persoonsgegevens

De volgende typen persoonsgegevens worden in Studiemeter verwerkt.

Persoonsgegevens	Medewerker	Minderjarigen
Algemene contact- gegevens	X	X
Feiten en waarderingen over iemand zijn gedragingen, eigenschappen of opmerkingen		
Overige contact- gegevens	X	X
Personeelsnummer		
Nationaliteit en geboorteplaats		
Gezondheidsgegevens (op eigen verzoek t.b.v. beheersmaatregel)		
Godsdienst (op eigen verzoek t.b.v. beheersmaatregel)		
Gesprekscyclus (documenten)		
Ervaringen (werkervaring en opleidingen)		X
Gegevens met betrekking tot financiën		
Beeldmateriaal		
Verzuimregistratie		
BSN		
Overige gegevens • ECK-iD: Studiemeter gebruikt Entree Federatie dus ook ECK-iD. Nodig om te koppelen aan een eigen user-id. • Sectornaam: VO, VSO, MBO.	X	X

• Klassencode: in de applicatie zelf (dan weet de leraar wie er in de klas zit). • Leerresultaten (*oefenopgave, toetsresultaten*). • Diagnostische gegevens* • Logginggegevens**		

* Session ID (*niet herleidbaar naar de individuele gebruiker*), Browser, Browser versie, Applicatieversie (Studiemeter), Handeling, tijdstip en URL. GA4[8] wordt door Uitgeverij Deviant gebruikt voor het genereren van analytische en gegranuleerde gegevens voor productverbetering. Hiervoor is inzicht nodig in welke browsers, devices en resoluties Studiemeter wordt gebruikt. Uitgeverij Deviant heeft daarnaast een eigen custom analytics methode ontwikkeld dat extra inzicht geeft in hoe gebruikers door de applicatie heen navigeren (klikken), hiervoor worden geen cookies geplaatst. Dit wordt voor analyse doeleinden gebruikt. Dit om bijvoorbeeld te beslissen: deze pagina wel/niet meer gebruiken.

Het gebruik van GA4 is als volgt: Als een betrokkene inlogt dan worden er geen Cookies geplaatst en er vindt geen opslag van analytics data plaats. Pas als de gebruiker in de leeromgeving komt, dan wordt GA4 gebruikt. Uitgeverij Deviant heeft aangetoond d.m.v. printscreens dat GA4 standaard met de meest uitgeklede functies wordt gebruikt. GA4 wordt '*anoniem*[9]' gebruikt. Google verwerkt geen persoonsgegevens van de betrokkene als verwerkingsverantwoordelijke. Uitgeverij Deviant heeft de instellingen zo ingesteld dat er geen gegevens worden gedeeld met Google. Google is subverwerker bij het gebruik door Uitgeverij Deviant van GA4. Hierdoor is het voor Google – indien Uitgeverij Deviant geen gegevens deel met Google – niet toegestaan gegevens voor '*eigen gebruik*' aan te wenden. Er vindt vanuit Uitgeverij Deviant geen analyse plaats op de gebruiker. Er wordt alleen gekeken hoeveel gebruikers bepaalde pagina's gebruiken. GA4 wordt gebruikt om 'generieke' informatie te verzamelen (*niet op individu niveau*) over het gebruik van Studiemeter. De retentietermijn is 14 maanden. Voor beide analytictools is volgens Uitgeverij Deviant het IP-adres (*dat geanonimiseerd wordt in GA4*) het enige persoonsgegeven dat wordt verwerkt (*maar nooit opgeslagen door Uitgeverij Deviant*).

De privacy-juridische rol van Uitgeverij Deviant bij het gebruik van deze analyticmethode is die als verwerker. Vanwege deze reden zal Uitgeverij Deviant daarom GA4 en de eigen analytictool en de wijze waarop GA4 wordt gebruikt (en welke gegevens worden gebruikt op een gegranuleerd niveau) nog toevoegen in de lijst van subverwerkers van de verwerkersovereenkomst.

SIVON heeft naar aanleiding van de toelichting van Uitgeverij Deviant geen reden te veronderstellen dat dit – gegranuleerde - gebruik van GA4 door Uitgeverij Deviant niet is toegestaan. De Autoriteit Persoonsgegevens heeft zich nog niet uitgelaten over het gebruik van Google Analytics.

** Logging: Uitgeverij Deviant genereert loginformatie. Deze loginformatie is thans nog niet beschikbaar in een bruikbare vorm voor de onderwijsinstelling. Uitgeverij Deviant zal hiervoor per 1 september 2024 een schoolspecifieke functionaliteit aanbieden, bestaande uit de laatste activiteitdatum van een gebruiker voor scholen op de bestaande gebruikersoverzichten. Daarnaast wordt de logging met betrekking tot exports uitgebreid; hierbij wordt zichtbaar wie een export heeft gedownload. Deze gegevens kunnen worden opgevraagd bij de servicedesk. Overige logging is via de servicedesk opvraagbaar en wordt altijd gehonoreerd.

---

[8] GA4 staat voor 'Google Analytics 4'. Het anonimiseren van IP adressen gebeurt automatisch. Het delen van gegevens met Google is door Uitgeverij Deviant uitgezet.

[9] Het anonimisering van IP adressen gebeurt automatisch; '*In Google Analytics 4, IP masking is not necessary since IP addresses are not logged or stored*.' Zie: https://support.google.com/analytics/answer/9019185#IP&zippy=%2Cin-this-article%2Cin-dit-artikel.

Overzicht tabel

De hiervoor genoemde informatie wordt samengebracht in één tabel:

Categorie betrokkene	Categorie persoonsgegevens	Persoonsgegeven	Bron/verkrijging persoonsgegeven
(Minderjarige) leerlingen	Algemene contactgegevens	- Voornaam - Tussenvoegsel - Achternaam	SSO-dienst Entree Federatie, of eigen invoer
	Overige contactgegevens	- E-mailadres leerling - Studentnummer - Schoolnaam - Brincode	SSO-dienst Entree Federatie, of eigen invoer
	Overige gegevens	- Sectornaam - Klassencode - ECK-iD - Leerresultaten (oefenopgave, toetsopgave en toetsresultaten)	SSO-dienst Entree Federatie, of eigen invoer
Medewerker	Algemene contactgegevens	- Voornaam - Tussenvoegsel - Achternaam	SSO-dienst Entree Federatie, of eigen invoer
	Overige contactgegevens	- E-mailadres docent - Schoolnaam - Brincode	SSO-dienst Entree Federatie, of eigen invoer
	Overige gegevens	- Sectornaam - Klassencode	SSO-dienst Entree Federatie, of eigen invoer

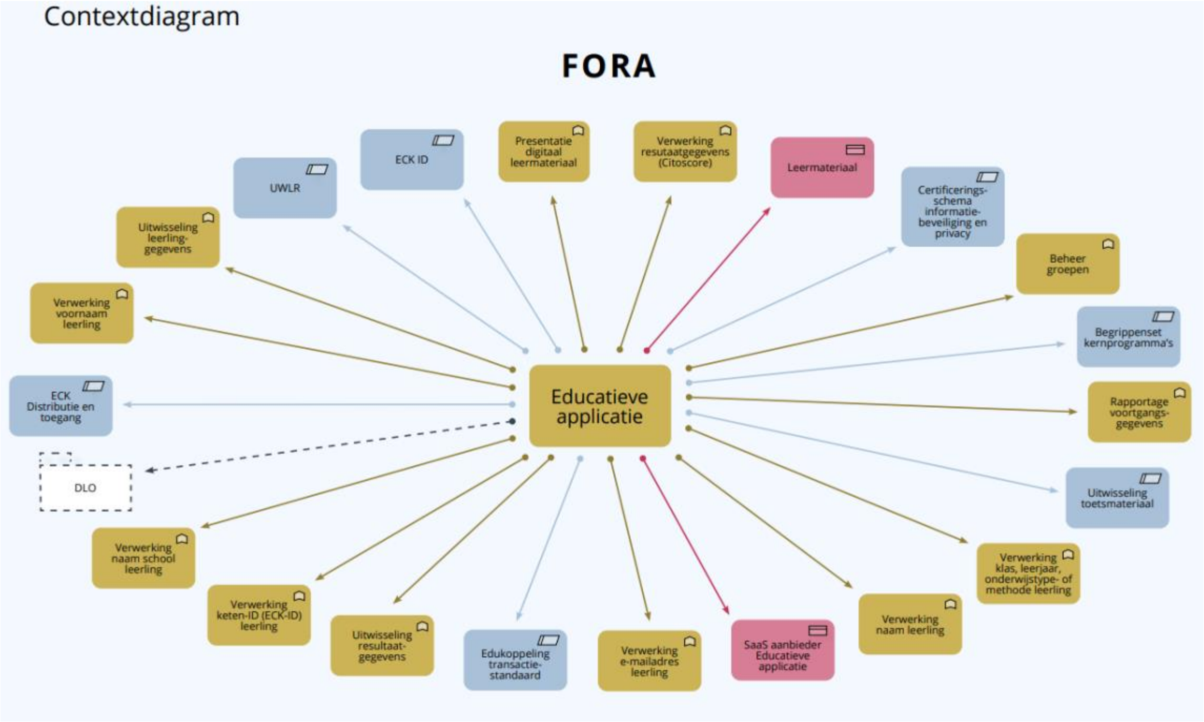
De persoonsgegevens worden rechtstreeks van betrokkenen (*leerlingen en medewerkers*) verkregen bij de inschrijving op de school of indiensttreding, alsmede door het invoeren van eigen gegevens.

3. Gegevensverwerkingen

Voor het schetsen van de scope van de gegevensverwerkingsanalyse wordt gebruik gemaakt van de referentiearchitectuur (de FORA[10] voor het primair en voortgezet onderwijs).

De verwerkingen binnen Studiemeter 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 begeleiden.

Studiemeter kan in termen van FORA worden geduid als ‘Educatieve applicatie’.



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

In de verwerkersovereenkomst staan de verwerkingen opgesomd. Deze staat ook aan de basis van de scope bepaling van deze DPIA, zie onderdeel 2. VII van deze DPIA. Raadpleging van de FORA (*zie hierboven weergegeven afbeelding ‘Contextdiagram*[11]’) heeft geen aanleiding gegeven tot het verder uitbreiden van de scope. De binnen de FORA vastgelegde elementen omvatten de elementen zoals deze in de scope van de DPIA zijn meegenomen.

Bij het gebruik van de digitale leermiddelen voor het voortgezet onderwijs vinden altijd de volgende verwerkingen plaats, in lijn met artikel 5 van het Convenant Digitale Onderwijsmiddelen en Privacy:

- De opslag, analyse en interpretatie van leer- en testresultaten;
- Het terugontvangen door de onderwijsinstelling van leer- en testresultaten;

---

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

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

• De beoordeling van leer- en testresultaten om leerstof en toetsmateriaal te verkrijgen of aan te bieden, dat is afgestemd op de specifieke leerbehoefte van een leerling;

• Het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;

• Het verkrijgen van toegang tot de aangeboden digitale leermiddelen, waaronder de identificatie, authenticatie en autorisatie;

• De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik, en het voorkomen van inconsistentie en onbetrouwbaarheid in de verwerkte persoonsgegevens;

• De continuïteit en goede werking van het digitale leermiddel, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning.

Adaptiviteit

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

Optionele verwerkingen bij digitale leermiddelen voor het voortgezet onderwijs.

Bij het gebruik van de digitale leermiddelen voor het voortgezet onderwijs kunnen met specifieke toestemming van de onderwijsinstelling ook andere verwerkingen plaatsvinden.

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

Het betreft de volgende verwerkingen, en deze zijn buiten de scope van deze DPIA (zie 2. VI, scope):

• Het kunnen uitwisselen van leer- en testresultaten met leerling administratiesystemen van de onderwijsinstelling;

> *NB: Hier wordt ten tijde van het uitvoeren van de DPIA geen gebruik van gemaakt.*

• Het kunnen uitwisselen van leer- en testresultaten met dashboards die de onderwijsinstelling in gebruik heeft;

> *NB: Hier wordt ten tijde van het uitvoeren van de DPIA geen gebruik van gemaakt.*

• Het beschikbaar stellen van gegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan digitale onderwijsmiddelen;

• Het door de Onderwijsinstelling 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.

> *NB: Hier wordt ten tijde van het uitvoeren van de DPIA door geen enkele onderwijsinstelling gebruik van gemaakt en is nog nooit door Uitgeverij Deviant toegepast.*

Applicatielandschap

In deze DPIA ligt de focus op de applicatie Studiemeter. In het applicatielandschap van een schoolbestuur kunnen vanuit de applicatie koppelingen worden gelegd met andere applicaties. De andere applicaties vallen niet binnen de scope van deze DPIA.

[School: geef hier aan het applicatielandschap. etc.].

Koppelingen

Voor wat betreft de koppeling met Entree geldt de onderstaande overzichtsplaat*.

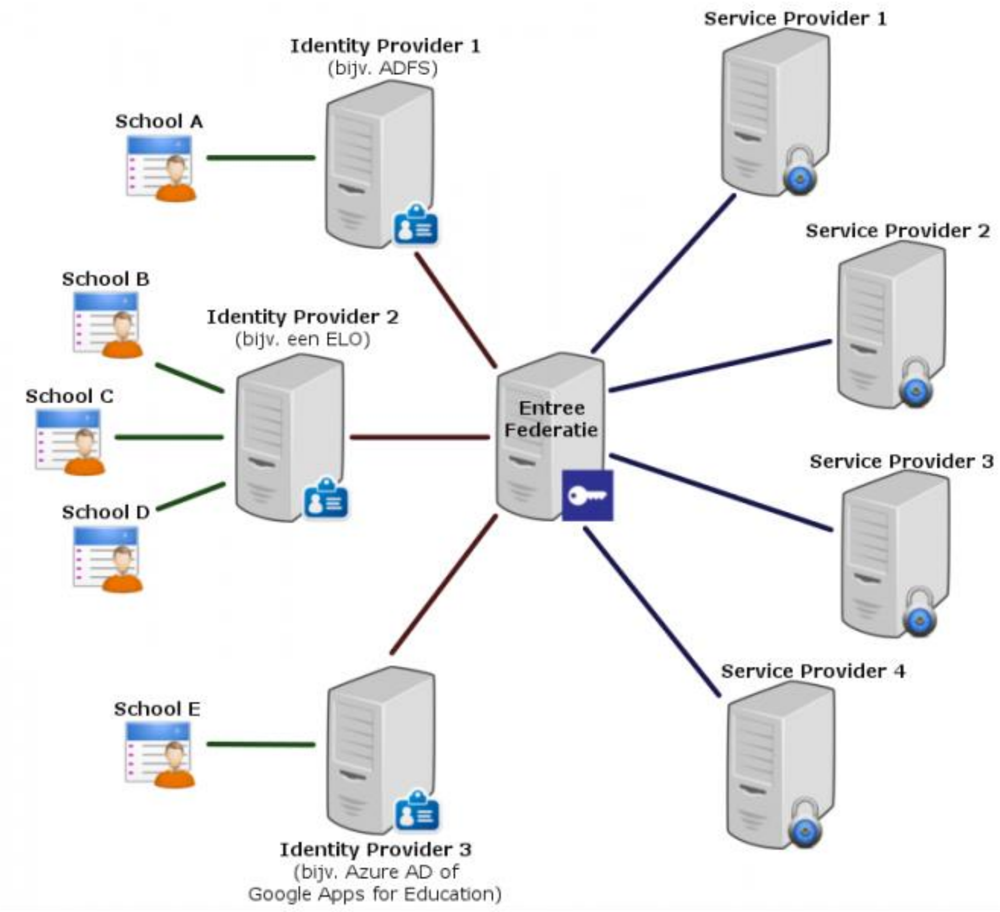
Entree Federatie geeft gebruikers in het VO en MBO toegang tot een groot aantal educatieve diensten met slechts één login (ook wel bekend als Single Sign On of SSO). De federatie wordt gevormd door aanbieders van een educatieve dienst of content (service Providers), beheerders van identiteiten (Identity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

Een Identity Provider is de applicatie die voor de school de communicatie met Entree Federatie verzorgt. Voorbeelden van Identity Providers zijn:

- Elektronische Leeromgevingen (een centrale digitale omgeving die meestal door meerdere scholen wordt gebruikt);
- Active Directory Federation Service (ADFS), zoals Microsoft;
- Google Apps for Education;
- Azure AD.

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

Studiemeter biedt een educatieve dienst aan en kan daarom worden beschouwd als een 'Service Provider'.



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

Bovenstaande visualisatie laat zien hoe Entree Federatie (SSO t.b.v. VO en MBO) zich verhoudt tot Studiemeter als service provider ten aanzien van het tot stand komen van toegang tot digitaal lesmateriaal.

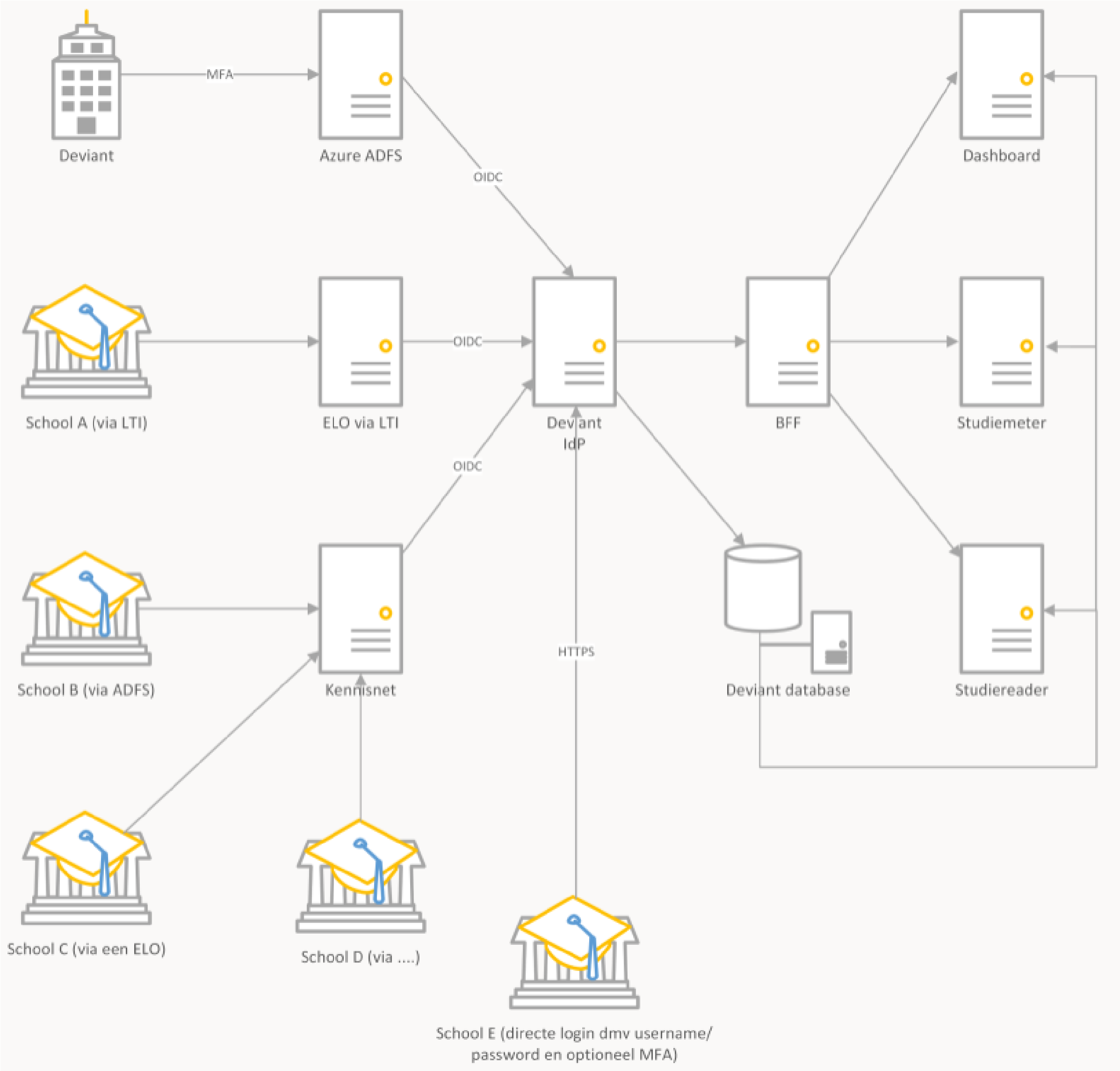
Hierbij is nog belangrijk te benadrukken dat ten tijde van het uitvoeren van deze DPIA, Studiemeter zelf niet beschikt over een 2FA/MFA toegang. De toegang via een 2FA/MFA kan alleen gerealiseerd worden via een koppeling met Entree, waarbij de onderwijsinstelling ervoor zorgt dat deze via 2FA/MFA is ingesteld. De toegang via 2FA/MFA wordt in deze DPIA als een belangrijke beheersmaatregel gezien, omdat de applicatie Studiemeter veel gevoelige persoonsgegevens bevat, waaronder leerresultaten over een langere periode. Deze worden door de Autoriteit Persoonsgegevens[12] gezien als '*profilering*'.

Gegevensstromen/stroomschema

Uitgeverij Deviant heeft de onderstaande architectuurschets aangeleverd.

---

[12] Zie: https://www.autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia; Staatscourant 2019, nr. 64418, 27 november 2019, onderdeel 15. Profilering: Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering), zoals bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.



Toelichting terminologie:

- **ADFS** = Active Directory Federation Services. Met deze techniek worden organistatieaccounts aan andere systemen gekoppeld, en wordt ervoor gezorgd dat de toegang centraal beheerd kan worden voor meerdere applicaties. Voor Uitgeverij Deviant betekent dit dus dat als iemand wil inloggen op Studiemeter dit met een werkaccount moet gebeuren. Als de organisatie het werkaccount stopzet, of de rechten inperkt verliest de gebruiker ook direct toegang tot Studiemeter.

- **LTI** = Learning Tools Interoperability, een standaard met afspraken hoe te communiceren en gegevens uit te wisselen tussen een onderwijsinstelling en een leersysteem. Een koppeling die gebruik maakt van LTI wordt altijd in opdracht van de onderwijsinstelling gerealiseerd. Zie: Learning Tools Interoperability | 1EdTech.

- **BFF** = Backend for Frontend. Dit is de applicatie waarmee Studiemeter communiceert naar de backend diensten (database en identity provider) van Studiemeter. De naam komt van het architectuurpatroon, dit zorgt voor een veilige communicatie tussen een webapplicatie en de systemen van Uitgeverij Deviant. Je kunt dit terugzien in de applicatie als je het netwerkverkeer bekijkt, praktisch alle communicatie verloopt via het domein 'bff.uitgeverij-deviant.nl'.

- **OIDC** = Open ID Connect Protocol. Een veelgebruikt authenticatie protocol om te bepalen wie een gebruiker is en waar deze toegang tot heeft.

4. Verwerkingsdoeleinden

De verwerkingsdoeleinden sluiten aan bij de in het Privacyconvenant[13] 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.
Inkoop en contractbeheer Ict-ondersteuning Onderwijsuitvoering	Het geleverd krijgen / in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier.	Inkoop Beheer ict-middelen (Toegang tot) aanbod leermateriaal.
Onderwijsuitvoering Ict-ondersteuning	Het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie.	(Toegang tot) aanbod leermateriaal Beheer identiteiten Authenticatie en autorisatie.
Informatiebeveiliging en privacy	De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de met	

---

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

	behulp van het Digitale Onderwijsmiddel Verwerkte Persoonsgegevens.	
Ict-ondersteuning (Inkoop en contractbeheer)	De continuïteit, verbetering en goede werking van het Digitale Onderwijsmiddel in opdracht van de Onderwijsinstelling conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het aanbrengen van verbeteringen onder andere na geconstateerde fouten of onjuistheden, en het krijgen van ondersteuning.	Beheer ict-middelen (Contractbeheer).

5. Betrokken partijen

De hieronder genoemde organisaties zijn betrokken bij de volgende 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
Uitgeverij Deviant / Studiemeter	Verwerker	Aanbieder digitaal leermateriaal	Alle genoemde persoonsgegevens	Ontvanger	Binnen Uitgeverij Deviant is een autorisatiematrix vastgesteld waarbij toegang op basis van 'need to know' toegang wordt verkregen. De systeembeheerder heeft geen toegang tot de persoonsgegevens in de database.

True B.V.	Subverwerker	Hostingpartij	Alle genoemde persoonsgegevens	Ontvanger	Geen toegang tot de persoonsgegevens in de database.
Google GA4	Subverwerker	Analyse (anoniem) gebruik t.b.v. verbeteringen	Geen.	Ontvanger	Beheerder / onderzoekers.

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 Uitgeverij Deviant en haar subverwerkers hebben, is het leveren van een goed werkende digitale omgeving waarin leermiddelen en toetsen kunnen worden aangeboden.

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

7. Verwerkingslocaties

De gegevensverwerkingen vinden plaats in Nederland (EER).

Partijnaam	Statutaire vestigings-plaats (sub-) verwerker	Beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt verwerkt door deze subverwerker	Plaats/land van opslag en verwerking persoonsgegevens en doorgifte mechanisme indien buiten de EER
Uitgeverij Deviant	Amersfoort	Leverancier/verwerker	Nederland
True B.V.	Amsterdam	Hostingprovider	Nederland
Google Analytics	USA, CA	GA4, op anonieme wijze	USA

8. Data Transfer Impact Assessment (DTIA)

De verwerkingen vinden alle in Nederland (binnen de EER) plaats. Er is daarom geen noodzaak tot het uitvoeren van een DTIA. Wat betreft GA4 (Google) kan worden opgemerkt dat deze dienst door Uitgeverij Deviant wordt gebruikt binnen de leeromgeving voor analysedoeleinden: productverbetering. De Nederlandse Autoriteit Persoonsgegevens heeft in onderzoek of deze dienst[i] in strijd is met de beginselen van de AVG. Vooralsnog is het gebruik hiervan niet verboden in Nederland. Het delen van gegevens ‘data’ met Google is door Uitgeverij Deviant uitgezet. Uitgeverij Deviant zal het gebruik van GA4 en de eigen analysetool opnemen in de verwerkersovereenkomst. Zie hoofdstuk 3, onder punt 2 voor een verdere uitleg van het gebruik van GA4 door Uitgeverij Deviant.

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. Daarvoor is in het kader van deze DPIA geïnventariseerd welke beveiligingsmaatregelen (moeten) worden toegepast om de persoonsgegevens te beveiligen. In Hoofdstuk 3 is al aangegeven dat de onderwijsinstelling zelf moet borgen dat de toegang tot Studiemeter wordt voorzien van een 2FA/MFA toegang via Entree.

Voorts is er technisch onderzoek verricht naar Studiemeter. Dit onderzoek geeft geen aanleiding tot nadere verbeterpunten, omdat Uitgeverij Deviant de Cookie pop up, voor de leeromgeving, gedurende het uitvoeren van deze DPIA heeft uitgeschakeld.

Status van informatiebeveiliging

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

Uit dit onderzoek is de volgende informatie verkregen:

- Er wordt door Uitgeverij Deviant een BIV classificatie[14] toegepast voor de applicatie Studiemeter op het niveau H-H-M. Dit betekent dat Uitgeverij Deviant de ‘Vertrouwelijkheid’ van de persoonsgegevens beoordeeld als ‘Midden’. Vanuit SIVON is aangegeven dat er sprake is van een Vertrouwelijkheidsscore ‘Hoog’. Dit vanwege het feit dat in de applicatie sprake is van ‘*profilering*’ conform de omschrijving van de Autoriteit Persoonsgegevens[15]:

  15. Profilering
  Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering), zoals bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.

  Hierbij gaat de Autoriteit Persoonsgegevens duidelijk in op het verwerken van persoonsgegevens van *kwetsbare jongeren* in een geautomatiseerd systeem dat toetsresultaten en andere persoonsgegevens verwerkt. Dit wordt vervolgens *profilering* genoemd en gelabeld als een ‘*hoog risico verwerking’*, waarbij de juiste technische en organisatorische maatregelen moeten worden toegepast.

---

[14] BIV staat voor ‘Beschikbaarheid, Integriteit en Vertrouwelijkheid. Deze drie categorieën ‘B, I en V’ worden op basis van de ROSA certificering ingedeeld in drie niveaus: ‘laag’, ‘midden’ of ‘hoog’.

[15] Zie: https://www.autoriteitpersoonsgegevens.nl/documenten/lijst-verplichte-dpia; Staatscourant 2019, nr. 64418, 27 november 2019, onderdeel 15. Profilering: Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering), zoals bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.

Hierdoor is een discrepantie in de beoordeling van de maatregelen op het niveau van Vertrouwelijkheid 'Hoog' ten opzichte van de score door Uitgeverij Deviant gedaan op basis van de ROSA, waarbij Uitgeverij Deviant uitkomt op een 'Midden'.

Dit heeft tot gevolg dat de volgende maatregelen ontbreken:

  - 2FA toegang (*deze is wel te realiseren via Entree en SSO vanuit de onderwijsinstelling*). 2FA wordt nu niet afgedwongen maar kan per medewerker worden geactiveerd. Dit dient echter verplicht gesteld te worden door de beheerder.
  - Encryptie van de database (dubbele encryptie) welke ontbreekt.
  - Uitgebreide loggingfunctionaliteit.

- Studiemeter is ISO27001 gecertificeerd. DigiTrust Certificaat ISO 27001, inclusief een 'Verklaring van toepasselijkheid' (VVT). Studiemeter beschikt over een Informatiebeveiligingsbeleid, en ISMS. De toegang van medewerkers tot het systeem is gereguleerd via een proces van logische toegangsbeveiliging en een autorisatiematrix. 2FA toegang is via Single Sign On ingeregeld voor medewerkers van Uitgeverij Deviant. Medewerkers hebben op basis van een '*need to know'* toegang.

- Jaarlijks wordt de omgeving van Studiemeter aan een Security Audit onderworpen. De meest recente is van mei 2022. Tevens is een security rapport door een externe partij uitgebracht. Het resultaat en de beoordeling door SIVON is als volgt:

  - Uit de uitgevoerde penetratie test zijn geen hoog risicobevindingen geconstateerd, en drie 'middel hoog' risico's. De pentest bevindingen zijn geregistreerd en de opvolging is bewaakt. De laatste bevinding is in september 2022 opgelost (4 maanden na de pentest).

- Via de inlogpagina voor Studiemeter (*dit betekent de inlogpagina voor studenten/leerlingen en docenten*) wordt de gebruiker gevraagd om akkoord te gaan met de '*algemene voorwaarden'*. Hierbij worden tevens Cookies geplaatst. Hier zal Uitgeverij Deviant een onderscheid moeten maken voor de verwerking van persoonsgegevens via de 'commerciële website', waarbij Uitgeverij Deviant verwerkingsverantwoordelijke is, en de portal voor gebruikers waarbij zij gebruik maken van het leermiddel/toetssysteem Studiemeter. In deze laatste variant is Uitgeverij Deviant verwerker en kan de gebruiker niet gevraagd worden om akkoord te gaan met voorwaarden. In de besprekingen met Uitgeverij Deviant is door Uitgeverij Deviant besloten om dit scherm in de toekomst niet meer te zullen gebruiken. Derhalve worden er geen Cookies geplaatst en wordt er geen 'akkoord' meer gevraagd aan de betrokkene die Studiemeter gebruikt die door de onderwijsinstelling wordt aangeboden.

- Uitgeverij Deviant heeft een adequaat back-up beleid. Het back-up beleid voldoet aan alle vereisten zoals benoemd in het ROSA model.

- Uitgeverij Deviant past logging toe. De logging functionaliteit is op dit moment summier. Het ontbreken van adequate logging kan resulteren in het verlies van belangrijke audittrailgegevens die nodig zijn om te achterhalen wie toegang heeft gehad tot persoonsgegevens, wanneer dit is gebeurd en welke handelingen zijn uitgevoerd. De logging functionaliteit is thans beperkt tot de informatie inhoudende door welke gebruikers records worden opgevraagd. Deze loggegevens zijn niet door de onderwijsinstelling te benaderen, maar hiervoor moet een support medewerker bijstand verlenen. Daarnaast is er geen logging op de exportfunctionaliteit. Hierdoor ontbreekt het aan informatie welke gebruiker, welke exports heeft uitgevoerd. De loginformatie is thans nog niet beschikbaar in een bruikbare vorm voor de onderwijsinstelling. Uitgeverij Deviant zal hiervoor per 1 september 2024 een schoolspecifieke functionaliteit aanbieden, bestaande uit de laatste activiteitdatum van een gebruiker voor scholen op de bestaande gebruikersoverzichten. Daarnaast wordt de logging met betrekking tot exports uitgebreid; hierbij wordt zichtbaar wie een export heeft gedownload. Deze gegevens kunnen worden opgevraagd bij de servicedesk. Overige logging is via de servicedesk opvraagbaar en wordt altijd gehonoreerd.
- Studiemeter beschikt niet over een ‘mailfunctionaliteit’. Wel kan de docent intern binnen het systeem berichten sturen naar een leerling en vise versa. Tevens kunnen er intern berichten worden gestuurd naar de helpdesk.
- Metadata. Uitgeverij Deviant maakt gebruik van ‘metadata’ door gebruikmaking van GA4 en een eigen analysetool. Voor een beschrijving hiervan wordt verwezen naar hoofdstuk 3, onder punt 2 en naar de getroffen maatregelen (zie hoofdstuk 19).

IAMA: mensenrechten in beeld bij algoritmes

Er wordt door Uitgeverij Deviant binnen de applicatie Studiemeter geen gebruik gemaakt van AI technologie.

10. Juridisch en beleidsmatig kader

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
Leermiddelen (inzet van)	Algemeen belang o.b.v. onderwijswetgeving. Wet op het Voorgezet onderwijs (WVO 2020)	2.91 sub a WVO 2020 en *8.17 lid 10 WVO 2020*
Digitaal afnemen van toetsen	Algemeen belang o.b.v. onderwijswetgeving.	2.91 sub a WVO 2020 en *8.17 lid 10 WVO 2020*

	Wet op het Voortgezet onderwijs (WVO 2020)	
Inzet van leermiddelen en het digitaal afnemen van toetsen via een externe leverancier (als ketenpartner)	Normenkader IBP Normenkader IBP	Hoofdstuk 15, Ketenbeheer

11. Bewaartermijnen

De verkregen persoonsgegevens in digitale leermiddelen worden na verloop van tijd gewist. In de tabel hieronder staan de bewaartermijnen.

Binnen de applicatie van Studiemeter worden de persoonsgegevens door de verwerker verwijderd na vier (4) jaar na de laatste gebruikersactiviteit. Deze bewaartermijn is 'hard' in het systeem van Studiemeter ingevoerd maar kan worden aangepast door de school. De bewaartermijn van vier jaar hoeft dus niet overeen te komen met het eigen bewaartermijnenbeleid van de onderwijsinstelling. Het is echter mogelijk dat de onderwijsinstelling de eigen bewaartermijnen hanteert en doorvoert in de applicatie. Gegevens zullen dan handmatig moeten worden verwijderd.

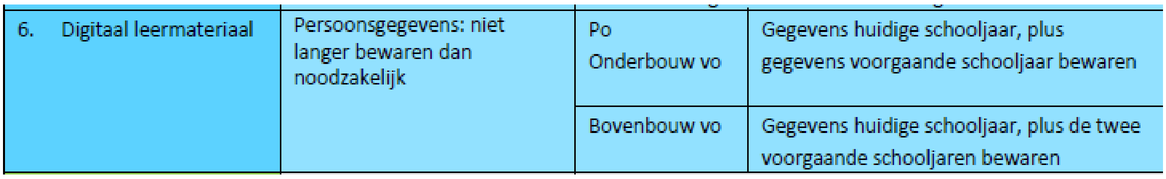
Gegevensverwerking	**Verwerkingsdoeleinde**	**Categorie persoonsgegevens**	**Bewaartermijn en grondslag**
Gebruikersgegevens, oefen- & toetsresultaten, inlogactiviteit	*Inzetten van leermiddelen en toetsen*	*Gewoon en gevoelig (studieresultaten over een langere periode)*	*Volgens de leverancier: 4 jaar na de laatste activiteit van de gebruiker* *Dit wordt gemotiveerd door Uitgeverij Deviant:* *Als de student later een vervolgstudie doet, zijn de resultaten nog beschikbaar. Hiermee vindt een behoud plaats van de studieresultaten t.b.v. een vervolgopleiding. De school kan zelf kiezen voor een minder lange termijn. Dat moet dan handmatig worden uitgevoerd.* *NB: De school kan ervoor kiezen om zelf de bewaartermijn korter te stellen, maar dan moet de school dit handmatig doen.*

			Na de vier jaar geldt dat de persoonsgegevens door het systeem zelf worden verwijderd: De hele keten vanaf het eerste leerjaar tot het laatste wordt verwijderd vanaf het moment dat het laatste jaar is afgerond.
Gebruikersgegevens, oefen- & toetsresultaten, inlogactiviteit	*Gegevens back – up (beveiligingsmaatregel)*	*Gewoon en gevoelig (studieresultaten over een langere periode)*	Iedere 2 uur wordt een backup gemaakt van de data. Deze worden 48 uur bewaard. Dagelijkse backups worden 30 dagen bewaard. Wekelijkse backups worden 5 weken bewaard. Maandelijkse backups worden 1 jaar bewaard. Drie maandelijks wordt een restore getest om te kijken of de backups functioneren. Redundantie: Uitgeverij Deviant heeft een active-passive configuratie waarbij de passive het overneemt bij uitval zonder dataverlies. Alle backups worden off-site opgeslagen (andere datacentrum)

Volgens de handreiking bewaartermijnen van Kennisnet[16] zijn op de persoonsgegevens die binnen Studiemeter worden verwerkt de volgende bewaartermijnen van toepassing. Deze termijnen kunnen door de onderwijsinstelling handmatig worden doorgevoerd in Studiemeter.

---

[16] Zie Kennisnet: Tijdelijke handreiking bewaartermijnen po/vo 1.2 (december 2020).



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

SIVON adviseert hierbij de onderwijsinstellingen de cijfers op te nemen in het LAS en niet verder langdurig te verwerken in de leeromgeving, zoals die van Studiemeter. Dit betekent dat de bewaartermijn beperkt kan worden tot het (jaarlijkse) moment waarop de relevante leerresultaten in het LAS zijn opgenomen. Hierdoor wordt het risico voor de rechten en vrijheden van betrokkenen, dan mogelijk iemand onbevoegd toegang krijgt tot deze gegevens verder geminimaliseerd.

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

Bepaal op welke grondslag(en) de gegevensverwerkingen zijn gebaseerd.

Artikel 6 AVG lid 1

- a) Toestemming van de betrokkene
- b) Uitvoering van een overeenkomst
- c) Wettelijke verplichting[17]
- d) Vitaal belang van de betrokkene
- **e) Taak van algemeen belang[18] (of openbaar gezag)**
- f) Gerechtvaardigd belang

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

Zie voor een overzicht van de grondslagen tevens Hoofdstuk 10, het beleids- en juridische kader.

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.

In deze '*Juridische paragraaf*' wordt uiteengezet wat de wettelijke grondslag is in relatie tot de doelen in het kader van het po en vo voor wat betreft het aanbieden van leermiddelen. Daarna wordt behandeld op welke wijze dit kan worden uitgevoerd met inachtneming van de beginselen vanuit de AVG.

AVG

Artikel 6 van de AVG geeft een zestal verwerkingsgrondslagen welke gebruikt kunnen

---

[17] De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn.

[18] Met betrekking tot de rechtsgrond taak van algemeen belang geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak persoonsgegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak ook worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

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 voortgezet onderwijs (WVO 2020). 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 WVO 2020 aangewezen)om deze taak uit te voeren.

AVG

Artikel 6

Lid 1: De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

Sub e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

Wet voortgezet onderwijs 2020

In de sectorspecifieke wetgeving die 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.[19]

Het is het schoolbestuur vrij welke (leer)middelen zij daarvoor inzet, deze kunnen zowel digitaal, fysiek als hybride zijn. Uit Artikel 8.17 lid 10 Gebruik persoonsgebonden nummer door bevoegd gezag, WVO 2020 volgt impliciet dat een onderwijsinstelling in het kader van haar taken digitale leermiddelen mag inzetten.

De AVG schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. Er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen voor de vervulling van een taak van algemeen belang. De relevante wetgeving in de WVO 2020 sluit aan op de verwerkingen die plaatsvinden binnen Studiemeter omdat dit een digitaal leermiddel en toetssysteem betreft, dat de noodzakelijke ondersteuning biedt voor de uitvoering van leertaken.

---

[19] Zie hiervoor de aanhef en WVO 2020 artikel 1.4: Karakter en doelen voortgezet onderwijs.
'Het onderwijs wordt zodanig ingericht dat de leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen. Het wordt afgestemd op de voortgang in de ontwikkeling van de leerlingen.'

Artikel 2.89 van de WVO 2020 *'Onderwijskundig beleid'* biedt daarmee een solide basis voor de gegevensverwerkingen die binnen het gebruik van Studiemeter plaatsvindt. De gegevensverwerking is op basis van de genoemde wetgeving dan ook rechtmatig.

> *Wet op het voortgezet onderwijs 2020*
>
> Artikel 2.91 sub a WVO 2020
>
> Schoolplan: Stelsel van kwaliteitszorg
>
> Sub a. *Het bewaken dat leerlingen een ononderbroken ontwikkelingsproces kunnen doorlopen en dat het onderwijs wordt afgestemd op de voortgang in de ontwikkeling van leerlingen, bedoeld in artikel 1.4 lid 2.*
>
> *Sub b. Het vaststellen van welke maatregelen ter verbetering nodig zijn.*
>
> *Artikel 8.17 lid 10 WVO 2020*
>
> *Het bevoegd gezag kan het pseudoniem gebruiken voor het genereren van een ander pseudoniem voor een leerling in het kader van de toegang tot en het gebruik van digitale leermiddelen of het digitaal afnemen van toetsen en examens, waarbij het bevoegd gezag er zorg voor draagt dat dit andere pseudoniem wordt bewaard in de systemen waarin de leerlingen zijn geregistreerd. Dit andere pseudoniem wordt uitsluitend verstrekt aan een leverancier die een digitaal product of een digitale dienst aanbiedt bestaande uit leerstof of toetsen en de daarmee samenhangende digitale diensten.*

Gegevensverwerkingen	**Juridisch en/of beleidsmatig kader**	**Wetsartikelen**
Leermiddelen (inzet van)	Algemeen belang o.b.v. onderwijswetgeving. Wet op het Voorgezet onderwijs (WVO 2020)	2.91 sub a WVO 2020 en *8.17 lid 10 WVO 2020*
Digitaal afnemen van toetsen	Algemeen belang o.b.v. onderwijswetgeving. Wet op het Voortgezet onderwijs (WVO 2020)	2.91 sub a WVO 2020 en *8.17 lid 10 WVO 2020*
Inzet van leermiddelen en het digitaal afnemen van toetsen via een externe leverancier (als ketenpartner)	Normenkader IBP Normenkader IBP	Hoofdstuk 15, Ketenbeheer

Voor wat betreft de voorgenomen verwerking van persoonsgegevens door onderwijsinstellingen, via de leverancier van het platform Studiemeter van Uitgeverij Deviant, wordt in het onderstaande uiteengezet wat de regels zijn omtrent het aanbieden van leermiddelen en het afnemen van toetsen in het voortgezet onderwijs (hierna ook: VO), en in het verlengde daarvan de verwerking van persoonsgegevens.

Er is dus een grondslag '*algemeen belang o.b.v. onderwijswetgeving'* om digitale leermiddelen in te zetten. Deze kan gevonden worden in artikel 6, eerste lid, sub e, van de AVG jo artikel 8.17 lid 10 WVO 2020.

De conclusie is dat de verwerking van persoonsgegevens bij het inzetten van een leermethode zoals Studiemeter kan plaatsvinden op grond van artikel 6 lid 1 sub e AVG (*algemeen belang, o.b.v. onderwijswetgeving*, zoals in deze paragraaf beschreven).

Verwerking/doeleinde (zie hiervoor 4. Verwerkingsdoeleinden)	**Grondslag AVG**	**Toelichting**
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.	Artikel 6, eerste lid, sub e, van de AVG jo artikel 8.17 lid 10 WVO 2020. Taak van algemeen belang (of openbaar gezag)[20].	De conclusie is dat het inzetten van een leermethode zoals Studiemeter is toegestaan op grond van artikel 6 lid 1 sub e AVG (*algemeen belang, o.b.v. onderwijswetgeving*).

---

[20] De conclusie is dat het inzetten van een leermethode zoals Studiemeter is toegestaan op grond van artikel 6 lid 1 sub e AVG (algemeen belang, o.b.v. een wettelijke verplichting, zijnde de WVO 2020, zoals in deze paragraaf beschreven).

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.		

13. Bijzondere persoonsgegevens

In het kader van de verwerking van persoonsgegevens via de leer- en toetsapplicatie van Studiemeter worden er geen strafrechtelijke persoonsgegevens verwerkt. Wel worden er ‘bijzondere’ persoonsgegevens verwerkt, in de zin van dyslexie en auditieve beperking. Deze gegevens worden echter door Uitgeverij Deviant omgezet in neutrale termen, zoals: ‘Extra tijd’, of ‘ondertiteling gewenst ja/nee'.

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

14. Doelbinding

In het kader van de verwerking van persoonsgegevens via de leer- en toetsapplicatie van Studiemeter worden er geen persoonsgegevens verwerkt voor een ander doel dan oorspronkelijk verzameld.

15. Kinderrechten-afweging (Best Interests Assessment Children)

Artikel 3 van het Verdrag inzake de rechten van het kind, schrijft voor dat bij alle maatregelen betreffende kinderen - *ongeacht of deze worden genomen door openbare of particuliere instellingen, rechterlijke instanties, bestuurlijke autoriteiten of wetgevende lichamen* - de belangen van het kind de eerste overweging (moeten) vormen. Deze belangenafweging gaat verder dan een veilige gegevensverwerking maar ziet ook op de mogelijke gevolgen van de verwerking. Met schoolbesturen als leden van SIVON in het primair en voortgezet onderwijs, betekent dit dat SIVON in haar DPIA's rekening houdt met 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 Studiemeter 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[21]. 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[22] van en voor kinderen relevant zijn in het kader van deze DPIA. Van belang is de leeftijd van de kinderen (leeftijdsadequaat). Hierbij wordt nagegaan of de gegevensverwerking (negatieve) gevolgen heeft voor de ondersteuning en van de behoeften van het kind op het gebied van veiligheid, gezondheid, welzijn, familierelaties, fysieke, psychologische en emotionele ontwikkeling, identiteit, vrijwaring van economische commerciële en/of fysieke uitbuiting, vrijheid van meningsuiting, privacy en de mogelijkheid om een eigen mening te vormen en deze te laten horen, het belang van toegang tot informatie, omgang met anderen en spel (buiten spelen) om de ontwikkeling van het kind te ondersteunen. Het gaat erom dat het kind in overeenstemming met zijn of haar ontwikkelende capaciteiten, een stem heeft (kan hebben) in zaken die hem of haar aangaan.

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

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

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

- 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.

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

Studiemeter beschikt wel over een zogenaamde ‘*inkijkfunctie*’. Deze functie betreft een functie om vanuit de docentrol te kijken wat een leerling precies heeft gedaan om een vraag op te lossen. Het is een manier om het door de leerling gemaakte werk te kunnen bekijken. Dit betreft een voor onderwijskundige doeleinden belangrijke functie. De docent kan bijvoorbeeld hiermee inzicht krijgen hoe de leerling tot een antwoord komt. Hiervoor is voor bijvoorbeeld Rekenen binnen Studiemeter een veld beschikbaar waarin de leerling uitschrijft hoe deze tot een conclusie komt. Door inzage in dit veld kan de docent de leerling helpen tot verbeterde inzichten te komen. Het betreft geen meekijkfunctie in de zin van het ‘live’ meekijken of een andersoortige ‘proctoring’ functie. De conclusie is dat deze inkijkfunctie geen inbreuk maakt op wezenlijke rechten van het kind. Deze digitale inkijkfunctie verschilt niet van bijvoorbeeld het in een schrift bekijken hoe de leerling tot een bepaalde conclusie komt. Het is hierdoor niet noodzakelijk de leerling er via een ‘privacyverklaring’ op te wijzen dat het werk kan worden ingezien: er wordt niet ‘live’ meegekeken worden.

3. Beoordeel of dit effect wenselijk is

Zoals onder punt 2 vermeld, lijken er geen negatieve gevolgen te zijn voor het gebruik van Studiemeter. Studiemeter 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.

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 Studiemeter 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 Studiemeter 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[14] voor de leerling.

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

De opsomming van verwerkingen en soorten persoonsgegevens zijn hierbij noodzakelijk om het leerplatform op de gewenste manier te kunnen gebruiken.

16. b. Proportionaliteit en subsidiariteit

De onderwijsinstelling is verantwoordelijk voor de uitvoering van goed onderwijs volgens de bepalingen van de Wet op het voortgezet onderwijs 2020. Hierbij staat de inbreuk op de persoonlijke levenssfeer in evenredige verhouding tot de verwerkingsdoelen, namelijk het waarborgen van een ononderbroken ontwikkelingsproces met behulp van (digitale) leermiddelen. Vanwege het feit dat via een autorisatiebeheer alleen medewerkers van de onderwijsinstelling (en de leverancier) 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 Studiemeter aan leerlingen aan te kunnen bieden.

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

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

De onderwijsinstelling die gebruik maakt van Studiemeter dient op haar website een duidelijke privacyverklaring en een privacyreglement opgenomen te hebben. Hierin staat beschreven welke rechten betrokkenen hebben betreffende de verwerking van hun Persoonsgegevens en hoe men hun rechten kan uitoefenen.

Uitgeverij Deviant ondersteunt de onderwijsinstelling bij het voldoen aan de verplichtingen van de verwerkingsverantwoordelijke om te voldoen aan de rechten van betrokkenen[21]. Verzoeken van de onderwijsinstelling worden via *privacy@uitgeverij-deviant.nl* in behandeling genomen. Daar wordt geverifieerd of de vragende instelling een accounthouder is bij Uitgeverij Deviant. Indien dit het geval is en de verwerkingsverantwoordelijke is geverifieerd worden persoonsgegevens verstrekt.

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

---

[21] Zie Hoofdstuk III van de AVG ‘Rechten van de betrokkene’, artikel 12 – 23 AVG.

Recht van betrokkene	Toelichting procedure	Evt. beperking verwerking*
Het recht op informatie	De onderwijsinstelling dient als verwerkingsverantwoordelijke te zorgen voor een: • Openbaar gepubliceerde privacyverklaring op de website.	n.v.t.
Het recht van inzage	Studiemeter kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht op rectificatie	Studiemeter kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht op gegevenswissing	Studiemeter kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht op beperking van de verwerking	Studiemeter kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens	Studiemeter kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht op overdraagbaarheid van gegevens	Studiemeter kan op verzoek van de instelling dit recht waarborgen.	n.v.t.
Het recht van bezwaar	Studiemeter kan op verzoek van de instelling 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 te vinden via de volgende link: Zie: https://sivon.nl/toetsen-verwerkersovereenkomsten-2/.

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	**Vraag of opmerking richting Leverancier**	**Reactie Leverancier**
Naam/Versie/Datum aangeboden verwerkersovereenkomst	Klopt het dat de datum verwerkt is in de bestandsnaam (nl. 20220909)? Graag tevens een versie opnemen.	Uitgeverij Deviant neemt een versienummer op.
Toets - Bijlage 1: Privacybijsluiter	**Vraag of opmerking richting Leverancier**	**Reactie Leverancier**
• Contactgegevens (e-mailadres, telefoonnummer)	Voor contactgegevens van de Onderwijsinstelling wordt verwezen naar de optionele Bijlage 4. Dat is niet wenselijk, want optioneel. Graag in Bijlage 1 ook ruimte reserveren voor contactgegevens van Onderwijsinstelling (conform Model 4.0).	Uitgeverij Deviant zal altijd de contactgegevens van de onderwijsinstelling opnemen.
Het meest recente versienummer van de Privacybijsluiter en de datum daarvan worden hier vastgelegd.	Graag tevens een versie opnemen.	Uitgeverij Deviant neemt een versienummer op.
• Naam Verwerker en vestigingsgegevens	Naam en plaats is voldoende. Volledige adres is beter.	Uitgeverij Deviant neemt het volledige adres op.
• Link naar productpagina (website/URL)	Het is geen link naar de productpagina's, maar via de link naar de leverancier in het menu en de optie Digitaal leren kom je wel op de productpagina's.	Uitgeverij Deviant neemt link naar productpagina op: https://www.uitgeverij-deviant.nl/studiemeter.
a. omschrijving van producten en/of diensten en bijbehorende Verwerkingen die een onlosmakelijk onderdeel vormen van het aangeboden product en/of de aangeboden dienst, inclusief de koppelingen en uitwisseling met derde partijen;	In plaats van Verwerkingen (geen onderscheid tussen onlosmakelijk onderdeel en optioneel) zijn hier Doeleinden opgesomd.	Uitgeverij Deviant neemt duidelijker op wat onlosmakelijk verbonden is (product/dienst, verwerking en doeleinden) en wat optioneel is.
b. omschrijving van aanvullende optionele producten en/of diensten en bijbehorende Verwerkingen die de Verwerker aanbiedt, inclusief de koppelingen en uitwisseling met derde partijen.	In plaats van Verwerkingen (geen onderscheid tussen onlosmakelijk onderdeel en optioneel) zijn hier Doeleinden opgesomd.	Uitgeverij Deviant neemt duidelijker op wat onlosmakelijk verbonden is (product/dienst, verwerking en doeleinden) en wat optioneel is.

In dit onderdeel wordt vastgelegd welke doeleinden, zoals vastgelegd in artikel 5 van het Convenant, van toepassing zijn op de Verwerking van Persoonsgegevens met behulp van de specifieke producten en/of diensten.	Niet volgens indeling en nummering Privacy Convenant. Doeleinden zoals vastgelegd in artikel 5 van het Privacy Convenant worden niet altijd 1-op-1 overgenomen (voor afwijkingen/opmerkingen zie Gegevensverwerkingsanalyse - tabblad Doeleinden).	Uitgeverij Deviant heeft de Doeleinden van de brancheorganisatie overgenomen. Afgesproken is dat SIVON hierover contact zoekt met de brancheorganisatie.
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 zijn niet expliciet opgenomen, maar goed te koppelen aan Gebruikers bij punt 1. Categorieën Persoonsgegevens zijn onvoldoende helder, o.a. door het gebruik van 'worden ... *in ieder geval* de volgende gegevens verwerkt'. Komen ook niet overeen met de gestandaardiseerde categorieën zoals gebruikt in Model 4.0. Graag deze als standaard gebruiken. Mogelijk nog zaken toevoegen bij 'Anders, nl. ...' zoals Vrijstelling (zie bijv. https://www.uitgeverij-deviant.nl/digitaal-leren/opstarten-in-studiemeter/). Als Gebruikers-id wordt op de website gesproken over de Uitgeverij Deviant-id of Studentnummer (zie bijv. https://www.uitgeverij-deviant.nl/digitaal-leren/opstarten-in-studiemeter/ of https://idp.uitgeverij-deviant.nl/). Is dit hetzelfde? Zo ja, graag duidelijk aangeven.	Uitgeverij Deviant zal persoonsgegevens duidelijker specificeren. Uitgeverij Deviant zal onderscheid duidelijk maken.

2. door de Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen).	Door deze opsomming van categorieën lijkt het alsof er andere persoonsgegevens zijn die niet worden verwijderd of teruggegeven. Graag geen onderscheid maken en conform Model 4.0 opnemen. Er wordt geen onderscheid gemaakt tussen de bewaartermijn i.v.m. Artikel 12.1 en Artikel 12.2 van de VWO (dus na aflopen onderliggende overeenkomst). Bewaartermijn i.v.m. Artikel 12.1 is voorbehouden aan de Onderwijsinstelling. Bewaartermijn i.v.m. Artikel 12.2 mag (in plaats van de opgenomen 4 jaar, indien daarvoor bedoeld) aangepast worden naar een gangbare 3 maanden (na einde contract).	Bewaartermijn van 4 jaar is gebaseerd op artikel 12.1 (na uitschrijving leerling/student dan wel inactiviteit) en op afspraken binnen het mbo. Indien gegevens eerder verwijderd moeten worden, kunnen daar afspraken op initiatief van onderwijsinstelling over gemaakt worden. Er is geen bewaartermijn opgenomen voor artikel 12.2 (is einde overeenkomst). Uitgeverij Deviant zal dit nader opnemen.
Onder G. wordt vastgelegd wat de plaats(en)/land(en) van opslag en Verwerking van de Persoonsgegevens zijn.	De Servicedesk blijkt ook bereikbaar via WhatsApp van WhatsApp LLC (onderdeel van Meta Platforms Inc. voorheen Facebook). Graag Locatie van opslag en Verwerking Persoonsgegevens vermelden. Google (GA4) is niet opgenomen in de verwerkersovereenkomst.	Uitgeverij Deviant neemt dit op in de verwerkersovereenkomst.

Verwerker legt hier vast van welke Subverwerkers hij ten tijde van het afsluiten van de Verwerkersovereenkomst gebruikmaakt.	De Servicedesk blijkt ook bereikbaar via WhatsApp van WhatsApp LLC (onderdeel van Meta Platforms Inc. voorheen Facebook). Graag opnemen. Google (GA4) is niet opgenomen in de verwerkersovereenkomst. Worden de volgende leveranciers zoals genoemd in de Privacyverklaring van Uitgeverij Deviant gebruikt voor Studiemeter? Zo ja, graag toevoegen, inclusief de locatie van opslag en verwerking bij het vorige punt G. + MailChimp + Microsoft (Office 365) + WordPress	Uitgeverij Deviant neemt dit op in de verwerkersovereenkomst. Uitgeverij Deviant neemt dit op in de verwerkersovereenkomst. Uitgeverij Deviant neemt dit op in de verwerkersovereenkomst (MailChimp wordt niet gebruikt, MS365 wel).
Toets - Bijlage 2: Beveiligingsbijlage	**Vraag of opmerking richting Leverancier**	**Reactie Leverancier**
Het meest recente versienummer van deze bijlage en de datum daarvan worden hier vastgelegd.	Graag tevens een versie opnemen.	Uitgeverij Deviant neemt een versienummer op.
Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden. Verwerker gebruikt hiervoor in beginsel het ‘Certificeringsschema informatiebeveiliging en privacy ROSA’ (te vinden op www.edustandaard.nl) als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy.	NB: Na aanpassing van de classificatie van de Vertrouwelijkheid van midden naar hoog dient ook de bijlage hierop aangepast te worden.	Uitgeverij Deviant zal dit hogere niveau binnen afzienbare termijn realiseren. Zie maatregelen en de verdere uitwerking hiervan in de risico’s en maatregelen van de DPIA.

Inlogpagina	Dit is waarschijnlijk de inlogpagina voor docenten, toch? URL voldoet wel aan moderne en veilige internetstandaarden. Dat geldt ook netjes voor de inlogpagina voor onderwijsdeelnemers, namelijk: idp.uitgeverij-deviant.nl. Op de website wordt ook verwezen naar www.studiemeter.nl (als doorverwijzing naar de bovengenoemde inlogpagina) en deze voldoet niet helemaal aan de standaarden. HSTS vraagt om aandacht, zie: https://internet.nl/site/www.studiemeter.nl/2580706/#control-panel-5 Indien ook vanuit @studiemeter.nl wordt gemaild (bijv. nieuwsbrief of na contact servicedesk), graag daar ook aandacht voor DMARC. Zie: https://internet.nl/mail/studiemeter.nl/1123423/	Is de inlogpagina voor zowel docenten als onderwijsdeelnemers. Uitgeverij Deviant maakt daarvoor een aanpassing. Er wordt niet gemaild vanuit @studiemeter.nl maar vanuit uitgeverij-deviant.nl waarin DMARC goed is ingeregeld.
Toets - Bijlage 3: Wijzigingenbijlage (indien van toepassing)	**Vraag of opmerking richting Leverancier**	**Reactie Leverancier**
Het meest recente versienummer van deze bijlage en de datum daarvan worden hier vastgelegd.	Bijlage 3 is geen optionele bijlage. Ook al zijn er geen wijzigingen tov het MEVW-model, graag toch opnemen. PS Bijlage 4 is wel een optionele bijlage.	Uitgeverij Deviant volgt de brancheorganisatie. Afgesproken wordt dat er contact wordt gezocht met de brancheorganisatie.

Uitgeverij Deviant zal de verbeteringen doorvoeren per 1 november 2024.

Voor wat betreft de verwerkersovereenkomst geldt dat Uitgeverij Deviant is aangesloten bij de MEVW. De MEVW heeft eigen bijlagen vastgesteld, welke door de Convenantpartijen zijn overeengekomen. Deze bijlagen zijn echter summier ten opzichte van de ‘modelbijlagen’ van het Convenant 4.0, welke veel meer gedetailleerde informatie bevatten. Dit punt zal verder worden besproken tussen de Convenantspartijen.

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

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

Beoordelingskader risico's

Alle mogelijke risico's van de gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen worden beschreven en afgewogen. Het gaat hierbij om de negatieve gevolgen die de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, de oorsprong van deze gevolgen, de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden: kans (waarschijnlijkheid) X impact (ernst) = risico.
Negatieve gevolgen van de gegevensverwerking zijn bijvoorbeeld:

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

De methodiek die wordt gevolgd, is beschreven door de Britse toezichthouder[22] om risico's te classificeren. Hierbij wordt een objectieve inschatting gemaakt van de kans en impact van negatieve gevolgen (eventuele fysieke, emotionele of materiële schade).

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

---

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

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

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

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

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

Aan de in deze DPIA voor Studiemeter genoemde onderstaande risico’s ligt een complete risico-inventarisatie ten grondslag, welke is gebaseerd op de SIVON methodiek: de DPIA vragenlijst voor de leverancier, een beoordeling van de ROSA certificering en een bredere scan op het gebied van informatiebeveiliging, het beoordelen van de verwerkersovereenkomst en een gestandaardiseerde risicomatrix. Alleen de belangrijkste risico’s die resteren zijn hieronder weergegeven.

Toelichting MAPGOOD-methode

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

- **M**ens – de mensen die nodig zijn om het informatiesysteem te beheren en gebruiken, denk aan: directe en indirecte gebruikers, en functioneel en technisch applicatiebeheer.
- **A**pparatuur – de apparatuur die nodig is om het informatiesysteem te laten functioneren, denk aan: webserver, applicatieserver, beheer van werkplekken en werkplekken van gebruikers.
- **P**rogrammatuur – de programmatuur waaruit het informatiesysteem bestaat, denk aan: de diverse applicaties die gebruikt worden.
- **G**egevens – de gegevens die door het systeem worden verwerkt, denk aan: basisregistraties, financiële verantwoording en vergunningen.

- **O**rganisatie – de organisatie die nodig is om het informatiesysteem te laten functioneren, denk aan: beheer-, gebruikers- en ontwikkelorganisatie.
- **O**mgeving – de omgeving waarbinnen het informatiesysteem functioneert, denk aan: locatie, serverruimte en werkplekken.
- **D**iensten – de externe diensten die nodig zijn om het systeem te laten functioneren, denk aan: technisch systeembeheer, netwerkinfrastructuur en onderhoudscontracten met externe dienstverleners.

Risicotabel:

Risico nr.	Mapgood	Risico-omschrijving	Oorzaak	Kans	Impact	Risico	Proces en/of systeem-risico+ verantwoordelijke
1	G	Dataminimalisatie: er worden te veel persoonsgegevens verwerkt.	Binnen Studiemeter wordt per leerling vastgelegd of er sprake is van ‘dyslectie’ of een ‘auditieve beperking’ Dit is een verwerking van bijzondere persoonsgegevens. Voor de verwerking van deze gegevens is geen grondslag. Dit kan leiden tot discriminatie of uitsluiting van een individu.	3	3	9	Systeem Uitgeverij Deviant
2	P	Het niet kunnen uitoefenen van rechten. Betrokkenen worden niet geïnformeerd over hun rechten en hoe ze deze uit kunnen oefenen. Het risico is dat er gegevens (door derden) worden verwerkt waarvoor geen	Betrokkenen worden onjuist geïnformeerd over de cookies die worden geplaatst Er worden meer of andere cookies geplaatst dan waarvoor toestemming is gegeven dan wel de mogelijkheid om per cookiesoort	3	3	9	Systeem Uitgeverij Deviant

		grondslag aanwezig is. Tevens; Niet toegestane profilering.	toestemming te geven ontbreekt.				
3	S	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregelen toegepast. De beveiliging van de persoonsgegevens in de applicatie is op dit moment hierdoor onvoldoende. Dit risico kan leiden tot reputatieschade of nadeel voor de betrokkene.	Geen multi factor authenticatie. Doordat de ‘Vertrouwelijkheid’ van de BIV classificatie op ‘Midden’ is geselecteerd i.p.v. ‘Hoog’ is er een aantal maatregelen die (nog) niet goed worden toegepast. Dit betreft: De 2FA / MFA op de toegang voor docenten.	3	3	9	Systeem Uitgeverij Deviant
4	S	Onrechtmatige toegang tot persoonsgegevens. Er worden onvoldoende beveiligingsmaatregelen toegepast. Het risico is dat er onvoldoende beveiligingsmaatregelen worden toegepast. Dit betreft: Dit risico kan leiden tot reputatieschade of nadeel voor de betrokkene.	Geen encryptie database. Doordat de ‘Vertrouwelijkheid’ van de BIV classificatie op ‘Midden’ is geselecteerd i.p.v. ‘Hoog’ is er een aantal maatregelen die (nog) niet goed worden toegepast. Dit betreft: Het ontbreken van encryptie van de database.	3	3	9	Systeem Uitgeverij Deviant
5	S	Onrechtmatige toegang tot persoonsgegevens. Het risico is dat er onvoldoende	De loggingfunctionaliteit is ontoereikend.	3	3	9	Systeem Uitgeverij Deviant

		beveiligingsmaatregelen worden toegepast. Dit risico kan leiden tot reputatieschade of nadeel voor de betrokkene.	Er is logging voor wie exports aanmaakt, niet voor wie ze download. Hierdoor is niet te achterhalen wie, wanneer welke data heeft gedownload.				
6	P	Onrechtmatige toegang tot persoonsgegevens. Door exports beperkte controle over de persoonsgegevens. Persoonsgegevens kunnen mogelijk worden ingezien door onbevoegden. Dit risico kan leiden tot reputatieschade of nadeel voor de betrokkene.	Het is mogelijk om een export te maken: dit wordt dan gedownload naar de eigen (OneDrive) omgeving. De naam, achternaam en resultaten van leerlingen zijn dan in een overzicht zichtbaar in een Excel. Door het gebruik van de export en/of download functie komen mogelijk gevoelige persoonsgegevens buiten de applicatie terecht wat verlies van controle over deze data tot gevolg heeft.	3	3	9	Systeem Uitgeverij Deviant
7	P	Bewaartermijnen worden niet nageleefd. Persoonsgegevens worden te lang bewaard, hetgeen een risico inhoudt voor de rechten en vrijheden van betrokkenen.	Persoonsgegevens worden te lang bewaard. Bewaartermijnen zijn standaard in de applicatie ingesteld op vier (4) jaar, dit is langer dan noodzakelijk en niet in	3	3		Systeem Uitgeverij Deviant Tevens: School

			overeenstemming met de bewaartermijn en zoals gepresenteerd door Kennisnet (2 jaar).				
8	P	Privacy-juridische rollen onduidelijk van verwerkingsverantwoordelijke of verwerker. Hier is Uitgeverij Deviant verwerker, zodat er geen toestemming van de betrokkene nodig is.	Privacy-juridische rollen zijn onduidelijk voor gebruiker/betrokkenen. De privacy-juridische rollen van Uitgeverij Deviant lopen door elkaar. Bij het voor de eerste keer inloggen moet je als leerling/docent toestemming geven voor de algemene voorwaarden. Dit heeft het risico in zich dat een gebruiker (leerling/ouder) persoonsgegevens laat verwerken door de leverancier als verwerkingsverantwoordelijke terwijl de applicatie door de school wordt gebruikt en Uitgeverij Deviant een verwerker is.	3	3	9	Systeem Uitgeverij Deviant
9	P	Toegangsrechten te ruim ingericht. Het risico is aanwezig dat gebruikers	Medewerkers hebben (mogelijk) te veel toegang tot andere klassen.	3	3	9	Systeem Uitgeverij Deviant

		(docenten) gegevens kunnen inzien van leerlingen die niet tot hun kerngroep behoren.	Dit heeft als oorzaak dat de bevoegdheden van docenten te ruim kunnen worden ingesteld. Hierdoor hebben te veel gebruikers toegang tot gegevens die niet noodzakelijk zijn.				
10	S	GA4 en een eigen analysetool van Uitgeverij Deviant wordt ingezet om gebruikersgegevens te analyseren.	Het risico bestaat dat er te veel persoonsgegevens worden verwerkt, zonder dat dit voor de gebruiker duidelijk is, hetgeen leidt tot het aantasten van rechten en vrijheden van betrokkenen.	3	3		Systeem Uitgeverij Deviant
11		Gebrekkige controle op verwerking persoonsgegevens door Uitgeverij Deviant.	Ontbreken van een register van verwerkingsactiviteiten bij Uitgeverij Deviant. Kans op het niet goed kunnen uitoefenen van de rechten van betrokkenen omdat onvoldoende inzichtelijk is welke persoonsgegevens verwerker precies voor de verwerkingsverantwoordelijke verwerkt.	3	2	6	Proces Uitgeverij Deviant
12		Onbevoegde toegang tot	Inactieve accounts van	3	3	9	Systeem

		persoonsgegevens. hetgeen tot nadeel kan leiden voor de betrokkene.	medewerkers onvoldoende inzichtelijk. Niet of te laat opschonen van accounts. Triggers hiervoor ontbreekt. Accounts blijven mogelijk open staan, waardoor onbevoegden toegang kunnen krijgen tot de persoonsgegevens. Deze functie is op dit moment niet geautomatiseerd. De beheerder kan een overzicht van de docenten maken en deze kan gematcht worden met een 'HR – in dienst – uit dienst lijst, zodat er een schoning kan worden doorgevoerd. Beheeraccounts kunnen niet verwijderd worden. Als een docent de school verlaat wordt dit soms niet per direct afgesloten.				Uitgeverij Deviant Tevens: School
13		Risico's verwerkersovereenkomst	Zie Hoofdstuk 18 van deze DPIA. Er zijn naast verschillende lage en midden	3	3	9	Proces Uitgeverij Deviant

			risico's (afwijking tov. vereisten) ook hoge risico's (voor de rechten en vrijheden van de betrokkenen) geconstateerd.			🟥	

6. Deel D: Beschrijving voorgenomen maatregelen

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

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

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

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

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

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

Gedacht kan worden aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- *Fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;*
- *Opslag van gegevens in een kluis;*
- *Project-, risico- en incidentenmanagement;*
- *Data opsplitsen;*
- *Dataminimalisatie;*
- *Back-ups;*
- *Integriteitscontroles;*
- *2FA/MFA;*
- *Monitoring en logging;*
- *Controle van toegekende bevoegdheden;*
- *Privacybewustzijn- en beveiligingstrainingen;*
- *Managementrapportages over risicobeheer;*
- *Beperken inzageniveau;*
- *Periodiek een audit of hack- of penetratietest uitvoeren;*
- *Richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;*
- *Responsible-disclosurebeleid;*
- *Geheimhoudingsverklaringen;*
- *Service level agreements (met boeteclausules);*
- *Verwerkersovereenkomsten.*
- *Screening personeel en VOG-verklaring.*

20. Maatregelen

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

Maatregelentabel:

Risico nr.	Omschrijving risico (steekwoord)	Risico	Maatregel(en) (Org/Techn/Jur)	Maatregel voor (Uitgeverij Deviant/school)	Restrisico (cijfer)	Toelichting aanvaardbaarheid restrisico	(datum) maatregel geïmplementeerd?
1	Binnen Studiemeter wordt per leerling vastgelegd of er sprake is van ‘dyslexie’ of een ‘auditieve beperking’ Dit is een verwerking van bijzondere persoonsgegevens. Voor de verwerking van deze gegevens is geen grondslag. Dit kan leiden tot discriminatie of uitsluiting van een individu.	9	Technisch: Verwijderen /aanpassen vragen over dyslexie en auditieve beperking. Voorgesteld alternatief: Andere omschrijving Bijv. ‘Extra tijd’, of ‘ondertiteling gewenst ja/nee'.	Uitgeverij Deviant	0	Er is na het doorvoeren van de maatregelen geen restrisico. De impact is hiermee gemitigeerd.	1 september 2024
2	Er worden meer of andere cookies geplaatst dan waarvoor toestemming is gegeven dan wel de mogelijkheid om per cookiesoort toestemming te geven ontbreekt.	9	Uitgeverij Deviant verwijdert de *‘toestemming pop up’* wanneer de betrokkene de leeromgeving bezoekt. Hierdoor wordt geen toestemming meer gevraagd die niet nodig was.	Uitgeverij Deviant	0	Uitgeverij Deviant verwijdert de pop-up / toestemming. Hiermee is de rol van Uitgeverij Deviant zuiver: verwerker. Hiermee is de kans en de impact van het risico gemitigeerd.	1 september 2024
3	De multifactor-authenticatie (MFA) ontbreekt op de toegang voor docenten.	9	Er is een koppeling met Entree Federatie te maken voor het gebruik van Studiemeter. Om veilige toegang te	Uitgeverij Deviant en school. De School moet zorgen dat de toegang tot het schoolaccoun	0	De school moet ervoor zorgen dat de toegang tot het schoolaccount alleen via MFA mogelijk is.	1 september 2024

			krijgen tot Uitgeverij Deviant via de Entree federatie, moet het schoolaccount multifactor authenticatie (MFA) hebben ingesteld. Zie ook de DPIA op Entree Federatie. Via SSO met de AD van MS-365 is op dit moment MFA niet mogelijk.	t van MFA is voorzien. Indien dit niet mogelijk is, kan de school MFA aanzetten voor de toegang tot Studie-meter voor docenten. De docent kan dit echter weer uitzetten, hetgeen de toegang tot het systeem onveilig maakt.		Voor alle medewerkers van de school wordt MFA by default ingesteld. Uitgeverij Deviant bouwt de mogelijkheid in om vanuit de beheerder MFA ‘by default’ aan te zetten voor gebruikers. Voor studenten: optioneel MFA (inloggen vindt plaats via Entree Federatie). Hiermee is het risico op onrechtmatige toegang tot een acceptabel niveau gemitigeerd.	
4	Onvoldoende encryptie van de database. Dit risico kan leiden tot reputatieschade of nadeel voor de betrokkene.	9	ROSA BIV, V=H geeft aan de dubbele encryptie. Deze kan worden toegepast op de database van Studiemeter.	Uitgeverij Deviant	0	Uitgeverij Deviant zal de dubbele encryptie toepassen op de database. Hiermee is de kans gemitigeerd.	1 januari 2025
5	Logging tot toegang tot persoonsgegevens is ontoereikend. Er is nu alleen logging voor wie exports aanmaakt, niet	9	Uitgeverij Deviant ontwikkelt een loggingmodule, waarmee de logging inzichtelijk wordt voor de school.	Uitgeverij Deviant	0	Daarnaast wordt de logging met betrekking tot exports uitgebreid; hierbij wordt zichtbaar wie een export heeft gedownload.	1 september 2024

	voor wie ze downloadt.		Logging op navraag is thans wel mogelijk.			Deze gegevens kunnen worden opgevraagd bij de servicedesk. Overige logging is via de servicedesk opvraagbaar en wordt altijd gehonoreerd.	
6	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.	9	Het is inmiddels technisch mogelijk om bij het genereren van de PDF de optie ‘automatisch downloaden’ uitzetten. Het direct downloaden in de downloadmap leidt tot mogelijke onbevoegde toegang en persoonsgegevens kunnen onbedoeld te lang bewaard worden. Persoonsgegevens blijven onbeheerd en zijn mogelijk toegankelijk voor anderen. Maatregel: interne richtlijn opstellen en automatisch laten wissen van de downloadmap.	Uitgeverij Deviant en School	0	Uitgeverij Deviant zal de optie automatisch downloaden’ uitzetten. Technisch wordt het mogelijk om dergelijk exportbestand in de browser te openen. Het vereist een extra handeling vanuit school om deze dan in de downloadmap op te nemen. Restrisico op ongestructureerde data blijft aanwezig wanneer er sprake is van onvoldoende uitgedragen beleid en bewustwording binnen school waardoor onzorgvuldig met downloads wordt omgegaan.	1 september 2024

7	Te lang bewaren van persoonsgegevens .	9	De school kan ervoor kiezen om zelf de bewaartermijn korter te stellen, maar dan moet de school dit handmatig doen.	School	0	Indien de school zelf de bewaartermijn en bijhoudt en persoonsgegevens op tijd verwijderd uit de applicatie, dan is het restrisico acceptabel. Hiermee wordt de kans gemitigeerd.	School
8	Privacy-juridische rollen onduidelijk. Dit heeft het risico in zich dat een gebruiker (leerling/ouder) persoonsgegevens laat verwerken door de leverancier als verwerkingsverantwoordelijke (suggestie), terwijl de applicatie door de school wordt gebruikt en Uitgeverij Deviant een verwerker is.	0	Uitgeverij Deviant verwijdert de ‘*toestemmings pop up’* bij het bezoeken van de betrokkene van de leeromgeving. Hierdoor wordt geen toestemming meer gevraagd die niet nodig was.	Applicatie	0	Uitgeverij Deviant verwijdert het ‘tussenscherm’ akkoord gaan met de AV. Vanaf 1 september 2024 wordt dit gewijzigd en zullen de Algemene Voorwaarden (en akkoord daarop) niet meer worden getoond. Hiermee is de kans en impact gemitigeerd.	
9	Te veel gebruikers hebben toegang tot de persoonsgegevens. Dit heeft als reden dat te veel gebruikers autorisaties hebben tot gegevens die niet noodzakelijk zijn.	9	Uitgeverij Deviant kan voor andere markten op dit moment losse scholen aanmaken als de locaties echt gescheiden moet blijven. Tevens kan er een ‘Persoonlijke groep’ worden aangemaakt door de leerkracht,	Uitgeverij Deviant	0	Uitgeverij Deviant kan losse scholen aanmaken t.b.v. het scheiden van de toegang. Uitgeverij Deviant zal hiervoor een duidelijke instructie maken.	1 september 2024

			dan heeft alleen die leerkracht daar toegang toe. NB: *De inregeling nu is ingericht voor het MBO, waar een docent op meerdere locaties kan werken en toegang moet hebben tot de klassen.*				
10	GA4 en een eigen analysetool van Uitgeverij Deviant wordt ingezet om gebruikersgegevens te analysen. Het risico bestaat dat er teveel persoonsgegevens worden verwerkt, zonder dat dit voor de gebruiker duidelijk is, hetgeen leidt tot het aantasten van rechten en vrijheden van betrokkenen.	9	Zie voor een uitleg en gebruik van GA4: hoofdstuk 3 onder punt 2. SIVON heeft naar aanleiding van de toelichting van Uitgeverij Deviant geen reden te veronderstellen dat dit – gegranuleerde - gebruik van GA4 door Uitgeverij Deviant niet is toegestaan. De Autoriteit Persoonsgegevens heeft zich nog niet uitgelaten over het gebruik van Google Analytics. Google heeft hier uitdrukkelijk de rol van (sub)verwerker en mag de	Uitgeverij Deviant	0	De privacy-juridische rol van Uitgeverij Deviant bij het gebruik van deze analyticmethode is die van verwerker. Google heeft de rol van subverwerker. Vanwege deze reden zal Uitgeverij Deviant daarom GA4 en de eigen analytictool en de wijze waarop GA4 wordt gebruikt (en welke gegevens worden gebruikt op een gegranuleerd niveau) deze nog in de lijst van subverwerkers toegevoegd worden.	Toegepast. 1 september 2024

			gegevens nooit voor eigen doelen verwerken.				
11	Ontbreken van een register van verwerkingsactiviteiten bij verwerker.	6	Opstellen van een register van verwerkingsactiviteiten.	Uitgeverij Deviant	0	Uitgeverij Deviant stelt een register van verwerkingsactiviteiten op.	1 september 2024
12	Risico op onbevoegde toegang tot persoonsgegevens, hetgeen tot nadeel kan leiden voor de betrokkene. Niet of te laat opschonen van accounts.	9	De beheerder kan een overzicht van de docenten maken en deze kan gematcht worden met een ‘HR – in dienst – uit dienst lijst’, zodat er een schoning kan worden doorgevoerd.	Uitgeverij Deviant en School	0	Uitgeverij Deviant gaat aan het gebruikersoverzicht voor beheerders de informatie toevoegen wanneer een gebruiker voor het laatst actief is geweest. Beheersmaatregel ligt bij de school, beheer autorisaties en handmatige verwijdering.	1 september 2024
13	Risico’s verwerkersovereenkomst	9	De risico’s zijn alle opgelost, zie hoofdstuk 18.	Uitgeverij Deviant	0	Uitgeverij Deviant zal op alle geconstateerde punten maatregelen nemen (zie kolom Reactie leverancier) waardoor de risico's voldoende worden gemitigeerd en er geen restrisico's zijn.	1 november 2024

7. Deel E: MODEL lokale DPIA

Dit hoofdstuk bevat de afweging die ieder 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 van de gegevensverwerking;
- beoordeling rechtmatigheid van de 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. Overwegingen implementatie en lokale DPIA: aanvullende risico's en maatregelen

In aanvulling op de in de centrale DPIA gevonden risico's en maatregelen, heeft de implementatie en gebruik van Studiemeter binnen [NAAM SCHOOLBESTUUR] verdere gevolgen voor de rechten en vrijheden van de betrokkenen.

[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

Risicotabel 1. Organisatie-specifieke risico's

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

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	Het bestuur heeft een eigen privacy coördinator of privacy officer.		
2	Binnen de organisatie zijn de volgende formele structuren geïmplementeerd: een autorisatiebeleid, toegangsbeheer (2FA toegang tot schoolaccount is ingesteld), toewijzing van verantwoordelijkheden en eigenaarschap betreffende gegevensverwerking.		
3	Het gedetailleerde autorisatiebeleid specificeert welke toegangsniveaus en rechten per medewerker of rol vereist zijn om hun taken uit te voeren. Het autorisatiebeleid wordt regelmatig geëvalueerd en bijgewerkt om te blijven voldoen aan de veranderende behoeften en veiligheidsvereisten van de school.		
4	Het bestuur heeft een (externe) Functionaris Gegevensbescherming.		
5	Het bestuur heeft een datalekprotocol/beleid en past dit actief toe.		

6	Het bestuur heeft een IBP beleid en deze vastgesteld.		
7	Er is een PDCA m.b.t. de AVG waarbij er periodiek wordt gekeken of men compliant is en wat er verbeterd kan worden.		
8	Het bestuur heeft een gedragscode waarin diverse maatregelen voor gedrag en ICT beveiliging is opgenomen.		
9	Het bestuur heeft op elke schoolwebsite een pagina, dan wel een link naar de juiste pagina, over de AVG waarop informatie wordt verstrekt met betrekking tot de verwerking van persoonsgegevens, waaronder het gebruik van digitale leermiddelen (Privacyverklaring).		
10	Er is een actueel proces voor de rechten van betrokkenen.		
11	Ouders en medewerkers kunnen altijd en met succes de rechten van betrokkenen inroepen.		
12	Het bestuur heeft op elke schoolwebsite een pagina, dan wel een link naar de juiste pagina, over de wijze waarop de ouders (of leerlingen > 16 jaar) hun rechten kunnen uitoefenen (Privacyreglement).		

Risicotabel 2. Algemene applicatie specifieke risico's

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

Nr.	Beheersmaatregel	Uitgevoerd?	Opmerking/toelichting
1	De verwerkersovereenkomst met verwerker is gecontroleerd en getekend.		
2	De verwerking is opgenomen in het register van verwerkingen van de onderwijsinstelling.		
3	Het bestuur zal de DPIA van Studiemeter 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. Hierin staat opgenomen of het gebruik van vrije invulvelden noodzakelijk is en zo ja voor welke informatie (dataminimalisatie). Over deze uitgangspunten zijn duidelijk gecommuniceerd met alle medewerkers die gebruik maken van de applicatie.		
5	Het bestuur hanteert de wettelijke bewaartermijnen. De bewaartermijnen zijn vastgesteld en beschreven. *NB: Studiemeter hanteert een bewaartermijn van vier jaar, maar de onderwijsinstelling kan zelf de bewaartermijnen (laten) nakomen.*		
6	Het bestuur zorgt ervoor dat persoonsgegevens na afloop van de bewaartermijn daadwerkelijk worden geschoond en heeft een procedure hiervoor. De logbestanden (m.n. exports) worden periodiek gecontroleerd en de downloadmap wordt periodiek geleegd. *NB: Studiemeter genereert nog geen logbestanden om te kunnen monitoren.*		
7	Het bestuur voldoet aan de transparantieverplichting (artikel 13 en 14 AVG) en geeft de juiste informatie in de privacyverklaring over het gebruik van Studiemeter.		

8	Het bestuur heeft autorisaties ingericht op basis van 'need to know' (role based access).		
9	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.		
10	Gebruikers van de applicatie zijn/worden afdoende geschoold in het gebruik ervan.		
11	Persoonsgegevens worden niet op verkeerde plekken opgeslagen omdat regels en/of bekendheid met Studiemeter dit voorkomt. Er is daarom geen sprake van een schaduwadministratie op verschillende schijven en mappen van medewerkers.		
12	Er is een functioneel beheerder aangewezen voor Studiemeter.		
13	De onderwijsinstelling neemt verantwoordelijkheid voor het veilig koppelen van Studiemeter met een ander systeem zoals een leerlingadministratiesysteem. *NB: Studiemeter koppelt niet met andere systemen.*		
14	Kennis over applicatiebeheer is belegd bij meerdere personen en is gedocumenteerd.		
15	De onderwijsinstelling neemt verantwoordelijkheid om bij het beëindigen van de softwarelicentie de verwerkte persoonsgegevens terug te vorderen van de Verwerker, samen met een schriftelijke bevestiging dat de vernietiging heeft plaatsgevonden.		

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

Nr.	Risico	Te nemen maatregel	Uitgevoerd?	Opmerking/toelichting
1	Docenten kunnen toegang krijgen tot de omgeving van Studiemeter zonder 2FA toegang. Dit leidt tot het risico dat er sprake is van onbevoegde toegang, hetgeen kan leiden tot het schenden van de rechten en vrijheden van betrokkenen.	De onderwijsinstelling zorgt voor 2FA toegang tot het schoolaccount. Wanneer buiten het schoolaccount wordt ingelogd op Studiemeter dan kan dit alleen via multifactor authenticatie.		
2	Exports blijven te lang in een downloadmap, waardoor het risico bestaat dan deze te lang worden bewaard of per ongeluk worden verder verspreid, hetgeen kan leiden tot een inbreuk op de rechten en vrijheden van betrokkenen.	Downloadmap per dag geautomatiseerd leeg laten maken.		
3	De bewaartermijnen worden niet nageleefd, waardoor gegevens te lang worden bewaard.	De onderwijsinstelling maakt beleid op het gebied van het bewaren van cijfers e.d. in het leermiddel na het overbrengen hiervan in het LAS.		
4	De toegang tot Studiemeter door docenten uit dienst blijft beschikbaar, hetgeen tot onbevoegde toegang leidt.	De onderwijsinstelling draagt er zorg voor dat accounts die geen toegang meer hoeven te hebben tot het leermiddel tijdig worden geschoond, waardoor geen toegang meer wordt verkregen.		

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 niet binnen de invloedssfeer van (de leverancier van] [SYSTEEM] liggen, terwijl deze aanbevelingen c.q. 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:

---

[i] De Autoriteit Persoonsgegevens heeft Google Analytics ‘Universal’ in onderzoek. Dit betreft de voorloper van GA4.