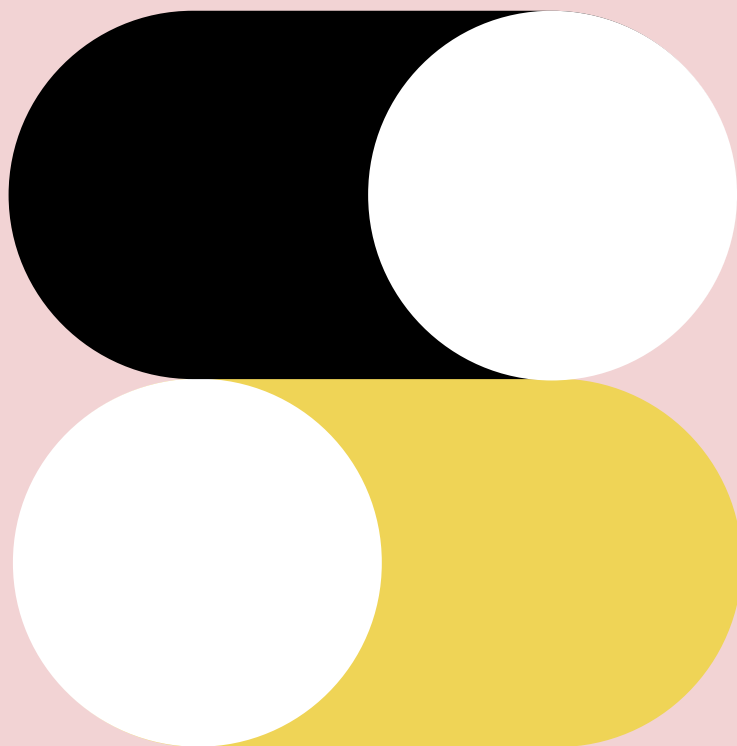




Referentiekader 2.0 - Verantwoord gebruik van studiedata en AI.

Handreiking bij het afwegen en maken
van keuzes

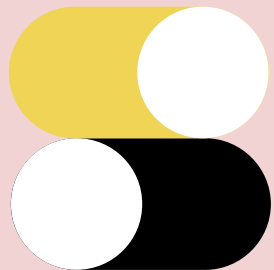
Referentiekader 2.0 - Verantwoord gebruik van studiedata en AI.

Handreiking bij het afwegen en maken van keuzes

April 2025



Op deze uitgave is de Creative Commons ShareAlike Naamsvermelding 4.0-licentie van toepassing. Maak bij gebruik van dit werk vermelding van de volgende referentie: Npuls (2025) Referentiekader, transformatiehub AI & Data. Npuls: Utrecht.



Inhoudsopgave

Samenvatting	5
1. Inleiding	11
1.1 Stormachtige ontwikkelingen rond AI	11
1.2 Referentiekader 2.0: verdieping en verbreding	12
1.3 Doel, doelgroep en opzet	12
1.4 Het Referentiekader als dynamisch kader	13
1.5 Leeswijzer	14
2. Studiedata en AI	15
2.1 Begripsomschrijvingen	15
2.2 Toepassingen en kansen van studiedata en AI	18
2.3 Risico's bij het gebruik van studiedata en AI	19
3. Waarden bij verantwoord gebruik van studiedata en AI	21
3.1 Inleiding	21
3.2 Rechtvaardigheid	22
3.3 Menselijkheid	27
3.4 Autonomie	29
4. Wettelijk kader: AVG	33
4.1 Relevante begrippen	33
4.2 Doel- grondslag – zorgvuldigheid	35
4.3 (Generatieve) AI en de AVG	42
5. Wettelijk kader: AI Act	45
5.1 Inleiding	45
5.2 Wat regelt de AI Act voor het onderwijs?	47
5.3 Wat moeten de instellingen regelen bij het gebruik van hoog risico AI?	52
5.4 Rolverschuiving van gebruiksverantwoordelijke naar aanbieder	53
5.5 Inkoop en AI	55
5.6 Voorbereiding op de AI Act	56
5.7 Andere juridische leerstukken bij het gebruik van studiedata en AI	56
6. Duidelijkheid over verantwoordelijkheden	57
7. Waar en hoe te beginnen?	59
ANNEX – businesscase	61
Colofon	63

Samenvatting

1. Inleiding

Binnen onderwijsinstellingen is het mogelijk om het gebruik van studiedata en AI breed in te zetten. Dit biedt veel kansen en mogelijkheden. Daarnaast zitten er risico's aan het gebruik van studiedata en AI. Hoe kun je deze kansen en mogelijkheden benutten en tegelijkertijd de risico's wegnemen of beperken? Daarom is de centrale vraag dit Referentiekader: hoe kan een instelling verantwoord studiedata en AI inzetten?

Daarvoor is duidelijkheid nodig over **waarden**, **wettelijke kaders** en **verantwoordelijkheden**. Het Referentiekader geeft richting en is een hulpmiddel om te bepalen waar en hoe te beginnen met het verantwoord inzetten van studiedata en AI.

Het Referentiekader richt zich op professionals in het wo, hbo en mbo die met studiedata en AI aan de slag willen. Het Referentiekader geldt in de gevallen waarin studiedata zonder en met behulp van algoritmen en AI worden ingezet.

2. Waarden bij gebruik van studiedata en AI

Het Referentiekader ziet waarden als nastrevenswaardige algemene, abstracte ideeën of idealen die richting geven aan het gebruik van studiedata en AI. De basis voor de waarden in het Referentiekader zijn de publieke waarden voor digitalisering in het onderwijs. Deze waarden zijn aangevuld en verrijkt in nauw contact en gesprek met deskundigen uit het onderwijs. Dat resulteert in de volgende waarden:

Rechtvaardigheid. Het gebruik van studiedata en AI is inclusief en bevordert gelijkheid. Het gebruik leidt niet tot onbedoelde kansenongelijkheid en vooringenomenheid ("bias") naar bepaalde personen en groepen. Daarnaast zijn betrouwbaarheid en veiligheid van systemen, transparantie en het afleggen van rekenschap belangrijk voor een verantwoorde inzet van studiedata en AI.

Menselijkheid. Het gebruik van studiedata en AI houdt rekening met betekenisvol contact tussen docent en student en tussen studenten onderling en de mogelijkheid van zelfontplooiing van studenten, zodat zij zich in een veilige en respectvolle omgeving kunnen ontwikkelen. Daarnaast is de menselijke blik cruciaal; bij geautomatiseerd gebruik van studiedata en AI is altijd een mens betrokken.

Autonomie. Het gebruik van studiedata en AI houdt rekening met zelfbeschikking van de student om zelf keuzes te maken, zelfstandig te handelen en controle uit te oefenen over het eigen leven en onderwijs. Autonomie raakt ook de docent en andere onderwijsprofessionals; zij kunnen invloed uitoefenen bij inhoudelijke en pedagogische keuzes binnen het onderwijs. Daarnaast zijn het gebruik van studiedata en AI en de bescherming van de persoonlijke levenssfeer (privacy) van betrokkenen met elkaar in evenwicht.

Instellingen maken bij het zelf invullen van deze waarden (en van eventueel eigen instellingsgebonden waarden) hun eigen afwegingen. Daarbij is het mogelijk om onder meer te kijken naar het doel en de impact van het gebruik van studiedata en AI op studenten, docenten en andere betrokkenen, de context waarbinnen studiedata en AI wordt gebruikt en de risico's van het gebruik van studiedata en AI.

3. Wettelijke kaders: AVG en AI Act

Naast waarden zijn er wetten en regels rond het gebruik van studiedata en AI, zoals het intellectueel eigendomsrecht, bescherming van persoonsgegevens (AVG) en de recente specifieke wetgeving rond AI (de AI Act). Het Referentiekader richt zich op de AVG en de AI Act.

AVG. Studiedata zijn (bijna) altijd persoonsgegevens. Dat betekent dat de AVG geldt bij het gebruik van studiedata en AI. Instellingen hanteren bij elk gebruik van studiedata en AI de drieslag: doel(binding) - grondslag - zorgvuldigheid.

Doel(binding)	Grondslag	Zorgvuldigheid
Het doel van het gebruik van studiedata en AI is <i>welbepaald, uitdrukkelijk omschreven</i> en <i>gerechtvaardigd</i> .	Het gebruik van studiedata en AI vereist het bestaan van een (geldige) grondslag, te weten:	Betrokkenen worden geïnformeerd over het gebruik van studiedata en AI.
Een instelling mag de studiedata in beginsel niet verder gebruiken voor een onverenigbaar doel.	Toestemming van de betrokkene waarbij de toestemming vrij, geïnformeerd, specifiek en ondubbelzinnig is gegeven	Alleen die studiedata mogen worden gebruikt die nodig zijn voor het realiseren van het beoogd doel.

Doel(binding)	Grondslag	Zorgvuldigheid
Een instelling mag de studiedata wel verder gebruiken voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek en voor statistische doeleinden. Het is belangrijk dat de instelling passende waarborgen treft voor de bescherming van de rechten en vrijheden van de betrokkenen.	Noodzakelijk voor de uitvoering van een overeenkomst waar betrokkene partij is	Bij het gebruik van studiedata is aandacht voor <i>privacy by design</i> en <i>privacy by default</i>
	Noodzakelijk om te voldoen aan een wettelijke verplichting	De studiedata zijn correct en volledig.
	Noodzakelijk om te voldoen aan een wettelijke verplichting door de instelling	Het uitvoeren van een Data Protection Impact Assessment (DPIA) is mogelijk vereist.
	Noodzakelijk in het licht van de vitale belangen van de betrokkene	De studiedata mogen niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor de studiedata worden gebruikt.
	Noodzakelijk voor het uitvoeren van een taak in het algemeen belang of uitvoering van het openbaar gezag door de instelling	De instelling treft passende technische en organisatorische maatregelen ter bescherming van de studiedata.
	Noodzakelijk voor de gerechtvaardigde belangen van de instelling of een derde	De rechten van betrokkenen worden gerespecteerd, waaronder het recht niet te worden onderworpen aan een uitsluitend geautomatiseerde verwerking van studiedata.
		De instelling past de AVG ook toe bij het uitwisselen van studiedata met andere instellingen en partijen en sluit de relevante AVG-overeenkomst af (zoals de verwerkersovereenkomst)

AI Act. De AI Act geeft regels voor het ontwikkelen en gebruiken van AI-systemen. De AI Act geldt ook voor instellingen. De aard en omvang van deze regels verschilt al naar gelang de instelling kwalificeert als een aanbieder van het AI-systeem of als gebruiksverantwoordelijke. Het is belangrijk dat instellingen de volgende acties nemen:

- **Inventariseren.** Instellingen inventariseren welke AI zij voor welke doeleinden gebruiken.
- **Classificeren.** Instellingen classificeren deze AI-toepassingen op basis van de AI Act; wat is de risico-classificatie van het AI-systeem (onacceptabel, hoog, transparantie of minimaal)? Wat is de rol van de instelling bij het betreffende AI-systeem?
- **Implementeren.** Instellingen nemen op basis van de classificering de voorgeschreven maatregelen ter beperking van de risico's.

Onderstaande tabel geeft in één opslag de systematiek weer van de AI Act.

Risico	Consequenties AI Act	Voorbeelden van AI-systemen in het onderwijs
Onacceptabel risico	Verboden	Emotieherkenning op de werkplek en in het onderwijs
Hoog risico	Toegestaan maar met vereisten voor aanbieders en – in mindere mate – gebruiksverantwoordelijken. Vereisten zijn: – Risico- en kwaliteitsmanagementsysteem – Data en data governance – Technische documentatie en gebruiksinstructies – Logging en monitoring – Menselijk toezicht – Conformiteitsbeoordeling – Informeren van betrokkenen – Uitvoeren Fundamental Rights Impact Assessment – Nauwkeurig, robuust en cyberveilig	De AI Act kent 4 hoog risico-toepassingen in het onderwijs: 1. Toegang, toelating en toewijzing tot onderwijs. 2. Evalueren van leerresultaten, ook voor sturen van het leerproces. 3. Beoordelen van het passend onderwijsniveau. 4. Monitoren en detecteren van ongeoorloofd gedrag tijdens toetsen. Let wel: de AI Act kent een aantal uitzonderingen
Transparantie risico	Toegestaan maar met informatieverplichtingen	Chatbots en deepfakes
Minimaal risico	Toegestaan zonder aanvullende verplichtingen uit de AI Act	

4. Verantwoordelijkheden

De basis voor een (blijvend) verantwoord gebruik van studiedata en AI is duidelijkheid over wie beslissingen neemt en wat de rollen en taken zijn rond alle aspecten van het gebruik van studiedata en AI. Belangrijk is dat tijdens de gehele levenscyclus van dat gebruik verschillende belanghebbenden (waaronder ook studenten en docenten) en deskundigen zijn betrokken bij de te nemen afwegingen rond het verantwoord gebruik van studiedata en AI. Daarbij zorgt het organiseren van een tegengeluid voor nieuwe perspectieven en andere inzichten. Op die manier worden waarden en wettelijk kader in samenhang besproken.

5. Waar en hoe te beginnen?

Instellingen kunnen de volgende stappen zetten voor een verantwoord gebruik van studiedata en AI.

1. Stel een 'businesscase' op voor het krijgen van inzicht in doel, voor- en nadelen van het gebruik van studiedata en AI en de waarden die in het geding zijn. Doe een check op de AVG en AI Act om na te gaan wat er geregeld *moet* worden.
2. Betrek belanghebbenden in een multidisciplinaire aanpak. Op die manier verkrijgt de instelling nieuwe inzichten bij het concretiseren van de waarden en in de kansen en risico's van het gebruik van studiedata en AI.
3. Stel beleid, richtlijnen en procedures op voor duidelijkheid rond de verschillende aspecten van een verantwoord gebruik van studiedata en AI.
4. Zorg voor data- en AI-geletterdheid bij onderwijsprofessionals.
5. Speel het Dilemmaspeel voor het verkrijgen van inzichten in kansen en risico's, de invulling van de waarden, de eisen vanuit wettelijke kaders én de te nemen maatregelen ter voorkoming of beperking van de risico's.

Het Referentiekader als dynamisch hulpmiddel

Op veel vragen van instellingen rond studiedata en AI is nu nog vaak geen kant-en-klaar antwoord mogelijk. Veel aspecten, zeker ook rond de AI Act, zijn nog volop in ontwikkeling en vragen nadere duiding. Bovendien zullen de ervaringen van instellingen met het gebruik van studiedata en AI de komende tijd toenemen. Zodoende is het Referentiekader een dynamisch hulpmiddel, en geen eindpunt. Wij moedigen instellingen daarom aan te leren van elkaars positieve én negatieve ervaringen, open en in vertrouwen.

1. Inleiding

1.1 Stormachtige ontwikkelingen rond AI

Hoe kun je als instelling studiedata benutten? De wens bestaat al langer om dat te onderzoeken. Belangrijk is dat studenten, docenten en andere betrokkenen vertrouwen hebben in een verantwoord gebruik van die studiedata. Om instellingen te ondersteunen bij het gebruik van studiedata, verscheen in november 2021 het *Referentiekader privacy en ethiek voor studiedata (versie 1.0)*.

Sinds dat dit Referentiekader in 2021 verscheen, is er een sterke toename van de mogelijke toepassingen van het gebruik van studiedata. De ontwikkelingen rond de mogelijkheden van (generatieve) AI staan hierbij centraal.

De stormachtige ontwikkelingen rond Artificial Intelligence (AI) waren vooral in de context van de mogelijkheden van 'big data'. Zie het onderzoek 'Verkenning data-gedreven onderwijsonderzoek in Nederland' uit 2017 van de Universiteit Twente ([Verkenning_datagedreven_onderzoek.pdf](#))

AI is geen nieuw fenomeen, maar met de lancering van ChatGPT in november 2022 is een nieuwe AI-fase ontstaan. Een fase met volop aandacht voor de mogelijkheden, maar ook voor de risico's en gevaren van AI. Die onstuimige ontwikkeling van steeds betere en nieuwe toepassingen en mogelijkheden op allerlei terreinen is nog lang niet voorbij. Er gaat bijna geen dag voorbij zonder de introductie van een nieuwe AI-toepassing. Maar er gaat ook bijna geen dag voorbij zonder de publicatie van een rapport, studie, richtlijn of framework dat wijst op de gevaren en risico's van AI.

De website theresanaiforthat.com geeft een overzicht van wat er dagelijks aan nieuwe AI-toepassingen op de markt komt. Een fraai totaaloverzicht van alle tot nu toe mogelijke risico's (meer dan 750!) verbonden aan het gebruik van AI is het MIT Risk Taxonomy Report, zie: [The AI Risk Repository](#)

1.2 Referentiekader 2.0: verdieping en verbreding

De ontwikkelingen rond AI raken – uiteraard – ook het onderwijs. De impact van het gebruik van studiedata en AI is groot voor studenten, docenten, ondersteuners, beleidsmakers en besturen. Ook staan veel instellingen nog aan het begin van hoe zij zich gaan verhouden tot AI, zowel vanuit de publieke waarden in het onderwijs als vanwege de recent ingegane AI Verordening (AI Act). Gelet op alle ontwikkelingen is er voldoende reden het Referentiekader over verantwoord gebruik van studiedata te verdiepen met AI.

Er is nóg een reden voor herziening van het Referentiekader. Het Referentiekader 1.0 richt zich op het hbo en wo. Veel van de onderwerpen en problematiek zijn ook relevant en herkenbaar zijn voor mbo. Echter, specifieke mbo-thema's komen niet aan bod, zoals minderjarigheid/relatie met ouders en voogden, de zorgplicht naar studenten en de samenwerking met allerlei partijen (zoals stagebedrijven en hulpinstanties). Dit nieuwe Referentiekader is daarom verbreed naar het mbo.

Het Referentiekader 2.0 is ontwikkeld op basis van een evaluatie van de opgedane ervaringen sinds 2021 en op basis van de vele gesprekken en dialogen met materie-deskundigen in het mbo, hbo en wo.

1.3 Doel, doelgroep en opzet

Het doel van dit Referentiekader is om instellingen in het mbo, hbo en wo te helpen bij het verantwoord gebruiken van studiedata en AI. Het Referentiekader is bedoeld voor professionals binnen instellingen die in de praktijk werken met studiedata en AI.

Instellingen in het mbo, hbo en wo staan voor verschillende vragen als het gaat om een verantwoord gebruik van studiedata en AI: Waar begin je als je met studiedata en AI aan de slag wilt en waarop moet je letten? Wat zijn de voor de instelling relevante waarden? Wat *kan* en – in het licht van bijvoorbeeld de AVG en AI Act – *moet* je (in ieder geval) doen en regelen? Wie betrek je bij je afwegingen en keuzes? Hoe borg je als instelling een blijvend verantwoord gebruik van studiedata en AI?

De beantwoording van deze vragen en de afwegingen die een instelling maakt, luisteren nauw. Is een instelling te voorzichtig, dan lopen studenten en docenten mogelijk kansen mis, maar is een instelling te weinig voorzichtig, dan lopen studenten en docenten onnodige risico's op bijvoorbeeld uitsluiting, onredelijke behandeling of leidt het tot kansenongelijkheid. Het Referentiekader wil richting geven bij de beantwoording van deze vragen en inspiratie

bieden als instellingen zelf doorgaan met het ontwikkelen van instelling-specifieke beleidskaders, werkwijzen en processen rond het verantwoord gebruik van studiedata en AI.

Die richting geeft het Referentiekader door het presenteren van waarden, wettelijke kaders en het scheppen van duidelijkheid rond verantwoordelijkheden.

De titel van het Referentiekader is een verantwoord gebruik van 'studiedata en AI'. Dat betekent dat het Referentiekader in drie gevallen van toepassing is:

1. Gebruik van studiedata *zonder* algoritme of AI.
2. Gebruik van studiedata met behulp van een algoritme (niet zijnde AI).
3. Gebruik van studiedata met behulp van (generatieve) AI.

In hoofdstuk 2 meer over wat het Referentiekader verstaat onder 'studiedata', 'algoritme' en '(generatieve) AI'.

1.4 Het Referentiekader als dynamisch kader

Veel aspecten, zeker ook rond de AI Act, vragen een nadere duiding en invulling. De verwachting is dat de komende periode steeds meer duidelijkheid komt van bijvoorbeeld de Europese Commissie, het Europese AI Office en nationale toezichthouders zoals de Autoriteit Persoonsgegevens.

Het Referentiekader is alleen al om die reden een dynamisch kader; nadere duiding kan en zal gevolgen hebben voor de inhoud van het Referentiekader.

Daarnaast zal het aantal succesvolle én niet-succesvolle toepassingen en *best practices* rond het gebruik van studiedata en AI de komende tijd waarschijnlijk toenemen. Het is belangrijk dat instellingen van elkaars positieve en negatieve ervaringen leren, open en in vertrouwen. Daarom nodigen we iedereen uit ervaringen te blijven delen, om daarmee ook het Referentiekader actueel en relevant te houden.

▶ Een mooi voorbeeld van het delen van elkaars ervaringen is de uitgave van MBO Digitaal over verschillende parels én missers op het gebied van digitalisering.

Tot slot, bespreek binnen de eigen instelling het gebruik van studiedata en AI. Heb het over vragen als: Wat willen we bereiken? Wat zijn de voor- en nadelen? Hoe draagt het gebruik bij aan de publieke waarden in het onderwijs? Hoe beperken we de risico's? Deze gesprekken met studenten, docenten, ondersteuners, beleidsmakers en bestuurders zijn cruciaal voor

een beter begrip van de (on)mogelijkheden van studiedata en AI, het maken van een gebalanceerde keuze over de inzet van studiedata en AI en voor een blijvend verantwoord gebruik daarvan. Het Referentiekader is een hulpmiddel, en geen eindpunt, ga er met alle betrokkenen in de eigen instelling actief mee aan de slag en volg de andere initiatieven rond studiedata en AI goed.

Een overzicht van lopende initiatieven en activiteiten van Npuls, SURF en MBO Digitaal:

- Verkenning algoritmeregister voor het onderwijs:
- Handreiking ChatGPT:
- Gezamenlijke inkooponderhandeling AI-tooling:
- Verkenning volwassenheidsmodel AI Ethiek:
- Leergang beleid en AI

1.5 Leeswijzer

Hoofdstuk 2 definieert en beschrijft enkele belangrijke begrippen uit dit Referentiekader. In dit deel ook meer over (mogelijke) toepassingen in het mbo, hbo en wo en de kansen en risico's van het gebruik van studiedata en AI.

Hoofdstuk 3 geeft waarden voor het verantwoord gebruik van studiedata, gebaseerd op de publieke waarden in het onderwijs, zoals opgenomen in de WaardenWijzer voor digitalisering in het onderwijs van Kennisnet en SURF. Instellingen hebben meer ruimte om deze waarden verder in te vullen, in tegenstelling tot de wettelijke kaders in de hoofdstukken 4 en 5.

Hoofdstukken 4 en 5 schetsen de wettelijke kaders waaraan een instelling aandacht moet geven. Het betreft de Algemene Verordening Gegevensbescherming (AVG) en de AI Verordening (AI Act). Deze wetten bepalen wat elke instelling in ieder geval moet regelen bij gebruik van studiedata en (bepaalde!) AI. Vanwege dit meer dwingende karakter, zijn deze hoofdstukken langer dan de andere hoofdstukken.

Hoofdstuk 6 beschrijft het belang van het goed regelen van verantwoordelijkheden en een multidisciplinaire aanpak rond het gebruik van studiedata en AI.

Hoofdstuk 7 sluit af met de stappen die een instelling kan nemen om te starten met het verantwoord gebruiken van studiedata en AI.

In (bijna) alle hoofdstukken staan ook voorbeelden, praktische tips en aandachtspunten.

2. Studiedata en AI

2.1 Begripsomschrijvingen

Studiedata

Zone Studiedata¹ omschrijft studiedata als een verzamelnaam voor een breed scala aan gestructureerde en ongestructureerde gegevens die binnen instellingen benut kunnen worden voor het verbeteren van de kwaliteit, effectiviteit en efficiëntie van onderwijs.

Voorbeelden van studiedata zijn: (voor)opleidingen van studenten, behaalde cijfers, ingediend werk, cijfers over instroom, doorstroom en uitstroom, studieadviezen, sociaaleconomische achtergrond van studenten, gevolgde colleges/werkgroepen, studiematerialen, roosters, docent-evaluaties, etc.

Studiedata ontstaan op verschillende manieren zoals bij het organiseren en het geven van onderwijs en door samenwerkingen tussen instellingen en derde partijen (bijvoorbeeld tussen Studielink, DUO, CBS en met stagebedrijven en maatschappelijke organisaties).

De meeste studiedata zijn vastgelegd in informatiesystemen voor onder andere het geven van onderwijs, de administratie van inschrijvingen en studieresultaten, kwaliteitszorg en afnemen van toetsen.

Artificial Intelligence (AI)

In de beschrijvingen en discussies over “AI” valt op dat het vaak wordt gebruikt als breed containerbegrip met termen als: ‘generatieve AI’, ‘machine learning’, ‘neural networks’, ‘algoritmen’, ‘AI-systemen’, ‘AI-modellen’, etc. Kortom, waar hebben we het over als we in dit Referentiekader spreken over “AI”?

Als dit Referentiekader spreekt over “AI”, dan wordt bedoeld op AI-systemen zoals gedefinieerd in de Europese Verordening over artificiële intelligentie (2024/1689), hierna de ‘AI Act’².

¹ Zie: doe-meer-met-studiedata.nl/datagedreven-werken/

² De definities van de AI Act zijn gebaseerd op de definities van de OESO (zie: Explanatory Memorandum on the updated OECD definition of an AI system, OECD Artificial Intelligence Papers, March 2024, No. 8. (Explanatory memorandum on the updated OECD definition of an AI system | OECD

Op die manier sluit het Referentiekader aan bij dit wettelijk kader. De AI Act wil met het gebruik van deze definitie technologieneutraal zijn zodat ook bij nieuwe (leer)technieken de AI Act relevant blijft. Deze wens geldt eveneens voor het Referentiekader.

AI-systemen zijn gedefinieerd als:

“Een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op de fysieke of virtuele omgevingen”.

Een AI-systeem is een systeem dat specifiek is ontworpen om data te analyseren, en patronen te herkennen en die kennis te gebruiken om weloverwogen beslissingen te nemen of voorspellingen te voldoen. AI-systemen kunnen leren van data en zich na verloop van tijd aanpassen. Het leren vindt plaats via machine learning technieken zoals neural networks en deep learning.

Geen AI-systeem

Van een AI-systeem volgens de AI Act en dit Referentiekader is géén sprake als de systemen zijn gebaseerd op regels die uitsluitend door mensen zijn vastgesteld om automatisch handelingen uit te voeren. Zie hierna bij algoritmen.

AI-systemen kunnen zowel specifiek als generiek worden toegepast. Een voorbeeld van een specifieke toepassing is een AI-systeem dat een voorspelling doet over studiesucces van studenten. Een generieke toepassing betreft het genereren van tekst, audio, video of een combinatie daarvan. Dit wordt ook generatieve AI genoemd. Voorbeelden van generatieve AI zijn ChatGPT, MidJourney en DALL-E.

Waar in dit Referentiekader wordt gesproken over AI, dan worden daarmee zowel specifieke als generieke/generatieve AI-systemen bedoeld.

Het is belangrijk te beseffen dat de *toepassing* van het specifieke en generieke AI-systeem de risicoclassificatie van de AI Act bepaalt. Wat betreft generatieve AI is dat soms best een lastig onderscheid. Zo is een chatbot op zich geen hoog risico toepassing maar als diezelfde chatbot wordt ingezet als onderdeel van een hoog risico toepassing is dat anders. In hoofdstuk 5 meer daarover.

De ontwikkeling en het in gebruik nemen van AI-systemen kent een aantal fasen (*lifecycle*).

Ruwweg zijn dat:

1. Het definiëren van het probleem en vaststelling van de doelen van het AI-systeem.
2. Het verkrijgen en bewerken van data.
3. Het ontwikkelen en trainen van het AI-model.
4. Het evalueren en aanpassen van het AI-model.
5. Het in gebruik nemen van het AI-systeem.
6. Het monitoren van het gebruik van het AI-systeem.

Algoritmen

De AI Act definieert het begrip algoritme niet. Toch is dit cruciaal voor een goed begrip van AI-systemen. Algoritmen zijn feitelijk een aantal te volgen instructies die tot een bepaald doel leiden. Voorbeelden van algoritmen zijn: wiskundige formules, recepten voor het bereiden van een maaltijd of op regels gebaseerde systemen die zijn vastgesteld om automatisch handelingen uit te voeren ('als-dan'-systemen). En ook beschrijvende rapportages over bijvoorbeeld trends rond aantallen studenten kunnen algoritmen zijn.

Deze voorbeelden van algoritmen zijn geen AI(-systemen) in de zin van de AI Act maar de impact voor studenten van het gebruik van studiedata met algoritmen (die geen AI zijn) kan toch groot zijn. Vandaar dat het Referentiekader ook van toepassing is op het gebruik van studiedata met algoritmen die geen AI zijn.

AI model

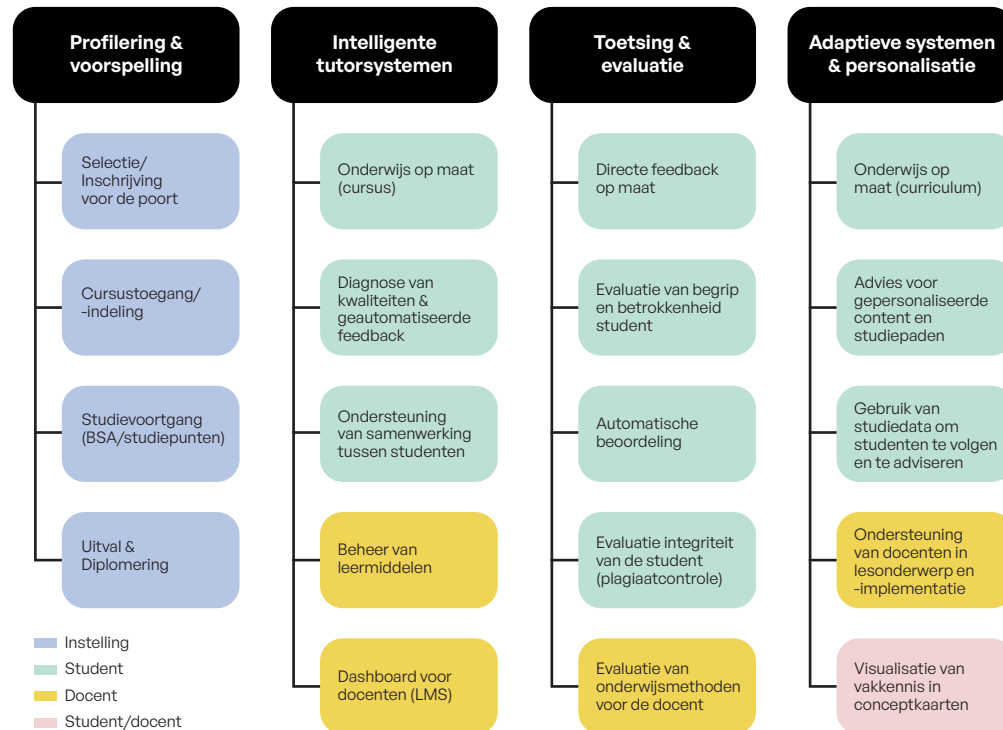
De AI Act kent ook het begrip 'AI-modellen voor algemene doeleinden'. Deze modellen worden in hoofdstuk 5 verder toegelicht. Voor nu is het belangrijk te benadrukken dat deze modellen op zichzelf geen AI-systeem zijn en dat de risico-classificatie van de AI Act voor AI-systemen niet van toepassing is op deze AI-modellen.

Betrokkenen

Dit Referentiekader spreekt geregeld over 'betrokkenen'. Dat zijn zowel de natuurlijke personen die direct of indirect geïdentificeerd kunnen worden (betrokkenen zoals bedoeld in de AVG) als diegenen die worden geraakt door het gebruik van studiedata en AI. Veelal betreft het studenten en docenten.

2.2 Toepassingen en kansen van studiedata en AI

Binnen het mbo, hbo en wo kan het gebruik van studiedata en AI breed worden ingezet. In onderstaand overzicht is dit weergegeven.



AIEd typologie gebaseerd op Bond (2024) De kleuren geven de belangrijkste doelgroep van de AI-toepassing. Bond et al., International Journal of Educational Technology Higher Education (2024), 21:4 (doi.org/10.1186/s41239-023-00436-z).

AI in het Referentiekader 1.0 is een aantal voorbeelden genoemd waar studiedata (al dan niet met AI) ingezet kunnen worden: welzijnsmonitoring, afstandsonderwijs en docenten die uit het Learning Management System (LMS) standaard rapportages ontvangen. Daarnaast kunnen studiedata (al dan niet met AI) gebruikt worden voor: het krijgen van inzichten in de studieprestaties van individuele studenten, het nagaan waar studenten terechtkomen, het voorspellen van uitval van studenten en toetsing en examinering.

Een bloemlezing van enkele concrete (pilot) toepassingen van studiedata mét AI in het onderwijs in Nederland en daarbuiten:

- Het helpen van studenten met het omgaan van stress (zie ixperium.nl/ai-helpt-studenten-omgaan-met-stress).
- Het ondersteunen van studenten met een beperking (zie de app van BeMyEyes).
- Het helpen van studenten bij het selecteren van cursussen die aansluiten bij hun individuele behoeften (Magazine-AI-in-onderwijs-NL-AIC.pdf (nlaic.com)).
- Het voorspellen van studiesucces (zie kennisnet.nl/onderzoek/kan-ai-studie-uitval-voor-spellen-in-het-mbo).
- Het geven van automatische feedback op het schrijfwerk van studenten (feedbackfruits.nl).

Zie onder meer:

- Praktijkgids AI in het onderwijs van Zuyd Hogeschool (1734605532357)
- SURF, Promises of AI in Education, discussing the impact of AI systems in educational practices, June 2022 (Promises of AI in Education | SURF.nl)

De mogelijkheden voor het gebruik van studiedata en AI zijn al met al groot en worden met toenemende data en nieuwe technologieën steeds groter.

2.3 Risico's bij het gebruik van studiedata en AI

De genoemde voorbeelden maken duidelijk dat het gebruik van studiedata en AI veel potentie heeft. Tegelijkertijd kan het gebruik van studiedata en AI tot onbedoelde en ongewenste negatieve consequenties leiden zoals:

- Verlies of beperking van de menselijke maat (en menselijk contact!).
- Verlies of beperking van autonomie en het recht op zelfbeschikking.
- Verlies of beperking van de vrijheid om eigen keuzes te maken en de mogelijkheid om te falen: het veranderen van een leeromgeving naar een presteeromgeving.
- Het buitensporig of onnodig volgen van studenten (inzage in gedrag, leef- en leerpatroon).
- Risico dat onderwijsinstellingen minder inclusief worden en kansenongelijkheid toeneemt, doordat op basis van beschikbare data bepaalde groepen worden uitgesloten.

- Uitsluiting of discriminatie³.
- Misverstanden door onjuiste of onvolledige data of door misbruik of misinterpretatie van gegevens.

Daarnaast zijn er in het algemeen zorgen over de privacy en bescherming van de persoonsgegevens van betrokkenen⁴, maar ook over het alles willen vatten met data in modellen waardoor andere relevante dynamieken worden miskend.

Een verantwoord gebruik van studiedata en AI is, kort gezegd, positieve interventies in het onderwijs mogelijk maken en tegelijkertijd negatieve consequenties minimaliseren.

³ Zie de klacht die een VU student bij het College voor de Rechten van de Mens heeft ingediend over discriminatie door AI-software van online proctoring. De student stelde dat de software haar gezicht niet herkende vanwege haar donkere huidskleur. Uiteindelijk is deze klacht afgewezen maar het College oordeelde dat niet uitgesloten kan worden dat het gebruik van dergelijke software in andere situaties wel tot discriminatie kan leiden. Zie: nieuwsbericht van 17 oktober 2023 op de website van het College voor de Rechten van de Mens.

⁴ Zo waarschuwt de Autoriteit Persoonsgegevens dat het gebruik van AI-chatbots kan leiden tot datalekken (doordat medewerkers (bijzondere) persoonsgegevens invoeren in AI-chatbots waardoor onbevoegden ongeoorloofd toegang krijgen tot die persoonsgegevens. Zie: bericht van 6 augustus 2024 op de website van de AP.

3. Waarden bij verantwoord gebruik van studiedata en AI

3.1 Inleiding

Wat zijn de waarden voor het verantwoord gebruik van studiedata en AI binnen instellingen? In dit deel staan deze waarden centraal.

Het Referentiekader ziet waarden als nastrevenswaardige algemene, abstracte ideeën of idealen die het handelen richting geven.

Naast waarden zijn er wetten en regels rond het gebruik van studiedata en AI, vooral de wetgeving rond intellectueel eigendomsrecht, privacy en bescherming van persoonsgegevens (de AVG) en de recente specifieke wetgeving rond AI (de AI Act). Deze wetten – evenals de Grondwet, het Europees Verdrag voor de Rechten van de Mens (EVRM) en het Handvest van de grondrechten van de Europese Unie – bevatten bepalingen en voorschriften die óók gebaseerd zijn op (Europese) waarden.

De bescherming van persoonsgegevens is uitgewerkt in de AVG en de waarden transparantie en menselijkheid zijn uitgewerkt in de AVG en de AI Act.

Aparte aandacht voor waarden

Waarom dan toch aparte aandacht voor waarden? Het specifiek noemen van waarden als vertrekpunt voor verantwoord gebruik van studiedata en AI is essentieel om twee redenen. In de eerste plaats is niet alles wat wettelijk mag in overeenstemming met waarden. Oftewel: wat wettelijk mag, is niet altijd ethisch verantwoord. Daarnaast biedt wet- en regelgeving soms ruimte voor een eigen invulling die met waarden zijn vorm te geven. In die zin kunnen waarden positief bijdragen aan bijvoorbeeld de ambitie van een instelling rond het gebruik van studiedata en AI.

Waarden in dit Referentiekader

Welke waarden hanteert dit Referentiekader? Dat zijn de publieke waarden voor digitalisering in het onderwijs, namelijk: **rechtvaardigheid**, **menselijkheid** en **autonomie**. Deze hoofdwaarden vertegenwoordigen een aantal andere waarden. Basis voor deze uitgewerkte waarden zijn de gesprekken, antwoorden op de vragenlijst en reviews met een groot aantal deskundigen uit het mbo, hbo en wo.

Laden en wegen van waarden

Niet al deze waarden zijn in alle gevallen evenredig van toepassing. Bovendien kan er spanning zitten tussen deze waarden en de toepassing daarvan voor een beoogd doel. Het is aan de instellingen deze waarden precies te laden en te wegen. Die keuze wordt bepaald door een aantal factoren, zoals: de omvang en organisatie van de instelling, de impact van het gebruik van studiedata en AI, de context waarin studiedata en AI wordt gebruikt, de risico's verbonden aan het gebruik van studiedata en AI (waarbij een hoog risico AI-systeem volgens AI Act wel een belangrijke factor is) en de eigen waarden van een instelling. Instellingen kunnen (en moeten) dus zelf invulling geven aan deze waarden. In hoofdstuk 7 staan tips hoe je dit als instelling kunt aanpakken.

Opbouw hoofdstuk

Dit hoofdstuk over waarden bestaat uit een vast stramien:

- een omschrijving van de waarden rechtvaardigheid, menselijkheid en autonomie volgens de Waardenwijzer voor digitalisering in het onderwijs;
- een omschrijving van wat die waarden betekenen voor het gebruik van studiedata en AI;
- enkele vragen/dilemma's om instellingen te helpen bij de invulling van die waarden.

Meedenken over verdere invulling waarden

De opgenomen vragen/dilemma's zijn een bloemlezing. Het Referentiekader nodigt iedereen uit om mee te denken over andere vragen en dilemma's en over de verdere invulling van de waarden. Het Dilemmaspel bij dit Referentiekader kan daarbij helpen. In het Dilemmaspel worden de waarden en dilemma's verder uitgewerkt op de specifieke toepassingen van studiedata en AI in het onderwijs, namelijk: (i) profilering en voorspelling, (ii) intelligente tutorsystemen, (iii) toetsing en evaluatie en (iv) adaptieve systemen en personalisatie (zie paragraaf 2.2).

3.2 RECHTVAARDIGHEID

3.2.1 Wat houdt rechtvaardigheid in?

De Waardenwijzer voor digitalisering in het onderwijs omschrijft wat rechtvaardigheid inhoudt.

Rechtvaardigheid omvat begrippen als gelijkheid, inclusiviteit en integriteit. In het onderwijs zou iedereen gelijke kansen moeten krijgen, zonder dat er groepen benadeeld of uitgesloten worden. En zonder dat sociale of culturele achtergrond of gender invloed hebben op de behandeling die leerlingen en studenten in het onderwijs krijgen. Het betekent dat zij zonder vooroordelen worden benaderd, niet door hun docenten en ook niet door algoritmes. In het onderwijs staat gelijkheid voorop. Inclusiviteit in onderwijs betekent toegankelijkheid voor alle leerlingen en studenten. Iedereen mag meedoen, hoort erbij en wordt voorbereid op een goed leven in de maatschappij.

Integriteit betekent onder meer dat wat er gebeurt in het onderwijs betrouwbaar, transparant en controleerbaar is, net zoals de data en de systemen die gebruikt worden. Integriteit betekent ook dat publieke middelen doelmatig worden besteed, met aandacht voor duurzaamheid, om recht te doen aan toekomstige generaties.

3.2.2 Rechtvaardigheid en het gebruik van studiedata en AI

Maar wat betekent rechtvaardigheid als het gaat om het gebruik van studiedata en AI?

Gelijkheid

Instellingen zien erop toe dat het gebruik van studiedata en AI niet leidt tot (onbedoelde) kansenongelijkheid en discriminatie van personen en groepen. Zeker bij het gebruik van AI-systemen bestaat het gevaar van (onbedoelde) vooringenomenheid ('bias') in de verschillende fasen van de ontwikkeling van het AI-systeem. Bijvoorbeeld doordat de trainingsdata niet-representatief en volledig zijn, het algoritme zelf vooringenomen is of de ontwikkelaars van het AI-systeem onbedoeld vooringenomen zijn. Vooringenomenheid kan wellicht leiden tot oneerlijke beslissingen die voor bepaalde groepen discriminerend kunnen uitpakken.

Vooringenomenheid

Het bureau Rhite heeft samen met de Radboud Universiteit een praktische handleiding gepubliceerd. Deze handleiding beschrijft niet alleen de verschillende vormen van vooringenomenheid tijdens de levenscyclus van een AI-systeem, maar omvat ook praktische aanbevelingen voor het adresseren van deze vooringenomenheid. Zie: [From-Inception-to-Retirement-Addressing-Bias-Throughout-the-Lifecycle-of-AI-Systems.pdf](#)

Zie verder ook de Handreiking non-discriminatie by design van de Tilburg Universiteit: [Handreiking voor niet discriminerende algoritmes | Tilburg University](#)

Specifiek voor AI en kansengelijkheid, zie: *AI en kansengelijkheid, Visie op de impact van AI op kansengelijkheid in het vervolgonderwijs*, Npuls, november 2024 ([AI en kansengelijkheid – Npuls](#))

Het voorkomen en bestrijden van vooringenomenheid bij het gebruik van studiedata en AI vereist dat studenten en docenten (of hun vertegenwoordigers) zijn betrokken bij de identificatie en de te nemen maatregelen ter beperking van deze risico's.

Procedure voor het organiseren van rechtvaardig gebruik

Het maken van afwegingen en het beoordelen van risico's voor een rechtvaardig gebruik vereist een duidelijke procedure voor de ontwikkeling, voor het daadwerkelijke gebruik van studiedata en AI en voor de monitoring van dat gebruik. In deze procedure krijgen alle relevante partijen een plek in een multidisciplinaire aanpak. Het is niet per se nodig om een nieuwe procedure op te stellen. Het is ook mogelijk om bestaande risico-procedures en/of de DPIA-procedure van instellingen te verrijken of aan te vullen op deze aspecten.

Procedure voor afhandeling van klachten

Het borgen van een rechtvaardig gebruik vraagt ook om een goede en makkelijk toegankelijke klachtenprocedure voor het snel en gedegen oppakken van klachten van betrokkenen.

Inclusiviteit

Studenten met een functionele beperking, een migratieachtergrond en een sociaaleconomische achterstand mogen niet worden benadeeld door het gebruik van studiedata en AI. De instelling weegt bij het gebruik van studiedata en AI zorgvuldig af of er mogelijke nadelige effecten voor deze (groepen van) betrokkenen zijn, bijvoorbeeld via scenario-analyses.

Integriteit

Betrouwbaarheid en veiligheid van systemen. Dit houdt onder meer in dat instellingen zorgen voor het beschikbaar komen, zijn en blijven van voldoende relevante data voor het vooraf bepaalde doel. Bovendien zorgen instellingen ervoor dat deze data betrouwbaar zijn, veilig worden gebruikt en opgeslagen, en van hoge methodologische kwaliteit zijn.

Belangrijke aandachtspunten bij het gebruik van studiedata en AI zijn:

- Onnauwkeurigheden in de studiedata worden begrepen en tot een minimum beperkt.
- De implicaties van onvolledige datasets zijn duidelijk.
- Er wordt een passende set gegevensbronnen gebruikt.

- De technieken van anonimiseren en pseudonimiseren worden begrepen en correct toegepast.
- Valse correlaties worden vermeden.
- Resultaten van eerdere onderzoeken worden meegenomen.
- De resultaten worden getoetst op bias (vooringenomenheid).
- De verwerking, analyse en benutting van studiedata wordt steeds in hun bredere context gezien en waar nodig gecombineerd met andere kennis en benaderingen.

Integriteit betekent ook dat wat er gebeurt in systemen betrouwbaar, transparant, veilig en controleerbaar is. Betrouwbaarheid vraagt om robuuste informatie- en cyberbeveiliging. Deze waarden zijn verankerd in de AVG en de AI Act. Tegelijkertijd vragen de specifieke beveiligingsrisico's verbonden aan AI óók om specifieke beveiligingsmaatregelen. Die specifieke beveiligingsrisico's rondom AI-systemen gaan over de toename van bestaande risico's zoals datalekken én over nieuwe risico's. Die nieuwe risico's zijn bijvoorbeeld het manipuleren en het 'kraken' van modellen (*jailbreaking*). Dit vraagt onder meer om nieuwe beheersmaatregelen, aanpassing van de governance en speciale tooling. Overigens biedt AI ook kansen voor informatie- en cyberbeveiliging.

Cyber Security Raad (CSR)

De CSR heeft naast een overzicht van de specifieke kansen en risico's van AI op het gebied van cybersecurity, een overzicht met de voorwaarden van een verantwoord gebruik van AI in dit verband. Zie: [Informerende+brief+aan+de+staatssecretaris+van+BZK+over+\(generatieve\)+AI+en+cybersecurity+DEF \(2\).pdf](#)

Transparantie. Transparantie betekent dat instellingen ervoor zorgen dat het voor alle betrokkenen die te maken krijgen met studiedata en AI duidelijk is voor welk doel studiedata en AI worden gebruikt, op welke data men zich heeft gebaseerd, hoe deze zijn verkregen, welke resultaten men wil bereiken en langs welke weg en hoe tot een bepaalde – al dan niet geautomatiseerde – uitkomst is gekomen. Deze keuzes en afwegingen zijn door de instelling gedocumenteerd om ze traceerbaar en verklaarbaar te maken. Daarnaast hebben betrokkenen het specifieke recht te weten als ze met een AI-toepassing te maken hebben.

Echter, volledig transparant zijn over de inzet van vaak ingewikkelde en ondoorzichtige AI-systemen brengt uitdagingen met zich mee. De uitdagingen zijn het begrijpelijk houden van de informatie zelf én het bieden van de transparantie over *welke data in welke mate verantwoordelijk zijn* voor een bepaalde uitkomst. Dat is in veel gevallen ondoenlijk, te meer omdat veel AI-systemen zelflerend zijn. Het openen van deze 'black box' vraagt uitlegbare AI ('explainable AI').

Transparantie

Instellingen kunnen transparantie op verschillende manieren vormgeven zoals:

- Zorgdragen dat medewerkers in relevante rollen en functies voldoende data- en AI-geletterd zijn om vragen, verzoeken en klachten van betrokkenen snel en gedegen af te handelen.
- Betrekken van leveranciers bij het geven van duidelijke informatie over hoe hun AI ‘werkt’ (op grond van welke input komt output tot stand, etc.), bijvoorbeeld door visualisaties die laten zien welke elementen het zwaarst hebben meegewogen bij de totstandkoming van de output.
- Inventariseren en vastleggen (bijvoorbeeld via een algoritmeregister) van de toepassingen van AI binnen een instelling.

Rekenschap. Rekenschap afleggen betekent verantwoordelijkheid nemen. Zeker bij conflicterende belangen is het van belang dat een instelling een zorgvuldige afweging maakt en deze afweging en keuze gedocumenteerd vastlegt (bijvoorbeeld in het Register van Verwerkingen of in een algoritmeregister). Instellingen maken inzichtelijk wie verantwoordelijk dan wel aanspreekbaar is bij twijfels over een bepaald gebruik van studiedata en AI.

Onder rekenschap afleggen, valt ook het aanspreekbaar zijn op de vraag naar nut en noodzaak van het gebruik van studiedata en AI en op de vraag hoe instellingen rekening hebben gehouden met de legitieme belangen van betrokkenen, eventuele andere belanghebbenden en de maatschappelijke en sociale aspecten. Instellingen dienen, in het kader van het afleggen van rekenschap, blijvend te toetsen of het nagestreefde doel van het gebruik van studiedata en AI bereikt is en/of aanpassingen nodig en gewenst zijn.

De instelling moet kunnen blijven uitleggen waarom en op basis waarvan bepaalde keuzes worden gemaakt, ongeacht of dit beleidsmatige keuzes zijn of keuzes die een individu zeer direct raken. Daar komt bij dat het gebruiken van (nieuwe) technieken nooit een doel op zich moet zijn, maar een middel om het (hoger) doel te bereiken.

Plan-Do-Check-Act (PDCA)

Een beproefde methode is het aanhouden van een PDCA-cyclus. In het kort betekent dit een gefaseerde aanpak met deze stappen:

- **Plan:** Bekijk de werkzaamheden en stel een plan op voor de uitvoering daarvan.
- **Do:** Voer de werkzaamheden van het plan uit.
- **Check:** Kijk naar de voortgang van de uitgevoerde werkzaamheden en inventariseer de risico's/knelpunten bij de uitvoering.
- **Act:** Pas de werkzaamheden/plan aan op basis van de gevonden resultaten.

De verantwoording over wat kan en mag met studiedata en AI is geen eenrichtingsverkeer. Studenten, docenten, ondersteuners en andere betrokkenen mogen verwachten dat de instelling hen actief betreft bij de keuzes rond het gebruik van studiedata en AI en hen – waar relevant – actief informeert over de realisatie van de (beoogde) doelen, de eventueel optredende risico's en de te nemen maatregelen om die risico's te beperken. Zo blijven instellingen in een voortdurende dialoog met alle betrokkenen en dragen ze daarmee bij aan het uitdragen van een cultuur van verantwoord gebruik van studiedata en AI.

Het betrekken van gremia als een studentenraad en/of een ondernemingsraad bij de inzet van studiedata en AI kan in bepaalde situaties een wettelijke verplichting zijn.

3.2.3 Enkele vragen/dilemma's rond de waarde rechtvaardigheid

- Zijn er toepassingen van studiedata en AI in het onderwijs ten behoeve van de student die als onaanvaardbaar moeten worden beschouwd, ongeacht de mogelijke voordelen van het gebruik van studiedata en AI voor bepaalde groepen van studenten? Zo ja, wat zijn de factoren die bepalen of een toepassing onaanvaardbaar is?
- Is het doel dat de instelling wil bereiken met het gebruik van studiedata en AI voldoende duidelijk en meetbaar? Hebben we voldoende en representatieve studiedata voor het bereiken van dit doel?
- Hoe worden studenten en docenten die worden geraakt door het gebruik van studiedata en AI hierover geïnformeerd? Krijgen zij betekenisvolle uitleg als er belangrijke beslissingen worden genomen? Hoe is dat geborgd?
- Waar kunnen studenten en docenten terecht met hun vragen, zorgen en klachten? Hoe handelt de instelling deze af?
- Hoe blijven de studiedata en de werking van de AI veilig en betrouwbaar? Hoe houdt de instelling het gebruik van studiedata en AI bij en hoe monitort zij de werking? En wie binnen de instelling doet dat?

3.3 MENSELIJKHEID

3.3.1 Wat houdt menselijkheid in?

De Waardenwijzer voor digitalisering in het onderwijs omschrijft wat menselijkheid inhoudt.

Menselijkheid betekent oog voor de mens in het onderwijs. Het gaat om sociale samenhang, betekenisvol contact, respect, veiligheid, gezondheid en welzijn en zelfontplooiing. Onderwijsinstellingen zorgen voor sociale verbondenheid, ontmoetingen en betekenisvol contact. De onderwijsinstelling heeft daarbij respect voor het unieke karakter van elke leerling en student die als mens gezien en gehoord wordt, en niet behandeld wordt als nummer of radartje in een systeem. Ze bieden een veilige omgeving, zowel online, fysiek als mentaal, waarbij de gezondheid en het welzijn van leerlingen en studenten gewaarborgd worden. Een omgeving waarin het mogelijk is om fouten te kunnen maken zonder dat die buiten de onderwijscontext impact hebben. De menselijke blik blijft in het onderwijs voorop staan: er worden geen beslissingen genomen of oordelen geveld over leerlingen of studenten die louter gebaseerd zijn op de analyse van data. Onderwijs levert een bijdrage aan zelfontplooiing: het tot uitdrukking brengen van het individuele karakter van leerlingen en studenten in relatie tot de wereld.

3.3.2 Menselijkheid en het gebruik van studiedata en AI

Maar wat betekent menselijkheid in het kader van het gebruik van studiedata en AI?

Betekenisvol contact

Betekenisvol contact gaat over interacties tussen docent en student en tussen studenten op het gebied van onder meer studeren en ontwikkeling. De instelling zorgt ervoor dat het gebruik van studiedata en AI niet in de weg staat van betekenisvol contact tussen docenten en studenten en tussen studenten onderling. Deze interacties dragen bij aan het leer- en ontwikkelingsproces.

Zelfontplooiing

Zelfontplooiing is de mogelijkheid van een individu om zichzelf te ontwikkelen in een veilige en respectvolle omgeving. Dat betreft zowel studenten als docenten. De instelling waarborgt dat het gebruik van studiedata en AI hierop is gericht en draagt bij aan het helpen van studenten hun eigen leertrajecten te bepalen en hun vaardigheden en interesses in verschillende gebieden te verbreden. De instelling zorgt bij het gebruik van studiedata en AI er ook voor dat de docenten voldoende ruimte en vrijheid houden bij de ontwikkeling van lesmaterialen en het geven van onderwijs.

Menselijke blik

Oog houden voor de menselijke blik is cruciaal, zeker wanneer studiedata en AI geautomatiseerd worden gebruikt. Instellingen zorgen dat altijd een mens betrokken is bij geautomatiseerd

gebruik van studiedata en AI: de menselijke tussenkomst. Dit geldt bij automatische processen met (mogelijk) gevolgen voor individuele of kleine groepen identificeerbare studenten en docenten. Het geldt echter ook voor de controle op de input, werking en output van de gebruikte studiedata en AI. De instelling zorgt ervoor dat een betrokkene op een makkelijke manier bezwaar kan maken tegen een (deels) automatisch gemaakte beslissing en dat een deskundige en beslissingsbevoegde snel en met redenen omkleed reageert op dit bezwaar.

Procedures voor de verwerking, analyse en benutting van studiedata en AI en interventies worden zorgvuldig ontworpen en regelmatig herzien (bijvoorbeeld via de PDCA-cyclus). Instellingen erkennen in dat kader ook dat geautomatiseerde analyses van studiedata en AI waarschijnlijk geen volledig beeld kunnen geven van iemands leerproces en dat niet altijd de persoonlijke omstandigheden kunnen worden meegenomen.

3.3.3 Enkele vragen/dilemma's rond de waarde menselijkheid

- Wat is de rol van het gebruik van studiedata en AI in educatieve beslissingen? Moet die rol alleen ondersteunend zijn of kan het ook verder gaan? En wanneer en in welke mate moet er een menselijke tussenkomst zijn?
- Hoe kunnen we de balans vinden tussen het gebruik van studiedata en AI voor individuele optimalisering van studie en leerprocessen enerzijds en het behouden van betekenisvol contact en zelfontplooiing in het onderwijs anderzijds?
- Hoe voorkomen we dat de blik op de student te veel vormgegeven wordt door studiedata en AI waardoor de mens achter de data verdwijnt?
- Beschikken docenten en andere professionals over de benodigde opleiding en informatie om studiedata en AI doeltreffend te gebruiken en ervoor te zorgen dat het veilig is en geen schade toebrengt aan of inbreuk maakt op de rechten van studenten?
- Is er bewust nagedacht over hoe de instelling de student, docent en andere medewerkers als mens blijft benaderen? En in welke mate doet het gebruik van studiedata en AI daaraan af of draagt het daaraan juist bij?

3.4 AUTONOMIE

3.4.1 Wat houdt autonomie in?

De Waardenwijzer voor digitalisering in het onderwijs omschrijft wat autonomie inhoudt.

Autonomie betekent letterlijk: jezelf de wet voorschrijven. Autonomie omvat waarden als zelfbeschikking, bescherming van de persoonlijke levenssfeer, onafhankelijkheid en vrijheid van onderwijs. Leerlingen en studenten hebben zelfbeschikking: zij krijgen voldoende keuzevrijheid om het onderwijs te volgen dat bij hen past en zijn autonoom in hun ontwikkeling en keuzes. Bescherming van de persoonlijke levenssfeer is een belangrijk onderdeel van autonomie: leraren, docenten en leerlingen en studenten moeten erop kunnen vertrouwen dat hun privacy goed gewaarborgd is als zij met digitale middelen van hun instelling werken en zelf bepalen wat er met hun data gebeurt. Onafhankelijkheid van onderwijs houdt in dat instellingen hun onderwijs vrij van externe beïnvloeding kunnen vormgeven. Professionals in het onderwijs hebben de ruimte om op basis van hun professionele autonomie eigen inschattingen en keuzes te maken bij het begeleiden van studenten. Vrijheid van onderwijs wil zeggen dat onderwijsinstellingen hun onderwijs vorm kunnen geven op basis van hun eigen signatuur en overtuigingen binnen de grenzen van de wet en passend in een vrije, pluriforme en democratische samenleving.

3.4.2 Autonomie en het gebruik van studiedata en AI

Maar wat betekent autonomie in het kader van het gebruik van studiedata en AI?

Zelfbeschikking

Zelfbeschikking van een student verwijst naar het vermogen en de vrijheid om eigen keuzes te maken, zelfstandig te handelen en controle uit te oefenen over het eigen leven en onderwijs. Het spoort studenten aan tot actieve deelname aan leerprocessen en bereidt hen ook voor op het leven na de studie. Instellingen zorgen ervoor dat het gebruik van studiedata en AI niet leidt tot onevenredige beperkingen in zelfbeschikking als het gaat om keuzes in het studieproces, leerpaden en ontwikkelingsrichtingen. Het gebruik van studiedata en AI is een hulpmiddel dat studenten ondersteunt en niet een systeem dat beslissingen voor hen neemt zonder hun input of keuze.

Onafhankelijkheid

De onafhankelijkheid van onderwijs en docenten in relatie tot het gebruik van studiedata en AI roept belangrijke vragen op over hoe technologie kan worden geïntegreerd zonder de kernwaarden van onderwijs en de professionele autonomie van docenten te ondermijnen. Instellingen zetten studiedata en AI in als een hulpmiddel dat docenten ondersteunt, niet ter vervanging. Een veel genoemd doel van inzet van studiedata en AI is het ontlasten van docenten van – vooral – routinematige taken zodat ze meer tijd en energie kunnen besteden

aan interactie met studenten. Voor een betekenisvolle rol als docent is professionele autonomie belangrijk. Dit houdt in dat onderwijsprofessionals altijd invloed moeten kunnen uitoefenen bij inhoudelijke en pedagogische keuzes binnen het onderwijsproces.

Bescherming persoonlijke levenssfeer

Het gebruik van studiedata en AI betekent het verzamelen en gebruiken van veel gegevens en persoonsgegevens van vooral studenten en docenten. Dat roept veel vragen op rond de bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens van studenten, docenten en andere betrokkenen. Veel studiedata kunnen als gevoelig worden beschouwd omdat het informatie is over de intellectuele capaciteiten, leerstoornissen en soms zelfs over de emotionele en psychologische toestand van studenten. Instellingen verzamelen en gebruiken alleen die studiedata die geschikt zijn voor het bereiken van het vooraf welbepaalde doel. Daarnaast is het belangrijk dat instellingen transparant zijn over het gebruik en dat studenten goed worden geïnformeerd over dat gebruik en de rechten die ze kunnen uitoefenen.

3.4.3 Enkele vragen/dilemma's rond de waarde autonomie

- Hoe voorkomen we dat te veel op het gebruik van studiedata en AI wordt vertrouwd en/of de afhankelijkheid ervan te groot wordt?
- In hoeverre staat de zelfontwikkeling van de student op gespannen voet met de belangen van de instelling en het bewaken van de kwaliteit van het onderwijs?
- Moeten studenten het recht hebben om *niet* deel te nemen aan gebruik van studiedata en AI, ook al heeft dat negatieve invloed op hun studieontwikkeling?
- Blijft er nog ruimte over voor studenten om hun eigen leerpaden te kiezen en beslissingen te nemen zonder inmenging van bijvoorbeeld voorspellende of aanbevelende algoritmes of AI?
- Hoe ver mag een instelling gaan bij het monitoren van studentengedrag voor educatieve doeleinden? Zou er een limiet moeten zijn aan welke studiedata de instellingen mogen verzamelen, zelfs als meer data kunnen leiden tot betere educatieve uitkomsten?
- Wat is nog de ruimte voor de docent om zelf inhoud en richting van het onderwijs te bepalen?

4. Wettelijk kader: AVG

4.1 Relevante begrippen

Studiedata zijn **persoonsgegevens** bij informatie die direct of indirect leidt tot de identificatie van studenten, aankomend studenten, belangstellenden, oud-studenten, docenten, begeleiders en alle andere personen van wie persoonsgegevens worden verwerkt (de ‘betrokkenen’ in de zin van de AVG).

De AVG onderscheidt de volgende persoonsgegevens:

- ‘gewone’ persoonsgegevens, bijvoorbeeld naam, e-mailadres, opleiding, studentnummer, behaalde studieresultaten, studieadviezen, gebruikte leermiddelen, studievoortgang en sociaaleconomische informatie;

▶ Hoewel de AVG formeel geen onderscheid maakt, zijn sommige persoonsgegevens, zoals studieresultaten en studieadviezen, te beschouwen als *gevoelige* persoonsgegevens. Bescherming van deze gevoelige persoonsgegevens verdient extra aandacht.

- bijzondere persoonsgegevens⁵, bijvoorbeeld gegevens over functiebeperkingen of gegevens waaruit politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken;
- persoonsgegevens betreffende strafrechtelijke veroordelingen, strafbare feiten en met burgerservicenummer (bsn).

▶ Pseudonimiseren en anonimiseren

De termen pseudonimiseren en anonimiseren worden veel gebruikt als het gaat om privacy en de bescherming van persoonsgegevens. Het belangrijkste verschil tussen deze termen is dat pseudonieme gegevens nog steeds persoonsgegevens zijn waarop de AVG van toepassing is. Van anonimiseren is sprake als gegevens, bijvoorbeeld door aggregatie, redelijkerwijs niet (meer) herleidbaar zijn tot een individu. De AVG geldt niet bij het gebruik van anonieme gegevens.

⁵ Bijzondere persoonsgegevens zijn persoonsgegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond, maar ook genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over de gezondheid of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Het verwijderen van de naam van een persoon of het vervangen van de naam door een nummer betekent niet per definitie dat de gegevens anoniem zijn, al helemaal niet als er ergens nog een document bestaat waarmee het nummer terug te herleiden is naar een naam. Echter, ook als een dergelijk document niet bestaat, is de kans groot dat de overgebleven gegevens, al dan niet in combinatie met andere informatie of documenten, direct of indirect herleidbaar zijn tot een persoon.

In de praktijk zal daarom eerder sprake zijn van pseudonieme gegevens dan van anonieme gegevens.

Zie voor een overzicht van het begrip pseudonimiseren en verschillende technieken van pseudonimisering de ENISA [recommendations on shaping technology according to-TP0618398ENN.pdf](#)

De AVG is technologie-neutraal geformuleerd en verwijst niet naar specifieke technologische toepassingen waaronder AI of machine learning. De AVG richt zich op persoonsgegevens en geeft verschillende regels, afhankelijk van de aard van de persoonsgegevens.

Zo mogen ‘gewone’ persoonsgegevens – kort gezegd – alleen worden gebruikt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen, als een wettelijke grondslag aanwezig is en de persoonsgegevens zorgvuldig worden verwerkt.

Bijzondere persoonsgegevens, strafrechtelijke persoonsgegevens en bsn niet gebruiken als studiedata

De AVG kent een verbod op het verwerken van *bijzondere persoonsgegevens* met een beperkt aantal duidelijk omschreven uitzonderingen op dat verbod. Het Referentiekader hanteert als uitgangspunt dat bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens in principe niet mogen worden gebruikt als studiedata. Indien een instelling dit toch overweegt, is het belangrijk contact op te nemen met de functionaris gegevensbescherming, privacy officer of juridisch deskundige van de instelling.

Het bsn mag alléén worden gebruikt als de wet daar expliciet in voorziet. Zo mogen instellingen het bsn verwerken voor de inschrijving en communicatie met overheidsinstanties. Het Referentiekader hanteert als uitgangspunt dat het bsn niet voor andere doeleinden mag worden gebruikt, dus ook niet als kenmerk om databases of bestanden te koppelen.

Als studiedata persoonsgegevens zijn, dan is het gebruik door een instelling van studiedata een **verwerking** van persoonsgegevens volgens de AVG. Het begrip ‘verwerken’ is een breed

begrip en bevat onder meer het opslaan, inzien, aanpassen, koppelen met andere bestanden, doorsturen, publiceren en daadwerkelijk gebruiken van persoonsgegevens.

Kortom, de AVG is van toepassing op het gebruik van studiedata (persoonsgegevens) en AI. Als het Referentiekader in het vervolg spreekt over studiedata dan zijn dat ook persoonsgegevens, tenzij anders wordt aangegeven.

Dit Referentiekader hanteert als uitgangspunt dat de instellingen (alleen of samen met anderen) het doel en de middelen rond het gebruik van persoonsgegevens bepalen. Deze instellingen zijn te kwalificeren als (gezamenlijke) **verwerkingsverantwoordelijke(n)**.

Wie is verwerkingsverantwoordelijke: de instelling of de medewerker?

De instelling is de verwerkingsverantwoordelijke volgens de AVG. Medewerkers van een instelling die persoonsgegevens/studiedata gebruiken in het kader van hun werkzaamheden zijn zelf géén verwerkingsverantwoordelijke volgens de AVG.

4.2 Doel-grondslag-zorgvuldigheid

De impact van de AVG op het gebruik van studiedata laat zich als volgt kort samenvatten:

DOEL

Waarom wil je persoonsgegevens verwerken?

GRONDSLAG

Wat is de juridische grondslag voor deze verwerking?

ZORGVULDIGHEID

Hoe zorg je ervoor dat je op een zorgvuldige manier met de gegevens omgaat?

4.2.1 Doel en doelbinding

Studiedata moeten voor een *welbepaald, uitdrukkelijk omschreven en gerechtvaardigd* doel worden gebruikt en mogen niet zomaar verder worden verwerkt voor andere doeleinden. Dat betekent allereerst dat moet worden vastgesteld wat het beoogde doel (of doelen) is van het gebruik van studiedata en welke studiedata daarvoor noodzakelijk zijn.

Het doel, of de doelen, moet(en) zo welbepaald en specifiek mogelijk geformuleerd zijn. Slechts verwijzen naar de algemene doelen van ‘verbetering van het onderwijs’, het ‘optimaliseren van onderwijsprocessen’ of het ‘doen van individuele interventies’, is niet voldoende specifiek.

Studiedata mogen dus alleen worden gebruikt voor een specifiek doel (doelbinding). Bij het gebruik van studiedata zal het echter bijna altijd gaan om een *verdere* verwerking van die data. De studiedata zullen immers niet initieel zijn verzameld voor bijvoorbeeld een specifiek doel als het inzichtelijk maken van in-/door- of uitstroom van studenten of het inzichtelijk maken van factoren voor studiesucces.

Overigens mag een verdere verwerking van studiedata wel met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, *mits* een aantal passende waarborgen voor de rechten en vrijheden van betrokkenen is getroffen. Denk daarbij aan technische en organisatorische maatregelen voor het waarborgen van dataminimalisering of aan pseudonimisering.

Of een verdere verwerking van studiedata voor een nieuw doel (anders dan hiervoor in het kader staat) mogelijk is, vraagt om een afweging van de instelling. De volgende factoren spelen daarbij een rol: de nabijheid van het nieuwe doel met het initiële doel, de verwachtingen die betrokkenen hebben, de context en aard van het verdere gebruik, de aard van de studiedata en de mogelijke gevolgen voor de betrokkenen. Een instelling moet deze afweging schriftelijk vastleggen.

Als een nieuw doel *niet* verenigbaar is, is het niet toegestaan om de studiedata verder te gebruiken voor het nieuwe doel, tenzij er een zelfstandige grondslag is voor het verwerken van de studiedata voor het nieuwe doel. Uiteraard dient die grondslag ook te voldoen aan de eisen die de AVG daaraan stelt (zie hierna).

4.2.2 Juridische grondslag

Het gebruik van gewone studiedata vereist de aanwezigheid van een (geldige) grondslag zoals opgesomd in de AVG. Die grondslagen zijn:

- **Toestemming** van de betrokkene. De toestemming moet vrij, geïnformeerd, specifiek en ondubbelzinnig gegeven zijn. De toestemming kan altijd worden ingetrokken. Het is tegen deze achtergrond belangrijk dat een instelling niet alleen goed weet bij wie en waar de toestemmingen zijn opgeslagen maar ook een procedure heeft voor waar en hoe verzoeken tot intrekking worden ingediend en afgewikkeld.

Toestemming bij kinderen

De bescherming van persoonsgegevens van kinderen verdient speciale aandacht en kent een aantal extra eisen. Zo kunnen kinderen onder de 16 jaar zelf geen geldige toestemming geven. Dat kunnen hun ouders of voogden doen.

De instelling kan de toestemming van de ouder/voogd niet zomaar aannemen.

De instelling heeft de plicht redelijke inspanningen te verrichten om te controleren of de ouder/voogd die toestemming daadwerkelijk heeft gegeven, bijvoorbeeld door controles uit te voeren om de leeftijd van het kind te verifiëren.

- Noodzakelijk bij de uitvoering van een **overeenkomst** waarbij betrokkene partij is.
- Noodzakelijk om te voldoen aan een **wettelijke verplichting** door de instelling. De wettelijke verplichting, waaronder ook lagere wet- en regelgeving, moet dan wel duidelijk en nauwkeurig zijn en de toepassing voldoende voorspelbaar.

Voorbeeld wettelijke verplichting: voortgangsrapportage

Een voorbeeld van een wettelijke verplichting is artikel 7.1.5 van de Wet educatie en beroepsonderwijs (WEB). Dit artikel verplicht instellingen in het mbo over de voorde- ringen van de studenten te rapporteren aan hun ouders, voogden of verzorgers dan wel aan de studenten zelf als zij meerderjarig (en handelingsbekwaam) zijn.

- Noodzakelijk voor de vrijwaring van de **vitale belangen** van de betrokkene.
- Noodzakelijk voor een taak in het **algemeen belang** of uitvoering van het openbaar gezag door de instelling.

Voorbeeld algemeen belang

Instellingen hebben een zorgplicht naar hun studenten bijvoorbeeld rondom het bevorderen van welzijn. De grondslag wettelijke verplichting zou in aanmerking kunnen komen als de betreffende wettelijke verplichting duidelijk en nauwkeurig is en voldoende voorspelbaar (voor wat betreft het gebruik van studiedata) voor de studenten. Meestal is dat niet het geval en ligt de grondslag algemeen belang (of toestemming) meer voor de hand.

Instellingen zouden voor verwerkingen van studiedata voor het bieden (verbeteren) van onderwijs gebruik kunnen maken van deze grondslag. Het geven van onderwijs door instellingen is immers een taak van algemeen belang.

- Noodzakelijk voor de **gerechtvaardigde belangen** van de instelling of een derde. Het is wel belangrijk dat een gerechtvaardigd belang goed wordt onderbouwd, dat een afweging plaatsvindt tussen de belangen van de instelling of een derde enerzijds en de belangen van betrokkenen anderzijds én dat de betrokkenen hierover worden geïnformeerd.

Voorbeeld gerechtvaardigd belang

Verwerkingen van studiedata die alléén betrekking hebben op verbeteringen van bedrijfsprocessen van de instellingen kunnen op deze grondslag worden gebaseerd.

Bij alle grondslagen, met uitzondering van toestemming, geldt de eis dat de verwerking van persoonsgegevens ‘noodzakelijk’ is. Maar wat houdt dat in? Heel kort: proportionaliteit en subsidiariteit.

Proportionaliteit: het doel van de verwerking moet in verhouding staan tot de nadelige gevolgen voor de privacy van betrokkenen. Belangrijke gezichtspunten zijn de mate waarin de verwerking bijdraagt aan het doel, de aard en omvang van de te verwerken persoonsgegevens en de mogelijke gevolgen voor de betrokkenen.

Subsidiariteit: als een doel van de verwerking met minder of geen persoonsgegevens kan worden bereikt, dan moet die manier worden gekozen. In dit kader komt belang toe aan het bestaan van alternatieven. Zijn die er? Heeft de instelling hiernaar gekeken? Hoe zijn deze beoordeeld en gewogen?

Welke grondslag een instelling kan gebruiken, hangt af van de specifieke toepassing van het gebruik van studiedata. De instelling bepaalt per toepassing welke grondslag het meest passend is.

Aantekeningen bij de grondslag toestemming

Bij het gebruik van de grondslag toestemming is het belangrijk het volgende te bedenken:

- Is een toestemming daadwerkelijk ‘vrij’ gegeven? Dus zonder dwang of drang. Dat blijft gezien de verhouding tussen instelling enerzijds en docent en student anderzijds een aandachtspunt. Als de toestemming niet vrij is gegeven, kan de gegeven toestemming niet als grondslag dienen.
- De toestemming moet geïnformeerd zijn gegeven. Dat betekent dat de betrokkene alle informatie moet hebben om een goed afgewogen keuze te maken om al dan niet in te stemmen met de voorgenomen verwerking van persoonsgegevens.
- Het geven van toestemming betekent dat een betrokkene die toestemming altijd kan intrekken, waarna die studiedata niet meer mogen worden gebruikt. Instellingen dienen dit goed in te regelen.
- Als een deel van de studenten toestemming geeft voor het gebruik van studiedata en een deel niet, bestaat het gevaar dat er ongelijkheid ontstaat tussen verschillende groepen studenten. Dat raakt het aspect van kansengelijkheid.

De keuze van een instelling voor grondslag voor het gebruik van studiedata en AI luistert nauw. Het is belangrijk dat een instelling hierover contact opneemt met de privacy-deskundige binnen de instelling, bijvoorbeeld de privacy officer, de privacy jurist of de functionaris gegevensbescherming (FG).

4.2.3 Zorgvuldigheid

De brede noemer zorgvuldigheid waakt over alle verplichtingen (die rusten op instellingen) die ervoor zorgen dat op een verantwoorde manier met studiedata wordt omgegaan.

Van die verplichtingen is het **recht op informatie** van betrokkenen van cruciaal belang. Instellingen moeten betrokkenen op een duidelijke manier informeren over onder meer welke studiedata van hen worden gebruikt, voor welke doelen dat gebeurt, wat voor dat gebruik de grondslag is en welke beveiligingsmaatregelen de instelling treft voor een veilig en zorgvuldig gebruik van studiedata. Die informatie kan het beste worden gegeven op het moment dat de studiedata daadwerkelijk gebruikt gaan worden.

Informeren van kinderen

Bij het informeren van kinderen (jonger dan 16 jaar) moet rekening worden gehouden met het feit dat het kinderen zijn. Dat betekent ook informeren op zo’n manier dat kinderen dit kunnen begrijpen. Dus geen al te moeilijke woorden en lange zinnen.

Daarnaast de volgende verplichtingen:

Dataminimalisatie; alleen die studiedata die noodzakelijk zijn voor het realiseren van het beoogde doel mogen worden verwerkt. Als het niet of niet langer nodig is om direct identificerende gegevens te gebruiken, verwijder, anonimiseer of pseudonimiseer de studiedata dan zo snel mogelijk.

Pseudonimiseren is een belangrijke maatregel voor de bescherming van persoonsgegevens en de AVG noemt deze maatregel dan ook expliciet. Doorgaans is het aan te bevelen persoonsgegevens zo veel en zo snel als mogelijk te pseudonimiseren.

Privacy by default en privacy by design; al bij het bedenken en ontwikkelen van nieuwe toepassingen of technologieën moet aandacht worden besteed aan de technische en organisatorische (beveiligings)maatregelen ter bescherming van persoonsgegevens. Dit heet ook wel *privacy by design*. Daarnaast moeten de instellingen toepassingen, applicaties en systemen standaard zo privacyvriendelijk mogelijk instellen. Dit heet ook wel *privacy by default*.

SURF heeft informatie beschikbaar over *privacy by design* en *privacy by default*: surf.nl/privacy-by-design-en-privacy-by-default.

Juistheid; de studiedata die worden verwerkt moeten correct en volledig zijn.

Data Protection Impact Assessment; een *Data Protection Impact Assessment* (DPIA) is een beoordeling van de risico’s op de gegevensbescherming bij een (voorgenomen) gebruik van

studiedata. Als een verwerking waarschijnlijk een hoog risico met zich meebrengt voor de betrokkene(n) is het uitvoeren van een DPIA verplicht. Dit vraagt van de instelling een analyse op basis van de aard, omvang, context en doeleinden van de verwerking. In de volgende gevallen zal een DPIA moeten worden uitgevoerd:

- Bij een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd die rechtsgevolgen hebben of anderszins de persoon aanzienlijk treffen.
- Als op grote schaal bijzondere persoonsgegevens worden verwerkt.
- Als op een stelselmatige of grootschalige wijze openbare ruimten worden gemonitord.

Het Referentiekader hanteert als uitgangspunt dat in alle gevallen bij het gebruik van studiedata met behulp van (of in combinatie met) AI, dit de kwalificatie hoog risico draagt in de zin van de AI Act (zie hierna in hoofdstuk 5). Het uitvoeren van een DPIA is dan altijd noodzakelijk.

De Autoriteit Persoonsgegevens ('AP') en de Europese privacy-autoriteiten hebben daarnaast een lijst van criteria opgesteld om te beoordelen of sprake is van een hoog risico.⁶

Een DPIA kan vormvrij worden uitgevoerd maar moet wel uit een aantal verplichte onderdelen bestaan.

Bewaartermijnen; studiedata mogen niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor de studiedata worden gebruikt. Voor zover het noodzakelijk is voor historisch of wetenschappelijk onderzoek mogen studiedata langer worden opgeslagen, mits passende technische en organisatorische waarborgen worden getroffen.

Informatiebeveiliging; de instelling treft passende technische en organisatorische maatregelen (zoals pseudonimiseren en het versleutelen van studiedata, het garanderen van de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de systemen en het regelmatig testen en evalueren van de genomen maatregelen). Deze maatregelen zijn gebaseerd op een risico-inschatting van de verwerking zodat sprake is van een passende beveiliging van studiedata.

SURF heeft hierover veel informatie beschikbaar op de website: surf.nl/informatiebeveiliging

⁶ Zie de website van de AP en de EDPB Guidelines on Data Protection Impact Assessments (WP 248)

Rechten van betrokkenen; betrokkenen hebben een aantal belangrijke rechten met betrekking tot het gebruik van hun studiedata: recht op inzage (en in voorkomend geval ook recht op kopieën van die studiedata), recht op correctie, recht op verwijdering, recht op beperking van de verwerking, recht bezwaar te maken en het recht op dataportabiliteit.

Daarnaast heeft de betrokkene het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Op deze regel geldt een aantal uitzonderingen, bijvoorbeeld als de betrokkene hiervoor uitdrukkelijke toestemming geeft.

Waar het in het kader van het Referentiekader vooral om draait is het aspect van *uitsluitend* geautomatiseerde verwerking, bijvoorbeeld bij beslissingen over toegang en toelating tot het onderwijs. Uit rechtspraak volgt dat van 'uitsluitend' sprake is als er *géén* betekenisvolle menselijke tussenkomst is door personen met voldoende competenties en bevoegdheden om beslissingen te beïnvloeden en zelfs terug te draaien.

Uitsluitend geautomatiseerde besluitvorming en kinderen

Enige onduidelijkheid bestaat over de vraag of kinderen (jonger dan 16 jaar) in het geheel niet onderworpen mogen worden aan uitsluitend geautomatiseerde besluitvorming (waaronder profilering). Hoewel de tekst van het betreffende artikel in de AVG een dergelijk absoluut niet lijkt te ondersteunen, hanteren de Europese toezichthouders verenigd in de Werkgroep 29 (thans de EDPB) als uitgangspunt dat kinderen *niet* mogen worden onderworpen aan uitsluitend geautomatiseerde besluitvorming en er dus geen beroep mogelijk is op de AVG-wettelijke uitzonderingen.

Om zaken nog gecompliceerder te maken, erkent de voorloper van de Europese Data Protection Board EDPB, de zogenoemde Werkgroep 29, wel de mogelijkheid van uitsluitend geautomatiseerde besluitvorming bij kinderen als dat bijvoorbeeld ter bescherming van hun welzijn is. In deze gevallen moeten er wel voor kinderen passende beschermingsmaatregelen worden getroffen.

Het advies aan de instellingen is zorg te dragen dat geen sprake is van uitsluitend geautomatiseerde besluitvorming bij kinderen. Als een instelling dit toch wenst, is het verstandig contact op te nemen met de FG, een privacy officer of juridisch deskundige.

Uitwisseling van studiedata: met andere instellingen, (stage)bedrijven en (gemeentelijke) jeugd(zorg)instellingen, gemeenten, leerplichtambtenaren RMC-trajectbegeleiders, uitkeringsinstanties en domein Veiligheid.

Veel instellingen werken samen met andere instellingen en (stage)bedrijven. Vooral stage-bedrijven spelen in meer of mindere mate een rol bij de opleiding van studenten en afgezien dat zij zelf studiedata kunnen genereren, kunnen zij van instellingen ook studiedata ontvangen. Dergelijke uitwisselingen zijn verwerkingen in de zin van de AVG en zijn toegestaan mits is voldaan aan de drieslag: doel – grondslag – zorgvuldigheid. In het kader van de zorgvuldigheid maken de instellingen en (stage)bedrijven afspraken over onder meer het gebruik, de beveiliging van de studiedata en de wijze van uitwisseling van studiedata.

In bepaalde situaties schrijft de AVG ook een specifieke overeenkomst voor. Denk vooral aan een verwerkersovereenkomst of aan een regeling die een aantal zaken regelt als er twee of meerdere partijen gezamenlijk verwerkingsverantwoordelijken zijn.

Daarnaast kunnen instellingen te maken hebben/krijgen met verschillende overheidsinstanties, zoals gemeenten, jeugd(zorg)instellingen en uitkeringsinstanties. Uitwisseling van studiedata is hier eveneens mogelijk mits is voldaan aan: doel(binding) – grondslag – zorgvuldigheid.

Zie voor het mbo meer informatie: servicedocument Delen van persoonsgegevens tussen onderwijs en zorg (met arbeid) op [Privacy | MBO Raad](#).

4.3 (Generatieve) AI en de AVG

De AVG is van toepassing op het gebruik van studiedata. Dat is ook het geval als de studiedata worden gebruikt met behulp van (generatieve) AI. De beginselen van de AVG, zoals die in dit hoofdstuk staan, gelden onverkort voor het verwerken van studiedata met behulp van (generatieve) AI.

Maar waar en hoe precies werken de AVG-beginselen door bij (generatieve) AI? Vooral bij generatieve AI waar persoonsgegevens in verschillende fasen van de *lifecycle* worden gebruikt, doen zich per fase enkele bijzonderheden en moeilijkheden voor, onder meer rond doel(binding), grondslagen, informatieverstrekking, rechten van betrokkenen en dataminimalisatie.

Praatplaat SURF

SURF heeft een 'praatplaat' gepubliceerd waarin in een oogopslag duidelijk wordt waar de AVG in beeld komt inclusief een toelichting, zie: [Praatplaat AI en Privacy – Privacy Expertise Centrum](#).

Toeziethouders

De European Data Protection Board (EDPB) heeft een opinie uitgebracht waarin nader

wordt ingegaan op verschillende aspecten van gegevensbescherming in de context van AI modellen, Zie: [edpb_opinion_202428_ai-models_en.pdf](#).

Verder hebben de Franse en Engelse toezichthouders – de CNIL en de ICO – aanbevelingen/richtlijnen gepubliceerd voor de ontwikkelingsfase van AI-systemen en hoe de risico's rond gegevensbescherming in AI-projecten beperkt kunnen worden. Zie: [AI: CNIL publishes its first recommendations on the development of artificial intelligence systems | CNIL](#) en [Guidance on AI and data protection | ICO](#).

De Belgische Gegevensbeschermingsautoriteit heeft een informatiebrochure –systemen en de AVG (en de wisselwerking tussen de AVG en de AI Act in de context van de ontwikkeling van AI-systemen). Zie: [informatiebrochure-over-artificiele-intelligentiesystemen-en-de-avg.pdf](#).

Hoewel er veel discussie en onduidelijkheid is over de hoe de eisen van de AVG invulling krijgen bij vooral generatieve AI, is het verbieden van het gebruik van generatieve AI binnen instellingen niet altijd een optie. Niet alleen vanwege de ruime, makkelijke en veelal gratis beschikbaarheid van generatieve AI, maar ook door het inzicht dat het goed is dat studenten en docenten kunnen experimenteren met en leren van generatieve AI.

De meeste instellingen gebruiken daarom vooral richtlijnen, adviezen en andere regels voor het verantwoord gebruik van generatieve AI in onderwijs. Kern van die richtlijnen is dat het voorwaarden stelt voor het gebruik van generatieve AI. Denk daarbij aan onder meer het volgende:

- (i) Waarvoor mag generatieve AI worden gebruikt (en waarvoor niet)?
- (ii) Wat zijn de voorwaarden als gebruik is toegestaan (bijvoorbeeld geen persoonsgegevens, studenten blijven zelf verantwoordelijk, etc.)?

Generatieve AI in het onderwijs

Een mooi voorbeeld van een dergelijke richtlijn is de HvA: Generatieve AI in onderwijs: regels en adviezen, Hogeschool van Amsterdam (april 2024), zie: [generatieve-ai-in-onderwijs-regels-en-adviezen-extern.pdf](#)

5. Wettelijk kader: AI Act

5.1 Inleiding

Op 2 augustus 2024 ging de AI Act in werking. De AI Act is onderdeel van een breder Europees regelgevingskader over productregulering waar het in de kern gaat om veilige en betrouwbare producten.

De AI Act heeft als belangrijk doel ervoor te zorgen dat AI-systemen verantwoord en veilig worden gebruikt in zowel de private als publieke sector. De AI Act is van toepassing als AI-systemen worden verhandeld of gebruikt in de EU of wanneer de output van het AI-systeem in de EU wordt gebruikt.

▶ Wanneer is de AI Act niet van toepassing?

De AI Act is *niet* van toepassing bij alleen een persoonlijk en niet-professioneel gebruik van een (generiek) AI-systeem.

De AI Act is daarmee niet van toepassing op studenten die voor eigen gebruik met behulp van ChatGPT en vergelijkbare tools bijvoorbeeld teksten genereren voor essays, samenvattingen maken van teksten of als zij informatie en duiding vragen.

De AI Act is ook niet van toepassing op docenten die voor hun eigen ontwikkeling experimenteren met (generatieve) AI. *Maar dat is anders* als een docent (en daarmee zijn/haar instelling) gebruikmaakt van generatieve AI, bijvoorbeeld voor het selecteren van studiematerialen, het formuleren van leerdoelen, het maken van opdrachten of het maken van een lesopzet. Dan is het belangrijk te kijken hoe die specifieke toepassing kwalificeert onder de AI Act.

De AI Act kijkt daarbij naar de *toepassing van een AI-systeem*; waarvoor wordt het AI-systeem gebruikt? De AI Act gaat daarbij uit van een risicogebaseerde aanpak; wat zijn bij de toepassing van een AI-systeem de risico's voor betrokkenen wat betreft gezondheid, veiligheid en grondrechten (zoals het recht op privacy en om niet gediscrimineerd te worden)? Op basis van die risico's verbiedt de AI Act bepaalde toepassingen en geldt voor andere toepassingen dat deze een 'hoog risico' inhouden. Daarnaast kent de AI Act AI-systemen met zogenoemde 'transparantierisico's'.

Let wel. Ook AI-systemen die volgens de AI Act geen hoog risico zijn en ook anderszins niet onder de AI Act vallen, kunnen nog steeds risico's met zich meebrengen. Denk aan privacyschendingen, ontoereikende informatiebeveiliging of onterechte bevoordeling. Het is belangrijk ook in deze gevallen de risico's goed in kaart te brengen en eventueel maatregelen ter beperking van deze risico's te nemen.

De AI Act geeft regels en verplichtingen voor AI-systemen. Wat deze zijn, hangt af van de risicoclassificatie van het AI-systeem én de rol die een instelling vervult met betrekking tot die AI-systemen. Een instelling kan zijn een 'aanbieder' of een 'gebruiksverantwoordelijke'⁷. Uitgangspunt is dat de meeste verplichtingen gelden voor aanbieders van hoog risico AI-systemen.

Een 'aanbieder' van een AI-systeem is een natuurlijke of rechtspersoon die het systeem ontwikkelt of laat ontwikkelen, op de markt plaatst of in gebruik stelt en dat doet onder eigen naam of handelsmerk.

Een 'gebruiksverantwoordelijke' van een AI-systeem is een natuurlijke of rechtspersoon die het systeem onder eigen verantwoordelijkheid gebruikt. Let wel: een gebruiksverantwoordelijke staat dus niet gelijk aan de degene die wordt geraakt door het AI-systeem.

De rol van de instelling onder de AVG en de AI Act

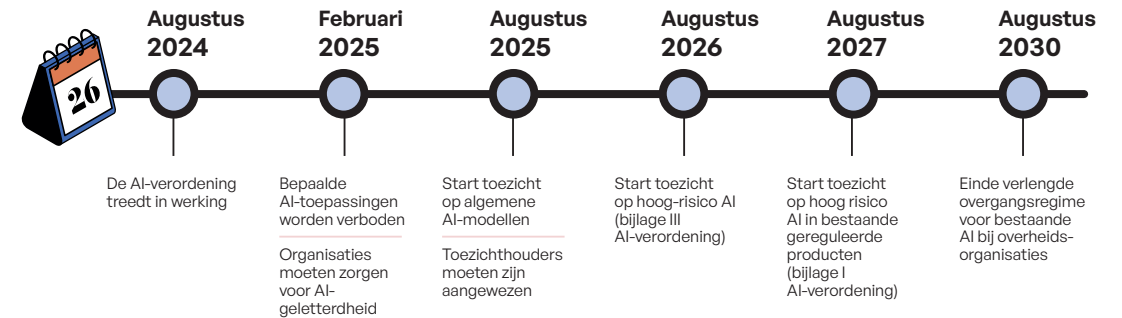
Zowel de AVG als de AI Act kijken naar de rol die een partij, zoals een instelling, vervult voor het bepalen van onder andere de aard en omvang van de verplichtingen van die partij. Die rollen worden zelfstandig bepaald door de AVG en de AI Act.

Een instelling zal meestal kwalificeren als een verwerkingsverantwoordelijke in de zin van de AVG. Welke rol een instelling vervult in de AI Act (aanbieder of gebruiksverantwoordelijke) is minder duidelijk. Het verdient aanbeveling goed na te gaan welke rol de instelling vervult bij een specifiek gebruik van studiedata en AI. De (privacy) jurist, privacy officer, de AI Compliance Officer en/of de FG kunnen hierbij behulpzaam zijn.

Tijdslijnen AI Act

De verplichtingen van de AI Act worden gefaseerd van kracht. De Autoriteit Persoonsgegevens heeft een mooi overzicht gegeven van de relevante tijdslijnen en bijbehorende verplichtingen.

⁷ Daarnaast kent de AI Act ook nog de rollen van 'importeur', 'distributeur' en 'gemachtigde'. Het Referentiekader gaat ervan uit dat instellingen deze rollen niet vervullen. Overigens blijkt uit deze rollen dat de AI Act ook een verordening is die past binnen het bredere wetgevende pallet van productregulering.



AI Act en persoonsgegevens

Voor de toepassing van de AI Act is het *niet* relevant of de studiedata persoonsgegevens bevatten. De AI Act kan van toepassing zijn op het gebruik van studiedata, ook als deze geen persoonsgegevens omvatten.

Verhouding AVG en AI Act

Bij het gebruik van studiedata en AI kunnen de AVG en de AI Act naast elkaar van toepassing zijn. Dat is het geval als studiedata kwalificeren als persoonsgegevens. De ene wet vervangt de andere dus niet.

Dat betekent ook dat het handelen in overeenstemming met de AVG niet automatisch meebrengt dat is voldaan aan de AI Act en vice versa.

5.2 Wat regelt de AI Act voor het onderwijs?

Wat zijn de gevolgen van de AI Act voor het onderwijs en welke bepalingen worden wanneer van kracht? Daarover gaat deze paragraaf.

Vanaf 2 februari 2025: Verboden AI in het onderwijs

De AI Act verbiedt bepaalde toepassingen van AI-systemen omdat de toepassing onaanvaardbare risico's voor betrokkenen met zich meebrengt. Dat zijn bijvoorbeeld systemen die kwetsbaarheden van personen op basis van leeftijd, handicap of sociale omstandigheden exploiteren. AI-systemen die zijn bedoeld voor emotieherkenning op de werkplek en in het onderwijs zijn verboden, tenzij dit wordt gedaan voor medische of veiligheidsredenen.

In artikel 5 van de AI Act staan de verboden AI-toepassingen. De Europese Commissie is gemachtigd de lijst van verboden AI te wijzigen en aan te vullen. Hiervoor is dus geen (uitgebreid) wetgevingstraject nodig.

De verwachting is dat in het onderwijs niet of althans heel weinig gebruik wordt gemaakt van verboden AI-toepassingen. Het is belangrijk dat instellingen goed inventariseren of zij verboden AI gebruiken en als dat het geval is dit gebruik stopzetten. Deze inventarisatie is ongeacht of de instelling aanbieder of gebruiksverantwoordelijke is.

Vanaf 2 februari 2025: AI Geletterdheid

De AI Act vereist dat aanbieders én gebruiksverantwoordelijken maatregelen nemen voor het borgen van een voldoende niveau van AI-geletterdheid van hun medewerkers die zijn betrokken bij de werking en het gebruik van AI-systemen. Op zich geldt de verplichting tot AI-geletterdheid dus niet automatisch voor *alle* medewerkers, maar het verdient aanbeveling alle medewerkers wel enigszins op de hoogte te brengen en te houden van de voor- en nadelen van het gebruik van AI.

Het gaat hier om kennis, begrip en vaardigheden voor een verantwoorde inzet van AI-systemen en bewustwording rond de mogelijkheden, risico's en mogelijke schade die een AI-systeem kan veroorzaken. Hoe uitgebreid die AI-geletterdheid moet zijn, hangt onder meer af van de context waarin het AI-systeem wordt gebruikt. De risicoclassificatie van een AI-systeem zal bepalend zijn voor de mate van AI-geletterdheid.

Hoe AI-geletterdheid vorm te geven?

- Ga na welke medewerkers betrokken zijn of worden bij het gebruik van AI.
- Maak AI- (maar ook data-) geletterdheid onderdeel van bestaande trainings- en onboardingprogramma's.
- Organiseer AI trainingen (e-learning) voor CvB, hoger management en medezeggenschapsraden (van studenten en van medewerkers).
- Organiseer periodieke workshops.

Vanaf 2 augustus 2025: AI-modellen

De gedachte van de Europese wetgever was dat een AI-systeem voor een bepaalde toepassing wordt ontwikkeld. De lancering van ChatGPT in november 2022 liet echter zien dat AI voor vele verschillende doelen kan worden ingezet. Dat paste niet goed bij het idee van een AI-systeem voor een bepaalde toepassing. De Europese wetgever heeft hierin willen voorzien door het geven van specifieke regels voor aanbieders van AI-modellen voor algemene doelen. De aard en omvang van die regels hangen af van de vraag of een AI-model 'systeemrisico's' kent of niet.

Volgens de AI Act zijn "AI-modellen voor algemene doeleinden" - kort gezegd - modellen die geautomatiseerd content (tekst, audio, video of een combinatie daarvan) kunnen maken op basis van verzoeken van gebruikers (*prompts*). Voorbeelden zijn GPT-4 van OpenAI, Google

Gemini, Meta LLaMA of Claude Sonnet. Deze modellen zijn getraind met grote hoeveelheden data op basis van machine learning (zoals *deep neural networks*). Vooral de BigTech bedrijven zijn zeer actief op het gebied van de ontwikkeling van deze modellen en zij integreren deze ook steeds meer in hun eigen producten en diensten (zoals Microsoft Copilot).

Voor een goed begrip is het belangrijk te beseffen dat deze AI-modellen op zichzelf géén AI-toepassingen zijn; een model is 'slechts' een onderdeel van een systeem. De AI-modellen kennen in de AI Act een eigen risicosystematiek naargelang het model wel of geen 'systeemrisico's' kent.

Aanbieders van AI-modellen voor algemene doelen moeten aan de volgende eisen voldoen:

- Technische documentatie leveren
- Gebruiksaanwijzingen leveren
- Voldoen aan de auteursrechtlijn
- Samenvatting publiceren over de content die voor training is gebruikt

Aanbieders die hun AI-model onder een gratis en open licentie publiekelijk beschikbaar stellen, hoeven alleen te voldoen aan de auteursrechtlijn en de samenvatting over de content die voor training is gebruikt te publiceren, tenzij het een AI-model met systeemrisico's is.

Van een AI-model met systeemrisico's is sprake als het model aan de volgende criteria voldoet:

- Het heeft high impact mogelijkheden, geëvalueerd op basis van passende technische instrumenten en methodes, inclusief indicatoren en benchmarks.
- Op basis van een besluit van de Europese commissie ambtshalve of na een gekwalificeerde waarschuwing door het 'wetenschappelijk panel', dat een GPAI-model over mogelijkheden of effecten beschikt die gelijkwaardig zijn aan die van het vorige punt.

Alle aanbieders van AI-modellen met systeemrisico's moeten:

- Modevaluaties uitvoeren, inclusief het uitvoeren en documenteren van contradictietests om systeemrisico's te identificeren en te beperken.
- Beoordelen en beperken van mogelijke systeemrisico's, inclusief de bronnen ervan.
- Ernstige incidenten en mogelijke corrigerende maatregelen traceren, documenteren en zonder onnodige vertraging rapporteren aan de 'AI Office' en relevante nationale bevoegde autoriteiten.
- Zorgen voor een adequaat niveau van cybersecurity.

Vanaf 2 augustus 2026: Hoog risico AI in het onderwijs

De waarschijnlijk meest belangrijke bepalingen van de AI Act voor instellingen hebben betrekking op de AI-systemen die volgens de AI Act kwalificeren als hoog risico.

Onderdeel 3 van Bijlage III van de AI Act somt de hoog risico toepassingen specifiek voor het onderwijs op. Daarnaast zijn er andere hoog risico toepassingen die op het onderwijs van toepassing kunnen zijn. De in onderdeel 1 opgesomde AI-systemen hebben betrekking op:

- biometrische identificatie op afstand, tenzij het systeem alleen voor verificatie wordt gebruikt;
- systemen voor biometrische categorisering op basis van gevoelige eigenschappen of kenmerken;
- systemen voor emotieherkenning.

Aangezien deze toepassingen verder af staan van het gebruik van studiedata blijven deze buiten beschouwing.

Wat zijn die hoog risico toepassingen in het onderwijs? Vooralsnog zijn dat alléén die systemen die het volgende doel beogen:

1. Toegang, toelating en toewijzing tot onderwijs.
2. Evalueren van leerresultaten, ook voor sturen van het leerproces.
3. Beoordelen van het passend onderwijsniveau.
4. Monitoren en detecteren van ongeoorloofd gedrag tijdens toetsen.

De AI Act geeft verder weinig duiding; zo zijn er bijvoorbeeld geen *use cases* opgenomen. De verwachting is wel dat die duiding op termijn zal worden gegeven door de Europese Commissie en/of nationale toezichthouders. Overigens kan de Europese Commissie op een later moment deze toepassingen wijzigen of aanvullen. Het is met andere woorden een dynamische lijst.

Gelet op deze 4 categorieën lijken de volgende toepassingen hoog risico te (kunnen) zijn:

- screenen van aanvragen
- rangschikken van kandidaten
- beoordeling (evalueren?) van examens, essays, etc.
- school- en (bindende) studieadviezen
- online proctoring
- fraudedetectie

Opvallend is dat alleen deze AI-toepassingen kwalificeren als ‘hoog risico’. Dat betekent dat andere toepassingen die – om wat voor reden – ook grote risico’s voor betrokkenen mee zouden kunnen brengen géén hoog risico zijn volgens de AI Act.

Toepassing Referentiekader

Instellingen hebben geen wettelijke verplichting om voor niet hoog risico AI-toepassingen een risico-inschatting te maken. Het Referentiekader hanteert als uitgangspunt dat instellingen het Referentiekader toepassen, óók als de AI-toepassing niet kwalificeert als een hoog risico AI in de zin van de AI Act of ook anderszins is uitgezonderd van de AI Act!

Hoewel de AI Act geen nadere duiding geeft over de hoog risico toepassingen, kent de AI Act wel enige uitzonderingen. Van ‘hoog risico’ is namelijk geen sprake als het AI-systeem geen wezenlijke invloed heeft op een besluit, omdat het systeem is bedoeld om:

- Een beperkte procedurele taak uit te voeren.
- Het resultaat te verbeteren van een eerder afgeronde menselijke activiteit.
- Besluitvormingspatronen of afwijkingen daarop op te sporen.
- Een voorbereidende taak uit te voeren voor een beoordeling die relevant is voor een van de hoog-risico toepassingsgebieden.

Echter, van deze uitzonderingen kan géén gebruik worden gemaakt als het AI-systeem profileert.

Wat is profileren?

De AVG: *‘elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.’*

Vanaf 2 augustus 2026: AI-toepassingen in het onderwijs met transparantierisico’s

Naast verboden en hoog risico kent de AI Act de categorie AI-systemen met transparantierisico’s. Dat zijn bijvoorbeeld AI-systemen die direct contact hebben met betrokkenen, zoals chatbots en virtuele assistenten. Maar ook systemen die audio, video, beeld of tekstinhoud genereren, *deepfakes* én toepassingen die emoties of biometrische kenmerken herkennen.

Wat zijn de verplichtingen voor deze AI-systemen?

Instellingen die gebruikmaken van deze toepassingen hebben informatieverplichtingen die ervoor moeten zorgen dat de betrokkenen bij het eerste gebruik bewust zijn dat ze te maken hebben met een AI-systeem dat de output genereert en dus niet met een natuurlijk persoon. En de instelling moet *deepfakes* altijd als zodanig identificeren.

Tot slot zijn er AI-systemen waarvoor de AI Act geen nadere regels geeft, bijvoorbeeld voor AI-toepassingen zoals spamfilters en spellingscontrole.

5.3 Wat moeten de instellingen regelen bij het gebruik van hoog risico AI?

De meeste en belangrijkste verplichtingen uit de AI Act hebben betrekking op aanbieders en gebruiksverantwoordelijken van hoog risico AI. En dan zijn het vooral de aanbieders van deze AI-systemen die aan veel eisen moeten voldoen.

Aanbieders van hoog risico AI-systemen moeten aan bepaalde eisen voldoen om ervoor te zorgen dat hun AI-systemen betrouwbaar, transparant en controleerbaar zijn:

- Een risicomanagement systeem opzetten tijdens de gehele levenscyclus van het AI-systeem.
- Data governance uitvoeren en ervoor zorgen dat de opleidings-, validerings- en testgegevens-reeksen relevant en voldoende representatief zijn en, voor zo ver mogelijk, geen fouten bevatten en volledig zijn met het beoogde doel.
- Technische documentatie opstellen om naleving aan te tonen en autoriteiten de informatie te geven om die naleving te beoordelen.
- Hun AI-systeem zo ontwerpen dat het automatisch gebeurtenissen registreert die relevant zijn voor het identificeren van risico's op nationaal niveau en ingrijpende wijzigingen tijdens de levenscyclus van het systeem.
- Gebruiksaanwijzingen geven aan gebruiksverantwoordelijken om ervoor te zorgen dat zij aan de eisen voldoen.

Het Knowledge Centre Data&Security (KCDS) ontwikkelde een template voor een gebruiksaanwijzing; T. Gils and W. Ooms (Knowledge Centre Data & Society), "Instructions for use (IFU) for high-risk AI systems under the EU AI Act – working template", October 2024. Zie: [KCDS-Template-instructions-for-use_PDF.pdf](#)

- Hun AI-systeem zo ontwerpen dat gebruiksverantwoordelijken menselijk toezicht kunnen implementeren.
- Hun AI-systeem zo ontwerpen dat de juiste niveaus van nauwkeurigheid, robuustheid en cyberbeveiliging worden bereikt.
- Een kwaliteitsmanagementsysteem opzetten om naleving te garanderen.
- Zorgdragen voor een geldige EU-conformiteitsverklaring.

Voor **gebruiksverantwoordelijken** gelden ook de nodige verplichtingen rond het gebruik van hoog risico AI:

- Nemen van passende technische en organisatorische maatregelen zodat het gebruik van de AI overeenstemt met de gegeven instructies van de aanbieder.
- Monitoren van de werking van het AI-systeem op basis van de gebruiksaanwijzingen, eventueel stopzetten van het systeem en de aanbieders van AI-systemen informeren bij serieuze incidenten. De logfiles van het gebruik moeten ten minste 6 maanden bewaard worden.

- Zorgdragen voor voldoende relevante inputdata (voor zover zij daar controle over hebben).
- Implementeren menselijk toezicht.
- Informeren van betrokkenen dat zij zijn onderworpen aan een AI-systeem met een hoog risico toepassing. Betrokkenen hebben bovendien recht op een duidelijke en betekenisvolle uitleg over de rol van het hoog risico AI-systeem in het besluitvormingsproces als beslissingen met hoog risico zijn genomen.
- Voldoen aan bepaalde meld- en registratieverplichtingen richting toezichthouder(s).
- Beoordelen door overheidsorganisaties – waaronder onderwijsinstellingen – van de mogelijke gevolgen voor de grondrechten bij het gebruik van het hoog risico AI-systeem. Een dergelijke beoordeling heet een *Fundamental Rights Impact Assessment* (FRIA), in het Nederlands ook wel bekend onder een Impact Assessment Mensenrechten en Algoritmes.

De FRIA

- Het gaat bij deze impact assessments om het identificeren van specifieke risico's op het gebied van mensenrechten en mogelijke beheersmaatregelen.
- Een FRIA, uitgevoerd door een aanbieder, mag worden gebruikt. Een aanbieder is echter niet verplicht dit te doen. De gebruiker blijft sowieso eindverantwoordelijk.
- Een FRIA kan onderdeel zijn van een DPIA en kan gelijktijdig met het uitvoeren daarvan worden uitgevoerd.
- De bevindingen van de FRIA moeten aan de toezichthoudende autoriteit (AP) worden gemeld.
- Voor het uitvoeren van een FRIA heeft de overheid een template ontwikkeld. Zie: [Impact Assessment Mensenrechten en Algoritmes | Rapport | Rijksoverheid.nl](#). Het AI Office binnen de Europese Commissie gaat een speciale template/tool ontwikkelen.

5.4 Rolverschuiving van gebruiksverantwoordelijke naar aanbieder

De AI Act maakt een scherp onderscheid tussen de rollen van aanbieder en gebruiksverantwoordelijke. De AI Act kent ook een bepaling die in de praktijk van groot belang kan zijn, namelijk dat onder bepaalde omstandigheden een instelling die 'slechts' gebruiksverantwoordelijke is, transformeert naar de rol van aanbieder. Deze transformatie heeft grote gevolgen voor de instelling, vandaar dat het Referentiekader hier aandacht aan besteedt.

Rolverandering

Wanneer is sprake van een dergelijke transformatie (rolverandering)? Dat is het geval als de instelling als gebruiksverantwoordelijke op enig moment:

1. De eigen naam of handelsmerk op een ‘bestaand’ hoog risico AI-systeem zet.
2. Een substantiële wijziging doorvoert op een ‘bestaand’ hoog risico AI-systeem en het daardoor een hoog risico AI-systeem blijft.
3. Het beoogde doeleinde (zoals voorzien door de aanbieder) van een niet hoog risico AI-systeem aanpast zodat het een hoog risico AI-systeem wordt.

Een aantal aspecten vraagt verduidelijking:

1. Zo is niet helder wanneer sprake is van een ‘substantiële wijziging’?
2. Wat is het ‘beoogde doeleinde’? Dat hangt sterk af van hoe de aanbieder van het AI-systeem dit heeft omschreven, bijvoorbeeld in de handleiding.
3. Kan het aanpassen van het ‘beoogde doeleinde’ door slechts 1 medewerker al leiden tot een rolverandering?

Gevolgen van rolverschuiving

Wat zijn de gevolgen van een rolverschuiving? Het belangrijkste gevolg is dat de instelling dan wordt gezien als aanbieder die moet voldoen aan alle verplichtingen die op een aanbieder van een hoog risico AI-systeem rusten. Dat is een flinke verzwarende voor de instelling (zie hiervoor). Bovendien rijst de vraag of de instelling wel kan voldoen aan al deze verplichtingen. Zo beschikt de instelling bijvoorbeeld niet over de technische documentatie over dat nieuwe beoogde doeleinde. Weliswaar heeft de oorspronkelijke aanbieder de plicht informatie beschikbaar te maken en de instelling te voorzien van technische toegang en informatie, maar hij heeft die informatie waarschijnlijk niet voor dat nieuwe beoogde doel. Dat heeft de instelling immers zelf bewust of onbewust bepaald.

Belangrijk!

Een rolverschuiving heeft voor een instelling grote gevolgen en het Referentiekader geeft het volgende mee aan instellingen:

1. Stel een duidelijk proces op rond gebruik én wijzigingen van het gebruik van AI-systemen zodat hierover een weloverwogen en geïnformeerd oordeel gegeven kan worden. Op die manier voorkomt een instelling dat het onbedoeld en ongewild van kleur verschiet.
2. Spreek in de overeenkomst met de aanbieder duidelijk af wat het ‘beoogde gebruik’ is van het AI-systeem. Welk gebruik valt er wel onder? En welk gebruik niet?
3. Spreek in de overeenkomst met de aanbieder ook af welke steun en bijstand hij moet verlenen als de gebruiksverantwoordelijke van rol verandert.

5.5 Inkoop en AI

Instellingen kunnen gebruikmaken van AI-systemen die zijn ontwikkeld door externe partijen. Dat kunnen *stand alone* AI-systemen zijn maar ook systemen die onderdeel zijn van al bestaande diensten die instellingen afnemen. Vóór de start van een inkooptraject dient de instelling af te wegen of de inzet van AI bij het gebruik van studiedata in een concreet geval in lijn is met de waarden van de instelling, ongeacht de keuze voor een leverancier.

Als deze afweging resulteert in de wens AI in te kopen, is het verstandig (gelet op de eisen van AVG en AI Act) dat instellingen bij de inkoop van AI-systemen (ongeacht of dit hoog risico is of niet) de eisen en wensen van de instelling rond verantwoord gebruik van studiedata en AI vroegtijdig meenemen in de inkoop-/aanbestedingsprocedures.

Voor hoog risico AI-systemen kan een instelling op zich volstaan door in de overeenkomst te bepalen dat het hoog risico AI-systeem (van de leverancier) voldoet aan de eisen van de AI Act (en de AVG) en dat het zodanig is ingericht dat de instelling het AI-systeem kan gebruiken voor de beoogde doeleinden. Bovendien is de aanbieder van een hoog risico AI-systeem al gehouden technische documentatie en gebruikershandleidingen op te leveren.

Het Referentiekader acht het toch wenselijk met leveranciers in gesprek te gaan om zo een verantwoord product of dienst te verwerven, ongeacht of sprake is van een hoog risico AI-toepassing volgens de AI Act. Dat heeft gevolgen voor de contracten die instellingen sluiten met leveranciers.

Check-/vragenlijst voor leveranciers

De UvA heeft voor de inkoop van AI een handige check-/vragenlijst opgesteld. De vragenlijst bestaat uit een ‘pre-flight check’ (vragen die vooral door de instelling zelf moeten worden beantwoord), ‘required checks’ en ‘optional checks’. Zie: [ai-checklist-vu-uva-taskforce.pdf](#)

Contractuele bepalingen

De Europese Commissie heeft *standard contractual clauses* opgesteld voor contracten tussen gebruiksverantwoordelijken (zoals instellingen) en aanbieders van AI-systemen. Die standaard clausules zijn er voor hoog risico AI-systemen en voor niet-hoog risico AI-systemen.

Zie: [public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/eu-model-contractual-ai-clauses-pilot-procurements-ai](#)

5.6 Voorbereiding op de AI Act

Hoewel veel bepalingen gefaseerd van kracht worden, is het belangrijk dat instellingen zich nu al voorbereiden. Dat is niet bepaald eenvoudig, ook omdat veel verplichtingen uit de AI Act de komende tijd nog nader worden uitgewerkt door onder meer allerlei standaarden en nadere duiding van de Europese Commissie en/of het AI Office.

Het Referentiekader gaat ervan uit dat de voorbereiding op de AI Act bestaat uit de volgende drie stappen:

1. **Inventariseer** binnen de instelling welke AI-systemen worden gebruikt en leg dit goed vast, bijvoorbeeld in een AI- of algoritmeregister. Dat kunnen zelfstandige AI-systemen zijn, maar ook AI-systemen die onderdeel zijn van al bestaande diensten. Kijk ook of deze AI-systemen gebruikmaken van persoonsgegevens.
2. **Classificeer** vervolgens deze AI-systemen. Zijn het hoog risico AI-systemen volgens de AI Act? Wat zijn de mogelijke risico's voor betrokkenen die zijn verbonden aan het gebruik van deze AI-systemen? Is hier een risicoanalyse of een DPIA op uitgevoerd?
3. **Implementeer** de relevante bepalingen van de AI Act door:
 - Het opzetten van een proces/procedure om de risico's van AI-systemen blijvend te monitoren en te beheersen. De instelling kan hierbij aansluiten bij al bestaande risico-processen zoals de DPIA-procedure en deze aanvullen.
 - Het opzetten van een AI- en datageletterdheidsprogramma.
 - Het inrichten van menselijke tussenkomst bij het gebruik van AI-systemen.
 - Het aanpassen van de informatievoorziening aan betrokkenen.
 - Het aanvullen van inkoop-/aanbestedingsprocedures met eisen/wensen rond AI.
 - Het aanpassen van modelcontracten, SLA's en algemene voorwaarden.
 - Het aanvullen van de procedure voor vragen/klachten van betrokkenen.

5.7 Andere juridische leerstukken bij het gebruik van studiedata en AI

Naast de AVG en de AI Act kunnen bij het gebruik van AI andere juridische leerstukken relevant zijn, zoals bepalingen rond cybersecurity, aansprakelijkheden, het auteursrecht (vooral bij generatieve AI) en de bescherming van consumenten. Het Referentiekader 2.0 gaat hier niet uitvoerig op in.

6. Duidelijkheid over verantwoordelijkheden

De basis voor een (blijvend) verantwoord gebruik van studiedata en AI vergt duidelijkheid over verantwoordelijkheden bij alle aspecten rond het wel of niet gebruik van studiedata en AI (inclusief over het wijzigen of stopzetten daarvan).

Zo moet binnen de instelling helder zijn 'wie wat doet en wanneer'. Onderwerpen in dat kader zijn: het afleggen van rekenschap, het betrekken van stakeholders, het monitoren en bewaken van uitkomsten, AI-geletterdheid, uitvoeren van FRIA, bewaken van de juiste rolverdeling bij het gebruik van AI, uitlegbare AI, verzoeken van betrokkenen, etc.

Mogelijk is het nodig om bestaande rollen en functies uit te breiden of aan te passen, of nieuwe rollen en functies te scheppen.

Het bundelen van kennis en expertise over meerdere instellingen

Veel instellingen kennen een beperkte bemensing en kunnen de noodzakelijke expertise niet binnen de eigen instelling organiseren. Het staat instellingen vrij gezamenlijk bepaalde expertise te delen. Organisaties zoals de MBO Raad zouden dat kunnen faciliteren.

Overigens is er vanuit de AI Act geen verplichting om AI-functies te benoemen (zoals de AVG wél voorschrijft om in bepaalde omstandigheden een functionaris gegevensbescherming aan te stellen).

AI Governance Officer

De Universiteit Utrecht en de Universiteit Tilburg hebben samen een AI Governance Officer aangesteld. Dit is een nieuwe functie. De AI Governance Officer ondersteunt onder meer bij het ontwikkelen van een holistische aanpak van AI.

AI Compliance Officer

Mede naar aanleiding van de AI Act is de functie van AI Compliance Officer in opkomst. Gespecialiseerde adviesbureaus organiseren cursussen/leergangen voor deze functie.

Tijdens de hele levenscyclus van het gebruik van studiedata en AI is een multidisciplinaire aanpak cruciaal. In deze aanpak zijn verschillende belanghebbenden en deskundigen betrokken,

zoals docenten, onderwijsondersteuners, (business) informatiemanagers, IT'er, data stewards/engineers, architecten, informatiebeveiligings-, privacy- en/of juridisch deskundigen, inkopers, contractmanagers en de functionaris gegevensbescherming. Betrek in deze multidisciplinaire aanpak ook (vertegenwoordigers van) medewerkers en studenten.

RACI-model

Een instelling kan de taken en verantwoordelijkheden vastleggen in een zogenoemd RACI-model. Hierin staan de betrokken functionarissen en hun rol:

R – responsible: verantwoordelijke voor het daadwerkelijk uitvoeren van de taak, legt daarover verantwoording af aan de persoon die accountable is.

A – accountable: (eind)verantwoordelijke voor het resultaat, geeft daar goedkeuring aan.

C – consulted: de rollen/functionies die vooraf betrokken moeten worden bij het uitvoeren van een bepaalde taak en zo het resultaat mede richting geven.

I – informed: de rollen/functionies die achteraf informatie krijgen over de beslissingen, de voortgang en het resultaat.

Via deze aanpak is het mogelijk om de waarden en wettelijke kaders in samenhang te bespreken. De instelling kan dan weloverwogen een keuze maken over het gebruik van studiedata en AI. Organiseer in deze aanpak actief het tegengeluid. Het betrekken van sceptici en critici zorgt namelijk voor een nieuw perspectief en andere inzichten. Dat is bevorderlijk voor de besluitvorming rond het verantwoord gebruik van studiedata en AI.

Ethische commissies

Beschikt een instelling over een ethische commissie voor de beoordeling van onderzoeksvoorstellen? Zet kan de instelling deze commissie inzetten voor het organiseren van de hiervoor genoemde multidisciplinaire aanpak en het tegengeluid.

Instellingen zonder ethische commissie, kunnen een bredere commissie instellen, desnoods ad hoc.

7. Waar en hoe te beginnen?

Na het lezen van de waarden, de wettelijke kaders en de verantwoordelijkheden blijft de vraag: waar en hoe te beginnen? Het Referentiekader stelt de volgende stappen voor.

1. Stel een 'businesscase' op

Via een 'businesscase' krijgt de instelling inzicht in het doel, de voor- en nadelen van het gebruik van studiedata en AI en de waarden die in het geding zijn. Het maakt inzichtelijk welke maatregelen de instelling moet nemen voor een verantwoord gebruik van studiedata en AI. Een voorbeeld van een businesscase zit als bijlage bij het Referentiekader.

2. Doe een check op AVG en AI Act

Een check op AVG en AI Act maakt duidelijk wat de instelling *moet* regelen.

3. Betrek belanghebbenden in een multidisciplinaire aanpak

Cruciaal is om belanghebbenden vroegtijdig te betrekken in het gesprek over het gebruik van studiedata en AI. Zo krijgt de instelling nieuwe inzichten over het concretiseren van de waarden, de kansen en risico's van het gebruik van studiedata en AI. Om de betrokkenheid te ondersteunen en de dialoog te voeren over vooral de waarden, zijn er diverse instrumenten, namelijk:

1. Het Dilemmaspel. Dit spel is ontwikkeld in het kader van het Referentiekader 1.0 en recent geüpdatet. Het spel schetst de verschillende dilemma's rondom het gebruik van studiedata en AI. De spelers worden uitgedaagd om hier, in een gezamenlijke dialoog, oplossingen voor te bedenken.
2. SURF heeft een overzicht met hulpmiddelen en tools die instellingen kunnen gebruiken bij deze dialoog, zie: [Aan de slag met Publieke Waarden: een overzicht van praktische hulpmiddelen | SURF Communities](#)

4. Stel beleid, richtlijnen en procedures op (of vul deze aan)

Stel beleid, richtlijnen en procedures op (of vul deze aan) voor verschillende aspecten rond het verantwoord gebruik van studiedata en AI, bijvoorbeeld over transparantie, betrokkenheid van stakeholders, risicobeoordelingen, datakwaliteit en data governance, logging en monitoring van het gebruik en aanpassingen van het gebruik (op basis van monitoring en opgedane ervaringen, incidentmanagement, menselijke tussenkomst, toezicht, afwikkeling van vragen,

zorgen en klachten, etc.). Gebruik de PDCA-cyclus om periodiek het beleid, de richtlijnen en procedures aan te passen.

5. Zorg voor data- en AI-geletterdheid

Zorg dat onderwijsprofessionals begrijpen waarom studiedata en AI worden gebruikt, wat de beoogde doelen zijn, hoe de gebruikte algoritmes en AI werken, wat de beperkingen zijn, wat de mogelijke risico's zijn bij gebruik van studiedata en AI als het gaat om fundamentele mensenrechten en wat de mogelijkheden zijn om deze risico's te beperken of weg te nemen.

Een handig hulpmiddel is [The AI Maturity in Education Scan \(AIMES\) - Vrije Universiteit Amsterdam](#). Hiermee kunnen docenten zelf bepalen waar zij staan wat betreft AI-geletterdheid en op basis daarvan hun geletterdheid vergroten.

ANNEX – businesscase

Voor het maken van deze businesscase is onderstaande vragenlijst opgesteld. Deze lijst is niet uitputtend.

Algemeen: doel en gebruik van studiedata en AI

- Wat wil je gaan doen met de studiedata? Wat wil je bereiken? Voor wie wil je dit bereiken? Zijn deze doelen duidelijk en meetbaar?
- Hoe kan AI helpen bij het realiseren van het (doel(en))? Zijn andere alternatieve mogelijkheden aanwezig en meegenomen in de beoordeling?
- Wat zijn de verwachtingen qua prestaties en nauwkeurigheid van de AI?
- Is de AI al beschikbaar of moet de instelling deze zelf ontwikkelen of inkopen bij een derde partij?
- Welke studiedata heb nodig voor het bereiken van het doel? Wat is de bron van deze studiedata?
- Is sprake van een rechtsgeldige grondslag voor het gebruik van deze studiedata? Zijn de betrokkenen daarover geïnformeerd?
- Heb je voldoende representatieve studiedata voor het bereiken van het doel(en)?
- Hoe is de studiedata voor het specifieke gebruik beveiligd?
- Hoe is de menselijke tussenkomst geregeld?
- Welke andere waarden zijn in het geding? En hoe geef ik hier invulling aan?

Risico's van het gebruik van studiedata en AI

- Welke voorziene en onvoorziene nadelen zijn er verbonden aan het gebruik van studiedata en AI? Zijn er mogelijke specifieke risico's voor bepaalde groepen van betrokkenen? Zo ja, specificeer deze risico's.
- Hoe wordt voorkomen dat het gebruik van studiedata en AI leidt tot (onbedoelde) discriminatie of uitsluiting?
- Hoe wordt voorkomen dat het gebruik van studiedata en AI leidt tot kansenongelijkheid?
- Wat zijn de mogelijke oorzaken van discriminatie, uitsluiting en/of kansenongelijkheid?
- Wat zijn de eventuele gevolgen als de risico's zich voordoen? Kunnen de eventuele nadelen snel en makkelijk worden verholpen?
- Hoe blijven de studiedata en de werking van de AI veilig en betrouwbaar? Hoe wordt het gebruik van studiedata en AI bijgehouden en de werking gemonitord? Waar wordt dan precies naar gekeken? En hoe vaak en door wie wordt gemonitord?
- Hoe worden de belanghebbenden betrokken bij de evaluatie van het gebruik van studiedata en AI?

- Waar kunnen betrokkenen terecht met hun vragen, opmerkingen en klachten? Hoe worden deze afgewikkeld?
- Zijn de betrokkenen, (aankomend) studenten, alumni, (oud)medewerkers of anderen geïnformeerd over het gebruik van hun studiedata met AI? Hoe zijn zij geïnformeerd?
- Krijgen de betrokkenen betekenisvolle uitleg als er belangrijke beslissingen op basis van de inzet van AI worden genomen? Hoe is dat geborgd?

Colofon

Projectteam

- Bram Enning (Npuls)
- Dominique Campman (Npuls)
- Menno Jehee (Npuls)
- George Wurpel (MSG Strategies)
- Mariken Betsema (MSG Strategies)
- Niek Reijmers (MSG Strategies)

Begeleidingsgroep

- Irene Eegdeman (Hogeschool Windesheim)
- Duuk Baten (SURF)
- Marlon Domingus (Erasmus Universiteit Rotterdam)
- Nigel Steenis (ROC Mondriaan)
- Frank van Tatenhove (Universiteit van Amsterdam)
- Floortje Jorna (SURF)

Klankbordgroep

- Frank van Tatenhove (Universiteit van Amsterdam)
- Annemiek Mandemaker (Aeres)
- Theo Nelissen (Avans Hogeschool)
- Jan van den Berg (Hogeschool van Amsterdam)
- Pascal Tielkens (ROC Nijmegen)
- Annie Slotboom-Memelink (Graafschap College)
- Abdullah Yerebakan (Universiteit Utrecht)
- Lex Freund (Hogeschool Rotterdam)
- Marlon Domingus (Erasmus Universiteit Rotterdam)
- Duuk Baten (SURF)
- Marlies van Hal (Koning Willem 1 College)
- Tri Hartanto (ROC Mondriaan)
- Claartje Uitterhoeve (Graafschap College)
- Shane Bozelie (Deltion College)
- Iglia Vassileva-van der Heiden (Radboud Universiteit)
- Quinta Dijk (SURF)
- Ineke Stoop (Tilburg University)
- Rowin Smits (ROC Mondriaan)
- Tom van Munster (Interstedelijk Studenten Overleg)

- Harry van de Vis (Albeda College)
- Yorick van der Heijden (Interstedelijk Studenten Overleg)
- Barbara Gerretsen (Universiteit van Amsterdam)
- Daphne Peters (JobMBO)
- Charlotte Vonk Noordegraaf (Deltion College)
- Jan Tjeerd Groenewoud (Rijksuniversiteit Groningen)
- Irene Eegdeman (Hogeschool Windesheim)
- Nigel Steenis (ROC Mondriaan)
- Mark Trimpe (VISTA College)
- Dominique Campman (Npuls)
- JaapJan Vroom (SURF)
- Simon Jong (Deltion College)
- Wladimir Mufty (SURF)

Review FG

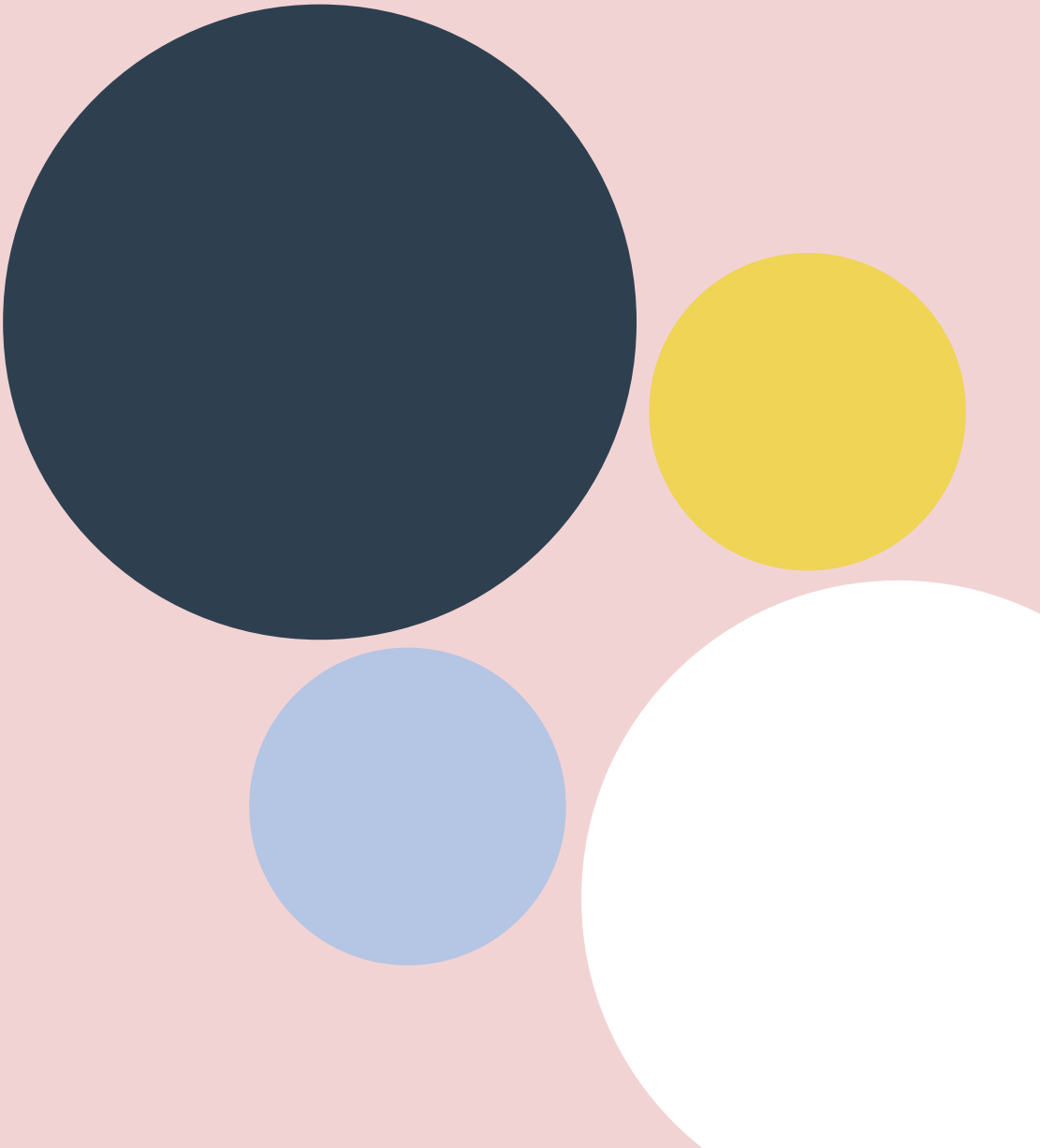
- Peter Vermeijs (MBO Raad)
- Moswa Herregodts (Tilburg University)
- Raoul Winkens (Universiteit Maastricht)
- Esther van der Ent (HAN Hogeschool)
- Ingeborg ten Oever (BUas)
- R. Kronieger (Iselinge Hogeschool)
- Silvia van Dijk (Haagse Hogeschool)
- Kees-Jan van Klaveren (Hogeschool Rotterdam)
- Machiel van Velzen (ROC Midden)

Geïnterviewden

- Andres Steijaert (SURF)
- Annie Slotboom (Graafschap College)
- Duuk Baten (SURF)
- Frank Benneker (Universiteit van Amsterdam)
- Frank van Tatenhove (Universiteit van Amsterdam)
- Han Werts (Radboud Universiteit)
- Irene Eegdeman (Hogeschool Windesheim)
- Jaap Jan Vroom (SURF)
- Justian Knobhout (Hogeschool Utrecht)
- Karianne Vermaas (SURF)
- Mark Trimpe (VISTA College)
- Marlon Domingus (Erasmus Universiteit Rotterdam)
- Niek Kersten (Graafschap College)
- Yvette Roman (Universiteit Utrecht)

Enquête

- Annie Slotboom (Graafschap College)
- Barbara Gerretsen (Universiteit van Amsterdam)
- Elisa Jochims (Graafschap College)
- Frank Benneker (Universiteit van Amsterdam)
- Ineke Stoop (Tilburg University)
- Irene Eegdeman (Hogeschool Windesheim)
- Jan Tjeerd Groenewoud (Rijksuniversiteit Groningen)
- Jan van den Berg (Hogeschool van Amsterdam)
- Jorrit Arntzen (Deltion College)
- Kim Schildkamp (Universiteit Twente)
- Lex Freund (Hogeschool Rotterdam)
- Marco van Leeuwen (BUas)
- Marlon Domingus (Erasmus Universiteit Rotterdam)
- Memon Boukiour (Haagse Hogeschool)
- Raoul Winkens (Universiteit Maastricht)
- Ronald Sarelse (Radboud Universiteit)
- Theo Bakker (Haagse Hogeschool)
- Wim Siemann (Albeda College)
- Alan Berg (Universiteit van Amsterdam)





**Onderwijs
bewegen.**