Referentiekader privacy en ethiek voor studiedata

Versie 1.0

Versnellingsplan
Onderwijsinnovatie met ICT

veilig en betrouwbaar benutten van studiedata

Referentiekader privacy en ethiek voor studiedata

Versie 1.0

Versnellingsplan Onderwijsinnovatie met ICT – Zone Studiedata

Versnellingsplan Onderwijsinnovatie met ICT

November 2021

Inhoudsopgave

Samenvatting

Verantwoord gebruik van studiedata vanuit het oogpunt van privacy en ethiek

Hoger onderwijsinstellingen zetten steeds vaker studiedata in ten gunste van de kwaliteit, effectiviteit en efficiëntie van het hoger onderwijs. Om de voordelen van studiedata te kunnen benutten, is het belangrijk dat er bij alle belanghebbenden vertrouwen is dat hoger onderwijsinstellingen op een verantwoorde wijze met de data omgaan. Instellingen houden zich aan de geldende wet- en regelgeving, maar hebben behoefte aan nadere duiding van deze regels voor het gebruik van studiedata.

Onder regie van de Zone Veilig en Betrouwbaar Benutten van Studiedata van het Versnellingsplan Onderwijsinnovatie met ICT is daarom dit landelijk 'Referentiekader privacy en ethiek voor studiedata' opgesteld. Een gezamenlijk kader vormt een instrument om gemeenschappelijke waarden te operationaliseren en kan een belangrijke bijdrage leveren aan het vertrouwen in de instellingen.

Het Referentiekader betreft zowel de ethische uitgangspunten als de juridische (privacy) kaders waar instellingen voldoende aandacht aan moeten besteden bij het verantwoord gebruik van studiedata. Beide aspecten komen uitgebreid aan bod in dit Referentiekader. Samenvattend zullen hoger onderwijsinstellingen de volgende vier ethische uitgangspunten in acht nemen bij het gebruik van studiedata:

1. **Instellingen zijn aanspreekbaar op en transparant over het gebruik van studiedata en leggen daar rekenschap over af.**
   Aanspreekbaarheid betekent verantwoordelijkheid nemen. Instellingen maken inzichtelijk wie verantwoordelijk dan wel aanspreekbaar is als er twijfels zijn over een bepaald gebruik van studiedata. Onder aanspreekbaarheid valt ook de verantwoordelijkheid om rekenschap te geven van het feit dat studiedata altijd in een bepaalde maatschappelijke context worden gebruikt.
   → 2.2.1

2. **Instellingen maken bij het gebruik van studiedata een eerlijke afweging tussen de belangen van alle betrokkenen en belanghebbenden.**
   Instellingen nemen maatregelen om te voorkomen dat heersende opvattingen en labeling het gedrag van docenten en studenten beïnvloedt, om negatieve effecten te voorkomen. Een eerlijke afweging wordt geborgd door zoveel mogelijk de medezeggen-

schap te betrekken bij het ontwikkelen van beleid, een gedragsode of richtsnoeren over het gebruik van studiedata.
→ 2.2.2

3. **Instellingen zorgen ervoor dat de analyses betrouwbaar en valide zijn.**
   Betrouwbare en valide analyses beginnen met een aanpak, waarbij vooral de vraag leidend is. Instellingen zorgen er verder voor dat het gebruik van studiedata van hoge methodologische kwaliteit is. Personen die een rol spelen bij het verwerken van studiedata dienen hiervoor te beschikken over een adequaat niveau van relevante kennis op het gebied van statistiek en onderwijs.
   → 2.2.3

4. **Er is altijd een plek voor de menselijke maat, ook wanneer instellingen gebruik maken van automatische processen.**
   Instellingen zorgen dat altijd een menselijk oordeel is bij geautomatiseerd gebruik van studiedata, de zogeheten '*human in the loop*'.
   → 2.2.4

Daarnaast besteden hoger onderwijsinstellingen bij het gebruik van studiedata aan de volgende vier juridische privacy-onderdelen specifieke aandacht:

1. **De interne verantwoordelijkheidsverdeling is voldoende duidelijk bepaald en vastgelegd.**
   De eindverantwoordelijkheid voor het zorgvuldig gebruik van studiedata ligt bij het College van Bestuur (CvB), als dagelijks bestuur van de instelling. Dit betekent echter niet dat andere functionarissen geen rol hebben in het zorgvuldig gebruik van studiedata. De eindgebruiker, zoals een docent of beleidsmedewerker, is bij uitstek degene die moet borgen dat studiedata op verantwoorde wijze wordt benut. Daarnaast geeft de Functionaris Gegevensbescherming (on)gevraagd advies en kan zij controlerend optreden binnen de instelling. Instellingen brengen zelf in kaart welke functionarissen betrokken (moeten) zijn bij het gebruik van studiedata: zoals een privacy functionaris, (medisch) ethische commissie, studiedata team, *(Chief) Information Security Officer*, etc..
   → Hoofdstuk 5

2. **Er wordt voldoende transparant gecommuniceerd over het gebruik van studiedata.**
   Wanneer studiedata door een instelling gebruikt gaat worden moet de instelling aan betrokkenen alle relevante informatie geven over dit gebruik, zoals het doel waarvoor de studiedata gebruikt gaat worden, of de studiedata wordt gedeeld met een andere organisatie en zo ja, met welke organisatie en hoe iemand contact kan opnemen met de instelling voor vragen. Dit kan het beste worden gedaan op het moment dat de persoonsgegevens daadwerkelijk als studiedata gebruikt gaan worden. Dit kan op een gelaagde manier worden uitgevoerd.
   → Hoofdstuk 6

3. **Betrokkenen worden gefaciliteerd bij het uitoefenen van hun rechten.**
   De instelling moet betrokkenen faciliteren om hun rechten uit te oefenen en man geen onnodige drempels opwerpen. Voor een deel van de betrokkenen kan hierin tot op zekere hoogte worden voorzien door bijvoorbeeld een *self-service* portal voor studenten of docenten.
   → Hoofdstuk 7

4. **Instellingen hanteren bij elk gebruik van studiedata de drieslag: doel-grondslag-zorgvuldigheid. Het doel is duidelijk bepaald; De grondslag is helder; en de zorgvuldigheidsnormen worden goed nageleefd.**
   Bij elk gebruik van studiedata moet het doel duidelijk zijn bepaald, moet een passende grondslag worden gebruikt en moeten alle noodzakelijke organisatorische en technische maatregelen worden getroffen om zorgvuldig gebruik van studiedata te garanderen. Bij het verstrekken of ontvangen van gegevens van andere partijen geldt deze drieslag ook. Als een verwerking waarschijnlijk een hoog risico met zich meebrengt voor de betrokkene(n) moet voorts altijd een DPIA worden uitgevoerd.
   → Hoofdstukken 4 en 8

1 Inleiding

Studiedata benutten vraagt om het vertrouwen van studenten en medewerkers dat het op verantwoorde wijze plaatsvindt. Onder regie van de Zone Veilig en Betrouwbaar Benutten van Studiedata van het Versnellingsplan Onderwijsinnovatie met ICT is daarom dit landelijk 'Referentiekader privacy en ethiek voor studiedata' opgesteld.

Een gezamenlijk kader vormt een instrument om gemeenschappelijke waarden te operationaliseren en kan een belangrijke bijdrage leveren aan het vertrouwen in de instellingen. Het Referentiekader zorgt daarnaast voor een gezamenlijke taal voor het gebruik van studiedata en schept de ruimte voor hoger onderwijsinstellingen om van elkaar te leren hoe verantwoord met studiedata kan worden gewerkt.

Dit Referentiekader betreft de ethische principes en de juridische uitgangspunten die worden gehanteerd voor het verantwoord gebruik van studiedata, evenals een praktische handreiking, waarin de wettelijke kaders die van toepassing zijn op studiedata worden toegelicht. Daarbij is waar mogelijk aangegeven hoe instellingen hier hun eigen afwegingen in kunnen maken.

Toelichting: samenhang tussen een ethische en juridische benadering

Het antwoord op de vraag wat verantwoord gebruik van studiedata is, betreft zowel een juridische als een ethische component. Die twee hangen nauw met elkaar samen en vragen om een voortdurende maatschappelijk dialoog over wat mensen met elkaar wenselijk vinden.

Zo bevat de Algemene Verordening Gegevensbescherming (AVG) in artikel 5 de belangrijkste principiële uitgangspunten, zoals eerlijkheid, rechtmatigheid en transparantie. Dit zijn echter niet puur juridische uitgangspunten, maar raken ook aan de ethische aspecten van verantwoord gebruik van persoonsgegevens.

Daarnaast heeft de AVG veel open normen in zich, zodat organisaties binnen de kaders van de wet eigen afwegingen kunnen maken. Daar waar nieuwe toepassingen ontstaan en daar waar de wet ruimte laat voor een eigen interpretatie kunnen ethische principes richting geven.

Het Referentiekader is in de eerste plaats bedoeld voor de professionals die in de praktijk met studiedata werken. Daarnaast wil het Referentiekader ook studenten en andere geïnteresseerden informeren over hoe met studiedata wordt omgegaan. Het Referentiekader zal in de praktijk gebruikt moeten worden. Een praktijk die sterk in beweging is. Het is daarom de bedoeling om het Referentiekader periodiek te blijven evalueren en waar nodig te verbeteren of uit te breiden.

1.1 Waarom een Referentiekader?

Er is een aantal instrumenten dat grenzen stelt aan, maar ook ruimte biedt voor, het benutten van studiedata. De bekendste is de AVG, waarin regels zijn opgenomen die gaan over het verwerken van persoonsgegevens. Daarnaast zijn er enkele instrumenten gericht op onderzoek, zoals de ISO-norm 20252:2019, de Nederlandse Gedragscode voor Wetenschappelijke Integriteit en de Gedragscode voor Onderzoek en Statistiek.

Ondanks deze kaders leidt het benutten van studiedata in de praktijk tot vragen over de (on)mogelijkheden van het gebruik van studiedata, bijvoorbeeld ten aanzien van de doelmatigheid, wettelijke kaders en de te maken afwegingen. Deze vragen en zorgen kunnen de benutting van studiedata (onnodig) belemmeren.

1.2 Doel van het Referentiekader

Dit Referentiekader is bedoeld om hoger onderwijsinstellingen te helpen bij het verantwoord gebruiken van studiedata. Op landelijk niveau geeft het richting aan verantwoord gebruik van studiedata en draagt het bij aan het vertrouwen in het gebruik van studiedata door hoger onderwijsinstellingen. Wat precies wordt verstaan onder studiedata wordt nader uitgewerkt in hoofdstuk 3.

Daarnaast is het Referentiekader een basis voor instellingen bij het ontwikkelen van instelling-specifieke beleidskaders, werkwijzen en processen voor het gebruik van studiedata. Het geeft ook ondersteuning aan de eindgebruikers van studiedata. Tot slot draagt het eraan bij dat duidelijkheid wordt geboden aan studenten, docenten en andere betrokkenen over de werkwijze die door de instelling wordt gehanteerd bij het gebruiken van studiedata. Een betrokkene in dit kader refereert daarbij steeds specifiek aan de definitie uit de AVG (zie 3.4.4) en is vaak een student. Als we willen spreken over iemand die betrokken is *bij* studiedata gebruiken we de term belanghebbende of geïnteresseerde.

Het Referentiekader is dus bedoeld als een richtinggevend instrument waarmee instellingen een eigen beleid, kader of code kunnen opstellen waarin ze vastleggen hoe ze omgaan met studiedata. Tevens is dit Referentiekader ontwikkelingsgericht en -ondersteunend, zodat het mogelijk blijft voor instellingen om een eigen invulling te geven aan het gebruik van studiedata.

1.3 Inhoud van het Referentiekader

Dit landelijke Referentiekader geeft de kaders weer voor het verantwoord gebruik van studiedata. De focus hierbij is privacy en ethiek, waarbij enerzijds de (ethische) uitgangspunten en principes worden beschreven en anderzijds nader wordt ingegaan op de (wettelijke) kaders waar een instelling aandacht aan moet geven bij het benutten van studiedata. Denk dan bijvoorbeeld aan het beleggen van de verantwoordelijkheden voor het gebruik van studiedata binnen de instelling, het voldoen aan het vereiste van transparantie en het faciliteren van het uitoefenen van de rechten van betrokkenen.

Binnen deze kaders moeten de instellingen zelf nadere invulling geven aan hoe zij op verantwoorde wijze gebruik maken van studiedata. Zij moeten bijvoorbeeld zelf besluiten op welke manier zij de *data governance* regelen, alsook op welke manier studenten inzicht krijgen in de van hen verwerkte persoonsgegevens.

1.4 Leeswijzer

In hoofdstuk 2 wordt allereerst ingegaan op de ethische uitgangspunten die worden gehanteerd bij het verantwoord gebruik van studiedata. De ethische uitgangspunten geven een gezamenlijk vertrekpunt voor alle hoger onderwijsinstellingen en beantwoorden de 'waarom-vraag'. De daaropvolgende hoofdstukken beschrijven vervolgens wat er nodig is om aan die ethische vertrekpunten recht te doen binnen de kaders van de wet. In tekstkaders worden praktijkvoorbeelden besproken die zijn gebaseerd op cases vanuit een gebruikersgroep.

Hoofdstuk 3 geeft de scope en definities voor dit referentiekader. Allereerst ten aanzien van de term studiedata en voor welke toepassingen studiedata door instellingen kan worden gebruikt. Vervolgens wordt verder ingegaan op de voor dit Referentiekader relevante begrippen, zoals privacy, (bijzondere) persoonsgegevens, verwerkingsverantwoordelijke en betrokkene. Hierbij wordt beschreven wat met deze begrippen wordt bedoeld en hoe dit in het kader van het gebruik van studiedata geduid kan worden. In hoofdstuk 4 wordt vervolgens nader ingegaan op de verantwoordelijkheden van de instellingen, zoals het bepalen van een duidelijk doel en zorgen dat er een juridische grondslag bestaat. Hoofdstuk 5 gaat nader in op het beleggen van de verantwoordelijkheden binnen een instelling. Vervolgens gaat hoofdstuk 6 over transparantie en aanspreekbaarheid. Hoofdstuk 7 gaat in op de manier waarop de verschillende rechten van betrokkenen in het kader van studiedata handen en voeten kunnen worden gegeven. In hoofdstuk 8 wordt ingegaan op verschillende aanvullende waarborgen en maatregelen die door de instellingen getroffen kunnen worden. In hoofdstuk 9 zijn enkele afsluitende paragrafen opgenomen met een korte schets van de totstandkoming van dit referentiekader en het vervolgproces.

2 Ethische uitgangspunten

In dit hoofdstuk worden de ethische uitgangspunten uiteengezet die voor de hoger onderwijsinstellingen leidend zijn in het benutten van studiedata. Uiteraard is voldoen aan de geldende wet- en regelgeving, met name op het gebied van privacy en de bescherming van persoonsgegevens, het startpunt voor alle instellingen. Maar niet alles wat wettelijk mag, is ook ethisch verantwoord. Daarnaast geldt dat de wet- en regelgeving ruimte geeft voor een eigen invulling en ook deze invulling moet op een ethische manier worden gedaan.

Praktijkvoorbeeld: welzijnsmonitoring

Bij welzijnsmonitoring worden persoonlijke en sociale factoren van individuele studenten vastgelegd en geanalyseerd. Dit geeft studenten inzicht in, en maatwerkadvies over, mogelijkheden om hun welzijn te verbeteren. Het verzamelen en gebruiken van dit soort studiedata kent zowel juridische als ethische aspecten. De afwegingen moeten expliciet worden gemaakt en transparant zijn voor betrokkenen. Een afweging zou onder andere antwoord moeten geven op de volgende vragen:

1. Welk doel heeft de instelling? Als de monitor uitsluitend bedoeld is om individuele studenten hierdoor zelf inzicht te laten krijgen in de eigen situatie, eventueel met praktische tips, leidt dat zeer waarschijnlijk tot een andere afweging en een andere uitkomst dan wanneer de instelling de gegevens (ook) wil gebruiken voor meta-analyses.
2. Zijn onderwijsorganisaties de aangewezen partij om dergelijke hulp aan te bieden? Bij afstandsonderwijs zullen die vragen wellicht anders beantwoord worden dan bij fysiek onderwijs.
3. Hoe ver gaat de zorgplicht en wat betekent deze tool voor de autonomie van de student?
4. In welke mate blijft menselijk contact mogelijk over welzijnsvragen?
5. Is de methode en onderbouwing van de aanpak voldoende valide?
6. Wat is de grondslag? Hierbij moeten aspecten als de relatie tussen student en onderwijsinstelling en het feit dat hier (zeer waarschijnlijk) bijzondere persoonsgegevens bij worden verwerkt, worden meegenomen.

De (ethische) keuzes die instellingen maken, zijn zichtbaar voor anderen en voeden het maatschappelijk debat over data en privacy. Meer dan ooit verwachten mensen transparantie, controle en keuze over hoe hun gegevens worden gebruikt.[1] Dit vormt een aanvullende motivatie om de feitelijke keuzes die instellingen maken, duidelijk te beschrijven.

2.1 Digitalisering en studiedata

Onderwijsinstellingen zien in het gebruik van studiedata veel potentie om hun werk, namelijk het geven van onderwijs en het doen van onderzoek en valorisatie, beter te doen. Studiedata kan daarbij worden gebruikt om instroom, doorstroom, uitstroom en aansluiting op de arbeidsmarkt van studenten te optimaliseren.

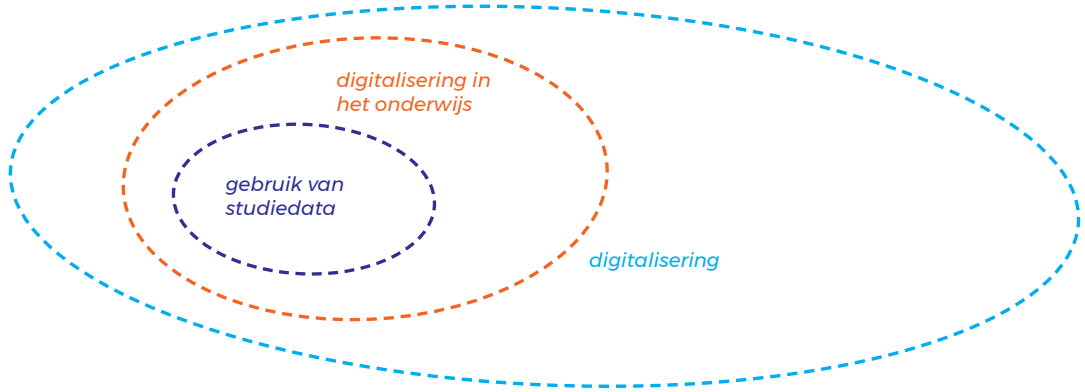
Het gebruik van studiedata past in een bredere trend van toenemende digitalisering, maar is natuurlijk niet nieuw.[2] Instroomcijfers, tentamenresultaten en onderwijsevaluaties vormen al decennialang bruikbare data voor hoger onderwijsinstellingen om hun onderwijsprocessen te begrijpen en te verbeteren en om hun studenten optimaal te ondersteunen. Wat verandert is dat het aantal databronnen toeneemt, net zoals de rekenkracht en de beschikbaarheid van nieuwe technologieën en van gebruiksvriendelijke analysemethoden. Daarmee groeit ook het aantal mogelijke toepassingen van studiedata. Algoritmes en kunstmatige intelligentie (*Artificial Intelligence* of *AI*) worden hierbij steeds vaker toegepast, ook bij het benutten van studiedata. Dit kader sluit daarom nauw aan bij het Toetsingskader algoritmes van de Algemene Rekenkamer www.rekenkamer.nl/onderwerpen/algoritmes-digitaal-toetsingskader en bij de waardenwijzer die is opgesteld door Kennisnet in samenwerking met SURF (www.surf.nl/publieke-waarden).

Deze ontwikkelingen roepen vragen en zorgen op met een ethisch karakter. Er kan steeds meer, maar wat zijn de consequenties van die nieuwe mogelijkheden? Wat vinden hoger onderwijsinstellingen verantwoord? Om die vraag te beantwoorden is het goed om een onderscheid te maken tussen digitalisering in het algemeen, digitalisering in het onderwijs en het gebruik van studiedata. Zodoende kan dit Referentiekader zo specifiek mogelijk ingaan op de vraag: wat is verantwoord gebruik van studiedata?

[1] Dit besef is bijvoorbeeld ook doorgedrongen tot marketingafdelingen van multinationals. Zie: Data Ethics van de World Federation of Advertisers, wfanet.org/leadership/data-ethics

[2] Het gebruik van studiedata kent verschillende activiteiten en omvat de hele keten van verzamelen, verrijken, analyse, toepassen, presenteren, visualiseren, rapporteren, communiceren, opslaan en uiteindelijk ook weer verwijderen.

Digitalisering is een proces dat zich over een groot deel van de maatschappij uitstrekt, bijvoorbeeld ook bij het ontwikkelen van *smart cities* en *connected cars*.[3] Digitalisering in het hoger onderwijs valt binnen de algemene trend van digitalisering die in de maatschappij waarneembaar is en omvat alle toepassingen van en interactie met digitale techniek in het onderwijs. Daar horen bijvoorbeeld ook bij de digitalisering van leermiddelen, de toepassing van cloud-technologie en gebruik van sociale media.[4] Het gebruik van studiedata vormt een deelverzameling van het bredere onderwerp digitalisering in het onderwijs.



Praktijkvoorbeeld: afstandsonderwijs

Bij digitalisering van het onderwijs gaat het niet alleen om wat er kan en mag, maar ook om wat een instelling wil: welke rol krijgt de technologie? Tijdens de Coronacrisis was afstandsonderwijs noodzakelijk, maar de technologie voor afstandsonderwijs kan ook worden ingezet als een bron van studiedata. Met het afstandsonderwijs kan een aantal kernwaarden voor het hoger onderwijs onder druk komen te staan. Het gaat dan bijvoorbeeld om menselijkheid, rechtvaardigheid en autonomie.

Niet iedere student bevindt zich in een situatie om op een adequate wijze deel te nemen aan het afstandsonderwijs, bijvoorbeeld vanwege de thuissituatie. Dit vergroot kansenongelijkheid en heeft daarmee consequenties voor de waarde

[3] Zie bijvoorbeeld de datastrategie van de Gemeente Amsterdam, www.amsterdam.nl/wonen-leefomgeving/innovatie/de-digitale-stad/datastrategie/

[4] De ethische aspecten die met digitalisering van het onderwijs gepaard gaan worden besproken in Waarden Wegen, een publicatie van Kennisnet, www.kennisnet.nl/app/uploads/kennisnet/publicatie/Kennisnet-Ethiekkompas-Waardenwegen.pdf

rechtvaardigheid. En hoewel er vaak meer digitaal contact is tussen de docenten en studenten, missen beide groepen het dagelijkse, menselijke contact. Bij het inzetten van afstandsonderwijs, al dan niet met het doel om studiedata te verzamelen, zullen instellingen aanspreekbaar moeten zijn op de afwegingen die zij maken rond dit type ethische vragen.

2.1.1 Mogelijke negatieve consequenties

Digitalisering kan leiden tot (onbedoelde en ongewenste) negatieve consequenties. Het is daarom belangrijk om deze ontwikkeling vanuit waarden te sturen. De WaardenWijzer van SURF en Kennisnet (www.surf.nl/publieke-waarden) biedt een gemeenschappelijke taal voor het voeren van de dialoog in het onderwijs over digitalisering en het belang van onderwijswaarden. Bij het gebruik van studiedata moet gedacht worden aan mogelijke negatieve effecten, zoals:

- Verlies van de menselijke maat, zoals de autonomie en het recht op zelfbeschikking, 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 mogelijk maken (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 discriminatie van groepen door profilering; en
- Misverstanden door misbruik of misinterpretatie van gegevens.

Praktijkvoorbeeld: Learning Management System

In een Learning Management Systeem (LMS) krijgen docenten een standaardrapportage over studenten die hun prestaties inkleurt op basis van twee variabelen: 1) de mate van activiteit (in het LMS) en 2) de resultaten op tussentoetsen tot nu toe. Dit wordt gevisualiseerd in een activity & grade matrix. Deze weergave kan leiden tot misinterpretaties. Bij het gebruik van deze visualisatie moeten daarom deze vragen worden gesteld:

1. Geven de variabelen het inzicht dat ze lijken te geven?
2. Zijn deze op de juiste wijze geoperationaliseerd? Is de methode valide?
3. Zijn de variabelen voldoende voorspellend? Is de visualisatie eenduidig? Brengt deze de informatie op de juiste wijze over? Hoe wordt gezorgd dat deze visualisatie voldoende in context wordt geplaatst (bijvoorbeeld door een duidelijke toelichting)?

De kans op negatieve effecten neemt toe naarmate er meer data verzameld wordt, zonder gedegen afwegingen over het doel waarvoor studiedata wordt ingezet, bijvoorbeeld:

- Grasduinen in data “omdat het kan”, zonder vooraf na te denken waarom, hoe en welke consequenties dit heeft.
- Technische toepassingen inzetten als doel op zich, in plaats van een middel om een (hoger) doel te bereiken.

Verantwoord gebruik van studiedata is, kortgezegd, positieve interventies in het onderwijs mogelijk maken en tegelijkertijd negatieve consequenties minimaliseren. Welke uitgangspunten hoger onderwijsinstellingen daarbij hanteren, wordt hieronder uitgewerkt.

2.2 Uitgangspunten bij het gebruik van studiedata

Hoger onderwijsinstellingen vormen leergemeenschappen waarin studenten en medewerkers ruimte vinden om te leren, ook door fouten te maken, en te onderzoeken. Dit zijn open gemeenschappen waarin iedereen meetelt en waarbinnen iedereen zich veilig voelt om in vrijheid eigen keuzes te maken. Transparantie, integriteit, diversiteit en inclusiviteit maken deel uit van de publieke waarden die sector-breed door hoger onderwijsinstellingen worden gedeeld en onlosmakelijk verbonden zijn aan de taak van hoger onderwijsinstellingen in onze maatschappij.

Deze kernwaarden, die door alle instellingen worden gedeeld, zijn op verschillende manieren te operationaliseren. Op basis van de gesprekken, antwoorden op de vragenlijst en reviews met een groot aantal partijen uit het hoger onderwijs kwamen de volgende ethische uitgangspunten naar voren als de meest belangrijke voor het gebruik van studiedata:

- Rekenschap afleggen (accountability*): instellingen zijn aanspreekbaar op en transparant over het gebruik van studiedata en leggen daar rekenschap over af.*
- Eerlijke afweging (rechtvaardigheid): *instellingen maken bij het gebruik van studiedata een eerlijke afweging tussen de belangen van alle betrokkenen en belanghebbenden.*
- Valide en betrouwbare analyse: *instellingen zorgen ervoor dat de analyses betrouwbaar en valide zijn.*
- Menselijke maat bij geautomatiseerde processen (menselijkheid en autonomie): *er is altijd een plek voor de menselijke maat, ook wanneer instellingen gebruik maken van automatische processen.*

2.2.1 Rekenschap afleggen (accountability)

Transparantie is een ethisch principe dat binnen dit referentiekader wordt gezien als een van de leidende principes voor de dagelijkse praktijk. Transparantie houdt onder andere in dat het voor anderen helder is op welke data men zich heeft gebaseerd, hoe deze zijn verkregen, welke resultaten men heeft bereikt en langs welke weg. De wettelijke privacy-aspecten t.a.v. transparantie zijn uitgewerkt in de AVG. De AVG bepaalt *welke informatie* moet worden gegeven en *op welk moment*. Instellingen bepalen zelf op welke manier zij de informatie delen (zie verder hoofdstuk 7).

Aanspreekbaarheid betekent verantwoordelijkheid nemen. Daar waar er sprake is van conflicterende belangen of uitgangspunten is het van belang om een zorgvuldige afweging te maken. Instellingen maken inzichtelijk wie verantwoordelijk dan wel aanspreekbaar is als er twijfels zijn over een bepaald gebruik van studiedata. Over de interne verantwoordelijkheidsverdeling is meer te lezen in hoofdstuk 5.

Onder aanspreekbaarheid valt ook de verantwoordelijkheid om rekenschap te geven van het feit dat studiedata altijd in een bepaalde maatschappelijke context worden gebruikt. Instellingen zijn aanspreekbaar op de vraag naar nut en noodzaak van het gebruik van studiedata en hoe zij daarbij rekening hebben gehouden met de legitieme belangen van betrokkenen en eventuele andere belanghebbenden.

In dat kader is de eerste afweging die instellingen moeten maken of een bepaald doel past bij de kernwaarden en maatschappelijke rol van de instelling. Daarnaast documenteren instellingen voor alle betrokkenen wat er met welke studiedata om welke reden wordt gedaan. Deze informatie is uitlegbaar en op een laagdrempelige manier toegankelijk voor de betrokkenen. Tot slot moeten instellingen, in het kader van het afleggen van rekenschap, toetsen of het nagestreefde doel bereikt is.[5]

De verantwoording over wat kan en mag met studiedata is geen eenrichtingsverkeer. Studenten en andere betrokkenen mogen verwachten dat de instelling hen actief betrekt bij de keuzes bij het gebruik van studiedata en hen – waar relevant – actief informeert over de resultaten. Zo blijven instellingen in een voortdurende dialoog met alle betrokkenen en dragen ze daarmee bij aan het uitdragen van een cultuur van verantwoord datagebruik.

[5] Hiervoor kan Plan Do Check Act (PDCA) cyclus worden aangehouden

2.2.2 Eerlijke afweging (rechtvaardigheid)

Elk gebruik van studiedata vereist een eerlijke afweging tussen de belangen die de instelling heeft bij het gebruik van studiedata en de mogelijke gevolgen hiervan voor de betrokkenen, vaak de studenten. Het gebruik van studiedata dient alleen te gebeuren ter ondersteuning van de maatschappelijke rol van hoger onderwijsinstellingen. Het gebruik van studiedata dient positief gericht te zijn, dus ten bate van de kwaliteit, effectiviteit en efficiëntie van het onderwijs en onderwijsbeleid, het geven van onderwijs, met een daarbij passende begeleiding van (individuele) studenten en het doen van onderzoek en valorisatie.

Daarbij maakt de instelling een zorgvuldige afweging ten aanzien van mogelijke nadelige effecten op (groepen van) studenten. Denk daarbij met name aan het borgen en bevorderen van diversiteit en inclusiviteit. Instellingen zien erop toe dat het gebruik van studiedata niet leidt tot (onbedoelde) discriminatie van groepen. Het gebruik van studiedata ondersteunt een actief diversiteitsbeleid dat bijdraagt aan minder ongelijkheid, aan het wegnemen van drempels en aan het garanderen van gelijke kansen voor iedereen.

Instellingen nemen maatregelen om te voorkomen dat heersende opvattingen en labeling het gedrag van docenten en studenten beïnvloedt, om negatieve effecten te voorkomen. Een eerlijke afweging wordt geborgd door zoveel mogelijk de medezeggenschap te betrekken bij het ontwikkelen van beleid, een gedragsode of richtsnoeren over het gebruik van studiedata.

Een eerlijke afweging wordt verder geborgd door zoveel mogelijk de medezeggenschap te betrekken bij het ontwikkelen van beleid, een gedragsode of richtsnoeren over het gebruik van studiedata, in elk geval voor zover dit verplicht is. Wanneer de zorgen en eventueel ook wensen van studenten en docenten tijdig worden meegenomen en meegewogen in het proces komt dit het verantwoorde gebruik ten goede en zorgt het voor meer vertrouwen in het gebruik van studiedata door de instelling.

2.2.3 Betrouwbare en valide analyse

Valide en betrouwbare analyses beginnen met een duidelijke vraagstelling. Het vraagt om bezinning op de stap die voorafgaat aan het verzamelen van data. Welke vraag willen we beantwoorden door het gebruik van studiedata? Welke soorten kwantitatieve en kwalitatieve informatie zijn daarvoor nodig? Hierbij zijn de principes van noodzakelijkheid en proportionaliteit leidend. Welke gegevens zijn echt noodzakelijk voor het doel? Kan het doel ook met minder of andere gegevens worden behaald? Kan het doel ook op een andere manier worden behaald?

Instellingen zorgen er verder voor dat het gebruik van studiedata van hoge methodologische kwaliteit is. Personen die een rol spelen bij het verwerken van studiedata dienen hiervoor een adequaat niveau van relevante kennis te ontwikkelen, op het gebied van statistiek en onderwijs. Alle algoritmen en statistieken – inclusief AI – die worden gebruikt, zoals voor voorspellende analyses of interventies, worden begrepen, gevalideerd, beoordeeld en waar nodig verbeterd door gekwalificeerd personeel.

Belangrijke aandachtspunten bij de verwerking van studiedata zijn:
- Onnauwkeurigheden in de gegevens 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 (zie paragraaf 8.3.1. voor een toelichting op deze begrippen);
- Valse correlaties worden vermeden;
- Resultaten van eerdere onderzoeken worden meegenomen;
- De resultaten worden getoetst op *confirmation bias*, *selffulfilling prophecy* of andere vormen van *bias;* en
- De verwerking, analyse en benutting van studiedata wordt steeds in hun bredere context gezien en waar nodig gecombineerd met andere kennis en benaderingen.

Belangrijke aandachtspunten voor de instellingen zijn:
- Een adequaat opleidingsniveau van medewerkers die met studiedata werken;
- Een zorgvuldige en tijdige communicatie van de resultaten naar de relevante belanghebbenden; en
- Een voortdurende geheugensteun over de verantwoordelijkheid die medewerkers die met studiedata werken, dragen.

2.2.4 Menselijke maat (menselijkheid en autonomie)

Door het gebruik van studiedata kunnen instellingen effectiever hun taken uitvoeren. Daarbij is het belangrijk om oog te houden voor de menselijke maat en de autonomie van betrokkenen. Dit geldt in het bijzonder wanneer op geautomatiseerde wijze, bijvoorbeeld met gebruik van kunstmatige intelligentie, studiedata wordt gebruikt. Instellingen zorgen dat altijd een mens betrokken is bij geautomatiseerd gebruik van studiedata, de zogeheten '*human in the loop*' of menselijke tussenkomst. Dit geldt in het geval van automatische processen die (mogelijk) gevolgen hebben voor individuele of kleine groepen identificeerbare studenten. Het geldt echter ook ten aanzien van de controle op de input, werking en output van de gebruikte algoritmes en andere vormen van kunstmatige intelligentie. Tevens moet een betrokkene bezwaar kunnen maken tegen een (deels) automatisch gemaakte beslissing.

Geautomatiseerd gebruik van gegevens, met name wanneer algoritmes en andere vormen van kunstmatige intelligentie worden ingezet, betekent niet dat de instelling niet verantwoordelijk is voor hetgeen het algoritme in gaat, erin gebeurt en er weer uitkomt. Integendeel, een instelling is ook verantwoordelijk voor het correct, zorgvuldig en eerlijk inzetten van algoritmes en kunstmatige intelligentie.

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

De instelling moet ook 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. Het gebruiken van (nieuwe) technieken moet daarenboven nooit een doel op zich zijn, maar een middel om het (hoger) doel te bereiken.

3 Scope en definities

In dit hoofdstuk wordt eerst ingegaan op wat wordt verstaan onder studiedata en voor welke toepassingen studiedata door hoger instellingen het meest gebruikt wordt. Daarna wordt ingegaan op de relevante begrippen ten aanzien van privacy en de bescherming van persoonsgegevens.,

3.1 Studiedata

Het begrip studiedata dat in dit Referentiekader wordt gebruikt omvat verschillende soorten informatie die gebruikt worden ten behoeve van de verbetering van de kwaliteit, effectiviteit en efficiëntie van het hoger onderwijs. Hieronder wordt met name verstaan het leveren van managementinformatie, de ontwikkeling van onderwijsbeleid, het uitvoeren van onderwijsonderzoek, het bevorderen van het studentsucces, wanneer nodig door gebruikmaking van individuele interventies. Het is niet beperkt tot alleen informatie over studenten, maar kan ook informatie over docenten en andere betrokkenen of onderwijsinformatie betreffen.

Geen enkel type data of persoonsgegeven is op zichzelf studiedata of wordt specifiek voor dat doel verzameld. Maar in potentie kan wel alle (veelal combinaties van) informatie die een hoger onderwijsinstelling heeft als studiedata worden gebruikt.

De specifieke verwerkingen van de informatie en het doel van de verwerkingen bepalen dus of de informatie onder het begrip studiedata valt.

Voor de context van het Referentiekader wordt een brede notie van studiedata gehanteerd, waaronder zowel big data als kleine datasets, zowel gestructureerde als ongestructureerde data, zowel data uit administratieve als uit managementsystemen en zowel historische als *real-time* data. Dit Referentiekader is met name van toepassing op studiedata die herleidbaar is tot individuele personen.

3.2 Toepassingen van studiedata

Binnen de instellingen wordt studiedata gebruikt door bestuurders, opleidingsdirecteuren, docenten, ondersteuners, beleidsmedewerkers, studentbegeleiders en onderzoekers die ieder vanuit hun eigen rol studiedata inzetten om het onderwijs te verbeteren. Ook maken

studenten zelf gebruik van de inzichten die studiedata biedt.[6] Analyses met studiedata zijn ook interessant en relevant voor partijen buiten de instellingen zelf. Denk aan beleidsmakers bij de nationale, regionale en lokale overheden en toezichthouders zoals de onderwijsinspectie.

In het kader van het gebruik van studiedata worden de termen '*learning analytics*', '*student analytics*', '*business analytics*' en '*predictive analysis*' veel gebruikt. Niet alle instellingen geven echter dezelfde invulling aan deze termen. Daarnaast zijn er instellingen die eigen terminologie hanteren om te beschrijven waarvoor zij studiedata gebruiken binnen hun instelling. Om verwarring te voorkomen, worden in dit Referentiekader geen specifieke termen gebruikt, maar worden de mogelijke toepassingen gehanteerd. Dit zijn:

- Individuele interventies;
- Verbeteren van de kwaliteit, effectiviteit en efficiëntie van onderwijs en onderwijsbeleid; en
- Wetenschappelijk onderwijsonderzoek.

Instellingen moeten zelf bepalen voor welke toepassing(en) zij studiedata willen gebruiken en of zij hier een specifieke term aan willen verbinden die passend is voor hun eigen instelling.

3.2.1 Individuele interventies

In bepaalde gevallen kan studiedata worden gebruikt voor individuele interventies of interventies gericht op een kleine groep studenten van wie de identiteit bekend of herleidbaar is. Dit zal met name gedaan worden om de student of een kleine groep studenten beter te begeleiden met als doel het bevorderen van hun studiesucces.

3.2.2 Verbeteren kwaliteit, effectiviteit en efficiëntie onderwijs en onderwijsbeleid en managementinformatie

Studiedata kan ook worden gebruikt ter verbetering van de kwaliteit, effectiviteit en efficiëntie van onderwijs of onderwijsbeleid of voor managementinformatie. Bijvoorbeeld om gericht instroom, doorstroom en uitstroom van studenten in alle opleidingsfasen te optimaliseren, alsook om inzicht te krijgen in de factoren die een rol spelen bij studentsucces. Dit richt zich op het verkrijgen van groepsinzichten en niet op het verkrijgen van inzichten in het individuele (toekomstige) functioneren van studenten.

[6] Een beschrijving van de voordelen van datagedreven werken voor hoger onderwijsinstellingen valt buiten de scope van dit stuk. Voor een overzicht van de mogelijkheden voor verschillende doelgroepen verwijzen we naar: doe-meer-met-studiedata.nl/

3.2.3 Wetenschappelijk onderwijsonderzoek

Studiedata kan, onder voorwaarden, worden gebruikt voor wetenschappelijk onderzoek, bijvoorbeeld naar studie-uitval, studiesucces of om de kwaliteit van het onderwijs te onderzoeken, bijvoorbeeld als wetenschappers willen onderzoeken welke lesmethode de beste resultaten oplevert.

In detail: wetenschappelijk onderzoek en de AVG

Volgens de AVG moet een ruime opvatting worden aangehouden van wetenschappelijk onderzoek, waaronder onder andere vallen wetenschappelijk onderzoek met het oog op technische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en studies op het gebied van de volksgezondheid in het algemeen belang.

Daarnaast wordt erkend dat wetenschappelijk onderzoek kan worden gefinancierd uit particuliere middelen. Wel moet de verwerking voor wetenschappelijke onderzoeksdoeleinden aan specifieke voorwaarden voldoen, met name wat betreft het publiceren of anderszins openbaar maken van persoonsgegevens voor wetenschappelijke onderzoeksdoeleinden.

In detail: gedragscode Wetenschappelijke Integriteit

De Nederlandse Code Wetenschappelijke Integriteit kent een vergelijkbaar toepassingsbereik als de AVG, namelijk wetenschappelijk onderzoek in den brede, zoals dat wordt uitgevoerd aan de instellingen die de code onderschrijven, waaronder de VSNU, VH en KNAW. Wetenschappelijk onderzoek omvat zowel publiek als privaat gefinancierd en zowel fundamenteel als praktijkgericht onderzoek. Onder onderzoek worden alle activiteiten verstaan die aan de onderzoekspraktijk verbonden zijn, zoals het opstellen van de aanvragen, opzet en uitvoering van het onderzoek, beoordeling en peer review, het optreden als inhoudelijk deskundige, verslaglegging, verantwoording en publiciteit.

In de Gedragscode Wetenschappelijke Integriteit worden de normen voor een goede onderzoekspraktijk genoemd. Hierin worden ook normen genoemd die in het kader van zorgvuldig gebruik van studiedata voor wetenschappelijk (onderwijs) onderzoek ook relevant zijn. Denk dan aan onder andere de volgende in de Gedragscode vervatte normen:

- Zorg dat de vereiste toestemmingen worden verkregen en dat voor zover nodig ethische toetsing plaatsvindt.
- Beschrijf eerlijk, zorgvuldig en zo transparant mogelijk de data die verzameld zijn voor en/of gebruikt zijn in het onderzoek
- Houd rekening met belangen van (proef)personen, (proef)dieren en de risico's voor de onderzoekers en de omgeving, waarbij in ieder geval alle relevante wettelijke voorschriften en gedragscodes in acht worden genomen.
- Wees transparant over de gevolgde methode en werkwijze, en leg deze waar relevant vast.

3.3 Privacy en de bescherming van persoonsgegevens

In deze paragraaf wordt uitgewerkt wanneer dit referentiekader van toepassing is. Dit houdt ook een duiding in van de belangrijkste begrippen in het kader van het verantwoord gebruik van studiedata vanuit het perspectief van privacy en ethiek.

Privacy is een meervoudig begrip. Wat wordt verstaan onder privacy kan per persoon, land of cultuur verschillen. Dit maakt het moeilijk om privacy te definiëren en vast te leggen in wetten of regels.

Het Europees Handvest voorziet dan ook niet in een recht op privacy, maar in het recht op 'eerbiediging van het privéleven en van het familie- en gezinsleven', alsook op het recht van 'de bescherming van persoonsgegevens'.[7] Het eerste betreft ook het recht op eerbiediging van woning en communicatie (denk aan het briefgeheim). Het tweede betreft het recht op bescherming van persoonsgegevens, wat voor een groot deel overlap heeft met het recht op eerbiediging van het privéleven.

Het recht op bescherming van persoonsgegevens wordt nader geregeld de Europese Unie in de AVG. Voor een deel bevat de AVG open normen, waarbinnen organisaties zelf afwegingen kunnen maken ten aanzien van het verantwoord gebruik van persoonsgegevens. Denk dan bijvoorbeeld aan de norm dat 'passende beveiligingsmaatregelen' worden getroffen; wat passend is hangt af van veel verschillende factoren, waaronder de organisatie, de betrokkenen, de aard van de gegevens en de wijze waarop de gegevens worden verwerkt.

Daarnaast geeft de AVG de ruimte aan de lidstaten van de EU om aan bepaalde onderwerpen een eigen nadere invulling te geven in nationale wetgeving. Hiermee krijgen lidstaten de ruimte om op bepaalde punten nadere invulling te geven specifiek voor de nationale context. In Nederland zijn deze nadere bepalingen vastgelegd in de Uitvoeringswet AVG (UAVG). Hierin zijn bijvoorbeeld de uitzonderingen, die gelden in Nederland, vastgelegd voor het gebruik van bijzondere persoonsgegevens voor wetenschappelijk onderzoek (zie hiervoor ook paragraaf 3.4.1.). De AVG en de UAVG zijn daarom voor dit Referentiekader leidend als het de verwerking van persoonsgegevens betreft.

3.4 Relevante begrippen uit de (U)AVG

De volgende begrippen uit de (U)AVG zijn met name van belang voor dit Referentiekader:

- Verwerken;
- Persoonsgegevens & bijzondere persoonsgegevens;
- Verwerkingsverantwoordelijke; en
- Betrokkene

3.4.1 Verwerken

Een verwerking is elke bewerking die relateert aan persoonsgegevens, al dan niet geautomatiseerd uitgevoerd. Dit betreft dus onder andere het verzamelen, ordenen, opvragen, opslaan, combineren, tot en met het vernietigen van persoonsgegevens.

In dit Referentiekader

In het kader van het (verantwoorde) gebruik van studiedata betreft dit dus in feite alle handelingen met de (persoons)gegevens die worden gebruikt voor studiedata. Dit betreft dan onder andere het selecteren, verzamelen, opslaan, combineren, verrijken en vernietigen van de data.

3.4.2 Persoonsgegevens & bijzondere persoonsgegevens

Persoonsgegevens zijn alle gegevens, of beter gezegd alle informatie, over een geïdentificeerde of identificeerbare persoon (ook wel de betrokkene, zie hiervoor paragraaf 3.4.4.). Dit moet altijd een natuurlijke persoon betreffen, dus een mens van vlees en bloed, die nog in leven is. Informatie van overleden personen zijn alleen persoonsgegevens voor zover het (ook) relateert aan iemand anders, bijvoorbeeld nabestaanden. Informatie die relateert aan rechtspersonen, zoals publieke instellingen, bedrijven of stichtingen, zijn geen persoonsgegevens.

Een persoonsgegeven kan alle informatie betreffen die direct of indirect leidt tot de identificatie van een persoon. Dit kan (in)direct identificerende informatie zijn, zoals een naam of een (online) identificatienummer, maar ook een of meer elementen tezamen die kenmerkend zijn voor de identiteit van een persoon. Het zal dus voor een deel van de context

[7] Zie artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie.

afhangen of bepaalde informatie een persoonsgegeven betreft of niet. In de praktijk zal vrijwel alle informatie die herleidbaar is tot een identificeerbaar persoon als persoonsgegevens beschouwd moeten worden.

Het verwerken van zogeheten “gewone” persoonsgegevens is toegestaan, mits wordt voldaan aan de vereisten uit de wet, zoals het formuleren van een welbepaald doel, het hebben van een grondslag en het treffen van passende beschermingsmaatregelen. Deze drieslag wordt in het volgende hoofdstuk nader uitgewerkt. Dit in tegenstelling tot het verwerken van “bijzondere” persoonsgegevens, waar een algemeen verbod op rust met een beperkt aantal duidelijk omschreven uitzonderingen.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn persoonsgegevens waaruit ras of etnische afkomst blijkt, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, 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.[8] Bijzondere persoonsgegevens mogen niet worden verwerkt, tenzij de betrokkene uitdrukkelijke toestemming heeft gegeven of als er een andere uitzondering van toepassing is die is voorzien bij of in de wet.[9]

In de UAVG is vastgelegd dat het verbod niet van toepassing is op verwerking van bijzondere persoonsgegevens voor wetenschappelijke of historische onderzoeksdoeleinden als aan *alle* onderstaande voorwaarden wordt voldaan:

1. De verwerking is noodzakelijk met het oog op het wetenschappelijk of historisch onderzoek;
2. Het onderzoek dient een algemeen belang;
3. Het vragen van uitdrukkelijke toestemming blijkt onmogelijk of kost onevenredige inspanning; en
4. Er zijn zodanige waarborgen getroffen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

[8] Dit is een limitatieve lijst, zie ook artikel 9(1) AVG.

[9] De algemene uitzonderingen op het verwerkingsverbod zijn in een limitatieve lijst opgenomen in artikel 9 (2) AVG en de uitzonderingen die specifiek in Nederland gelden zijn opgesomd in de UAVG.

In dit Referentiekader

Zoals ook in het vorige hoofdstuk staat, omvat het begrip studiedata alle verschillende soorten informatie die gebruikt worden ten behoeve van de verbetering van de kwaliteit, effectiviteit en efficiëntie van het onderwijs. Dit is niet beperkt tot alleen informatie over studenten, maar kan ook informatie over docenten, andere betrokkenen of onderwijsinformatie betreffen.

Bijzondere persoonsgegevens mogen in principe niet worden gebruikt als studiedata. Alleen als hier uitdrukkelijke toestemming voor gegeven is door de betrokkene zelf zou dit wel kunnen. Ook als studiedata voor wetenschappelijk of historisch onderzoek wordt gebruikt, kunnen, onder de hierboven genoemde voorwaarden, bijzondere persoonsgegevens worden verwerkt.

In detail: wetenschappelijk onderzoek, valorisatie en beleidsvorming

Wetenschappelijk onderzoek, waarbij persoonsgegevens zijn gebruikt, bijvoorbeeld van proefpersonen, zal resulteren in inzichten. Deze inzichten kunnen door een instelling gevaloriseerd worden binnen het proces van beleidsvorming.

Als de inzichten zelf geen persoonsgegevens meer betreffen, bijvoorbeeld doordat er voldoende geaggregeerd is of omdat voorbeelden of casussen volledig geanonimiseerd zijn (zie ook paragraaf 8.3.1.), kunnen zij worden gebruikt voor beleidsdoeleinden, zonder dat de instelling aan bepaalde eisen hoeft te voldoen. Deze inzichten bevatten dan namelijk geen persoonsgegevens.

Als het resultaat van het wetenschappelijke onderzoek, waaronder de inzichten, nog wel persoonsgegevens betreffen, is het niet zonder meer toegestaan voor een instelling om deze uitkomsten te gebruiken voor beleidsdoeleinden. In dit geval zal moeten worden beoordeeld of dit verdere gebruik van de persoonsgegevens voor beleidsdoeleinden verenigbaar is met het oorspronkelijke gebruik van de persoonsgegevens voor wetenschappelijk onderzoek (zie over doelbinding en verenigbaar gebruik meer in het volgende hoofdstuk).

Tot slot, voor het doen van wetenschappelijk onderzoek kunnen onder omstandigheden – zoals hierboven beschreven – bijzondere persoonsgegevens worden gebruikt. Als het resultaat van het wetenschappelijke onderzoek, waaronder inzichten en daaruit volgende beleidsaanbevelingen, ook nog bijzondere persoonsgegevens bevat, mogen deze in beginsel niet verder worden verwerkt voor

beleidsdoeleinden. Wanneer de inzichten geen persoonsgegevens bevatten, kunnen deze inzichten worden gebruikt voor beleidsdoeleinden.

Nationaal identificatienummer

Een nationaal identificatienummer, in Nederland het Burger Service Nummer (BSN), wordt niet gezien als een bijzonder persoonsgegeven, maar het gebruik ervan is wel aan strikte regels onderworpen. Het BSN mag alleen gebruikt worden voor die specifieke doeleinden die bij Nederlandse wet zijn vastgelegd en niet voor enig ander doel.

Instellingen moeten het BSN verwerken ten behoeve van de inschrijving en communicatie met overheidsinstanties. Het is instellingen niet toegestaan het BSN voor andere doeleinden te gebruiken, waaronder in het kader van studiedata, ook niet als kenmerk om databases of bestanden te koppelen.

In detail: studentnummer

Het studentnummer is niet hetzelfde als een nationaal identificatienummer. Niettemin is het een persoonsgegeven van de student dat onlosmakelijk met hem/haar verbonden is gedurende de studietijd (en wellicht ook nog enige tijd daarna).

Ondanks het feit dat het gebruik van het studentnummer dus niet valt onder het strikte regime van het BSN is het wel van belang dat ook bij het gebruik van een studentnummer voldoende aandacht wordt besteed aan de waarborgen ter bescherming van de student

3.4.3 Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke is de natuurlijke persoon of de rechtspersoon, overheidsinstantie, een dienst of een ander orgaan die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt, alleen of samen met anderen. De organisatie die, al dan niet samen met andere organisaties, bepaalt dat er persoonsgegevens (moeten) worden verzameld, waarvoor dat gebeurt en op welke wijze dat gebeurt, is dus de verwerkingsverantwoordelijke. Deze organisatie is er uiteindelijk verantwoordelijk voor dat op een behoorlijke en rechtmatige wijze met persoonsgegevens wordt omgegaan.

Wanneer twee organisaties gaan samenwerken en samen bepalen welke persoonsgegevens verwerkt moeten worden, voor welke doeleinden en op welke manier, zijn dit zogeheten gezamenlijke verantwoordelijken (zie voor meer informatie paragraaf 8.2). Gezamenlijke verantwoordelijken moeten afspraken maken over de onderlinge verdeling van taken en verantwoordelijkheden en moeten de essentie van deze afspraken kenbaar maken aan de betrokkenen. Ook moeten zij duidelijk aangeven hoe de rechten van betrokkenen kunnen worden uitgeoefend en wie de relevante informatie aan betrokkenen verstrekt (zie ook paragraaf 8.3).

In dit Referentiekader

Dit Referentiekader betreft het verantwoord gebruik van studiedata door (medewerkers van of onderzoekers verbonden aan) de hoger onderwijsinstellingen in Nederland. Voor het gebruik van studiedata, meer specifiek voor het gebruik van de persoonsgegevens als studiedata, is de instelling de verwerkingsverantwoordelijke. Wat deze verantwoordelijkheid inhoudt en hoe hieraan invulling kan worden gegeven, wordt in de volgende hoofdstukken verder behandeld.

In detail: verwerkingsverantwoordelijke en verantwoordelijkheden

De instelling is de verwerkingsverantwoordelijke in de zin van de wet. Medewerkers van een instelling zelf zijn geen zelfstandige verwerkingsverantwoordelijke wanneer zij persoonsgegevens gebruiken in het kader van hun werkzaamheden voor de instelling, maar handelen dan wel in naam van de verwerkingsverantwoordelijke. In hoofdstuk 6 wordt nader ingegaan op de interne verantwoordelijkheidsverdeling.

3.4.4 Betrokkene

De betrokkene is de natuurlijke persoon die kan worden geïdentificeerd, direct of indirect, door specifieke identificerende elementen of nummers, of door één of een combinatie van elementen die kenmerkend zijn voor zijn identiteit. Dit is een nog levende persoon van vlees en bloed aan wie de persoonsgegevens relateren. De betrokkene kan ook bepaalde rechten uitoefenen ten aanzien van zijn persoonsgegevens, zie hiervoor meer in hoofdstuk 7. Wanneer informatie over meerdere natuurlijke personen wordt gebruikt, spreek je van meerdere betrokkenen.

Toelichting: gebruik term ‘betrokkene’

De betrokkene is dus de juridische term waarmee degene wordt aangeduid aan wie de persoonsgegevens relateren. De term ‘betrokkene’ zal daarom ook in dit Referentiekader deze lading hebben. Wanneer we in dit Referentiekader een of meer personen bedoelen die een betrokkenheid of belang hebben bij het gebruik van studiedata, dan noemen we deze belanghebbenden.

In dit Referentiekader

De betrokkenen in het geval van studiedata zijn studenten, aankomend studenten, belangstellenden, oud-studenten, docenten, begeleiders en alle andere personen van wie persoonsgegevens worden verwerkt door hoger onderwijsinstellingen. Ondanks dat studiedata veelal gegevens van studenten betreffen, zal het dus ook persoonsgegevens van docenten en anderen kunnen betreffen. Daarnaast kunnen de persoonsgegevens ook gegevens betreffen over vakken, curricula en (clusters van) opleidingen die door een student zijn gevolgd of worden gegeven door docenten en over onderwijsinstellingen, faculteiten en academies waar de betrokkene aan verbonden is.

In detail: ‘eigenaarschap’ van persoonsgegevens

De term ‘eigenaarschap’ kan leiden tot veel verwarring wanneer het gaat over persoonsgegevens. In dit Referentiekader wordt daarom deze term niet verder gebruikt, maar wordt vooral ingegaan, met name in hoofdstukken 4 en 5, op wie de verwerkingsverantwoordelijke is voor de persoonsgegevens, wat diens verplichtingen zijn en hoe de interne verantwoordelijkheidsverdeling kan worden ingericht.

In de praktijk zullen er bij instellingen echter zogeheten ‘data-eigenaar’ zijn, die het beheer hebben over een bepaalde dataset en daarmee dus bepaalde verantwoordelijkheden hebben ten aanzien van die dataset. Deze personen kun je ook beschouwen als beheerders van een bepaald register of data stewards.

Dit betekent overigens niet dat degene die verantwoordelijk is voor een dataset, hier ook de ‘eigenaar’ van is in de juridische zin. De betrokkene noch de instelling is juridische gezien ‘eigenaar’ van persoonsgegevens. Een student kan immers niet zelf bepalen of hij / zij bijvoorbeeld zijn / haar rekeningnummer verstrekt aan een instelling, dit zal hij / zij moeten doen, zodat het collegegeld kan worden geïnd. Een instelling mag op haar beurt ook niet zonder meer beslissen aan wie het dit bankrekening beschikbaar stelt. De instelling mag dat alleen doen als dat is toegestaan bij wet.

4 Verantwoordelijkheden van instellingen

De hoger onderwijsinstelling is als organisatie de verwerkingsverantwoordelijke in de zin van de (U)AVG voor het verwerken van persoonsgegevens, waaronder studiedata. Dit betekent dat op de hoger onderwijsinstelling bepaalde verantwoordelijkheden rusten, waarvan de belangrijkste in dit hoofdstuk worden uitgewerkt. De essentie is terug te brengen tot drie elementen en de daarbij behorende vragen.

Hieronder worden de bovenstaande vereisten, die grotendeels volgen uit de AVG, nader uitgewerkt.

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?

4.1 Doel

Alle gegevens moeten voor een duidelijk en welbepaald doel worden gebruikt en mogen niet zomaar verder worden verwerkt voor andere doelen. Dat betekent allereerst dat moet worden vastgesteld waarom persoonsgegevens gaan worden verzameld en gebruikt. Dit kunnen overigens meerdere doelen tegelijkertijd zijn. Het doel, of de doelen, moet(en) zo specifiek mogelijk geformuleerd zijn.

Voordat persoonsgegevens voor een ander doel kunnen worden gebruikt dan waarvoor ze zijn verzameld, moet een afweging worden gemaakt of het nieuwe doel verenigbaar is met het oorspronkelijke doel. Om te beoordelen of sprake is van een verenigbaar gebruik moet een afweging worden gemaakt door de instelling zelf. Bij deze afweging moeten in elk geval aspecten worden meegewogen als het oorspronkelijke en het nieuwe doel, de context waarin de gegevens zijn verkregen, de aard van de gegevens, de aard van het gebruik en de mogelijke gevolgen voor de betrokkene van het verdere gebruik. Indien een nieuw doel niet verenigbaar is, is het niet toegestaan om de gegevens verder te gebruiken voor het nieuwe doel, tenzij toestemming is verkregen van de betrokkene(n) om diens gegevens voor het nieuwe doel te gebruiken.

In dit Referentiekader

Bij het gebruik van studiedata gaat het in feite altijd om een verdere verwerking van data. Daarom moet allereerst duidelijk worden gemaakt welk doel wordt nagestreefd met het gebruik van studiedata en moet dit doel bij het gebruik leidend blijven. Het doel moet zo specifiek en welbepaald mogelijk beschreven zijn. Slechts verwijzen naar de algemene doelen van verbetering onderwijs, onderwijsbeleid, het uitvoeren van onderwijsonderzoek of het doen van individuele dan wel kleinschalige interventies, is niet voldoende specifiek. Daarnaast zal moeten worden beoordeeld in hoeverre het gebruik van de data voor dit doel verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verzameld. Of een nieuw doel verenigbaar is, vraagt een afweging van de (eindgebruiker binnen de) instelling, waarbij rekening wordt gehouden met de context en aard van het gebruik, de aard van de gegevens en de mogelijke gevolgen voor de betrokkenen. Wanneer het doel van een verwerking bijvoorbeeld is om studenten maandelijks een nieuwsbrief van de faculteit te sturen, zal het waarschijnlijk wel verenigbaar zijn om de gegevens ook te gebruiken om een eenmalige informatie-mail uit te sturen over bijvoorbeeld de benoeming van een nieuwe decaan.

In detail: wetenschappelijk (onderwijs)onderzoek als doel

Wanneer studiedata voor wetenschappelijk (onderwijs)onderzoek wordt gebruikt, stelt de AVG dat in principe mag worden aangenomen dat dit een verenigbaar gebruik is. Om echter te borgen dat studiedata daadwerkelijk verantwoord wordt gebruikt, is niettemin vereist dat een duidelijk doel moet zijn bepaald voor de verwerking van de gegevens en moeten nog steeds passende waarborgen worden getroffen, waarbij ook de verwachtingen van en gevolgen voor de studenten worden meegenomen.

4.2 Juridische grondslag

Om te spreken van rechtmatige verwerking van persoonsgegevens moet de verwerking zijn gebaseerd op een van de zes grondslagen die worden voorzien in de AVG. Dit zijn de volgende grondslagen:

- Toestemming
- Noodzakelijk ter uitvoering van een contract (contract)
- Noodzakelijk om te voldoen aan een wettelijke verplichting (wettelijke plicht)
- Noodzakelijk voor de vrijwaring van de vitale belangen van de betrokkene (vitaal belang)
- Noodzakelijk voor een taak in algemeen belang of uitvoering van het openbaar gezag (algemeen belang)
- Noodzakelijk voor de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde (gerechtvaardigd belang)

Er is geen hiërarchische volgorde tussen de grondslagen. Het is echter wel vereist dat er een grondslag is voor de verwerking van gegevens en dat deze passend is voor de verwerking. Welke grondslag het meest passend is, zal ook afhangen van het doel van de verwerking. In het kader van studiedata zullen de grondslagen ‘toestemming’, ‘taak in algemeen belang’ en ‘gerechtvaardigd belang’ het meest voorkomen. Hieronder worden voor deze drie grondslagen de voorwaarden en vereisten die hieraan verbonden zijn nader toegelicht.

4.2.1 Toestemming

Toestemming moet vrij, geïnformeerd, specifiek en ondubbelzinnig gegeven zijn. Dit betekent dat de betrokkene alle informatie moet hebben om een goed afgewogen keuze te maken of zij al dan niet instemt met de voorgenomen verwerking van persoonsgegevens. Deze instemming moet tevens ondubbelzinnig zijn in de zin dat er geen twijfel mag bestaan dat toestemming is gegeven door de betrokkene. Dit hoeft niet altijd schriftelijke toestemming te betekenen. Andere vormen zijn ook mogelijk, zolang het maar duidelijk en aantoonbaar is dat toestemming is gegeven. De bewijslast ligt bij de verwerkingsverantwoordelijke om aan te tonen dat de toestemming is verkregen.

Toestemming moet ook vrij zijn gegeven, wat betekent dat iemand volledig vrij moet zijn om een keuze te maken. Hij mag geen druk voelen of in een afhankelijke relatie staan tot de verwerkingsverantwoordelijke waardoor ook maar enigszins de vrije keuze kan worden aangetast. Aan het weigeren van toestemming mogen dan ook geen enkele negatieve consequenties verbonden zijn. Ook moet de betrokkene de toestemming altijd in kunnen trekken.

4.2.2 Algemeen belang

Om de grondslag te gebruiken dat de verwerking van persoonsgegevens ‘noodzakelijk is voor de uitoefening van een taak in het algemeen belang’ moet bij wet zijn vastgelegd welke organisatie deze taak heeft en bij voorkeur ook het doel van de verwerking van persoonsgegevens, de betrokkenen, de categorieën persoonsgegevens die hiervoor noodzakelijk zijn, evenals de bewaartermijnen, de doelbinding en de entiteiten waaraan de gegevens worden verstrekt. Diezelfde wet moet voorts ook echt een doelstelling in het algemeen belang nastreven en de verwerking moet evenredig zijn met het nagestreefde doel.

Het moet tevens noodzakelijk zijn om de gegevens te gebruiken voor het vervullen van de taak in algemeen belang. Dit vraagt van de organisatie dat het beoordeelt welke gegevens echt onmisbaar zijn om het doel te behalen. Daarnaast moet het doel niet op een andere,

minder ingrijpende manier, kunnen worden bereikt en moet worden beoordeeld of het passend dan wel evenredig is dat de gegevens worden gebruikt voor het nagestreefde doel.

4.2.3 Gerechtvaardigd belang

Bij gebruik van de grondslag 'noodzakelijk voor de behartiging van de gerechtvaardigde belangen' moet een belangenafweging worden gemaakt tussen de belangen van de organisatie enerzijds en de belangen, rechten en vrijheden van de betrokkene(n) anderzijds. Elementen die in deze afweging meegewogen moeten worden zijn onder andere de aard van de gegevens, de categorie betrokkene(n), de relatie tussen de betrokkene(n) en de verwerkingsverantwoordelijke en de mogelijke gevolgen van de verwerking voor de betrokkene. De belangenafweging moet worden gedocumenteerd en moet indien nodig ook worden gecommuniceerd met de betrokkene.

In dit Referentiekader

Het zal afhangen van de toepassing van het gebruik van studiedata en de specifieke instelling welke grondslag het meest passend is voor het gebruik van studiedata. Per gebruik van studiedata zal moeten worden beoordeeld door de instelling welke grondslag in dat geval het meest passend is. Voor bepaalde toepassingen en voor bepaalde instellingen zal het bijvoorbeeld logischer zijn dat het gebruik van studiedata ten behoeve van het uitoefenen van een taak in algemeen belang gebeurt. Voor andere toepassingen en/of instellingen zal het echter meer geëigend zijn om een belangafweging te maken in het kader van de grondslag dat het gebruik van studiedata noodzakelijk is ter behartiging van de gerechtvaardigde belangen.

Wanneer (uitdrukkelijke) toestemming de gebruikte grondslag of uitzonderingsgrond is, moet met name rekening worden gehouden met het vereiste dat dit daadwerkelijk vrij gegeven is. Als aan een weigering negatieve consequenties zijn verbonden, is er geen sprake van vrije toestemming. Ook wanneer de student of werknemer het gevoel heeft dat ze niet kan weigeren, omdat er een afhankelijkheidsrelatie bestaat tussen de student of werknemer enerzijds en de instelling anderzijds, is er geen sprake van vrije toestemming.

4.3 Zorgvuldigheid

Onder zorgvuldigheid wordt verstaan: alle verplichtingen die rusten op organisaties die persoonsgegevens verwerken om te zorgen dat op een verantwoorde manier met gegevens wordt omgegaan.

Allereerst is het van belang dat iedere verwerking behoorlijk, rechtmatig en transparant gebeurt. Om te spreken van een behoorlijke gegevensverwerking mag de gegevensverwerking geen onevenredige inbreuk maken op de fundamentele rechten en vrijheden die een mens geniet. Wanneer een verwerking bijvoorbeeld leidt tot discriminerend handelen door een verwerkingsverantwoordelijke is dit onbehoorlijk. Rechtmatig houdt in dat de gegevensverwerking in overeenstemming met de wet plaatsvindt. Op de praktische invulling van de transparantieverplichting wordt nader ingegaan in hoofdstuk 6.

Daarnaast moet aan de volgende principes sowieso voldaan worden voor een zorgvuldige gegevensverwerking:

- Dataminimalisatie; alleen die (persoons)gegevens die noodzakelijk zijn, mogen worden verwerkt. Als het niet of niet langer nodig is om direct identificerende gegevens te gebruiken, moeten de gegevens zo snel mogelijk worden gepseudonimiseerd. Dit geldt in het bijzonder voor persoonsgegevens die worden verwerkt voor historisch of wetenschappelijk onderzoek.
- Juistheid; de (persoons)gegevens die worden verwerkt moeten juist zijn.
- Bewaartermijnen; (persoons)gegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doel. Voor zover het noodzakelijk is voor historisch of wetenschappelijk onderzoek mogen gegevens langere perioden worden opgeslagen, mits passende technische en organisatorische waarborgen worden getroffen.
- Beveiliging; er moeten passende technische en organisatorische maatregelen worden genomen zodat persoonsgegevens op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is.

Een aantal van deze zorgvuldigheidsprincipes en -uitgangspunten worden in de volgende hoofdstukken verder geconcretiseerd.

5 Interne verantwoordelijkheidsverdeling

Een hoger onderwijsinstelling is als rechtspersoon de zogeheten verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens, zoals ook in hoofdstuk 4 is uiteengezet. De mensen die werken voor of bij een hoger onderwijsinstelling kunnen dus niet worden aangemerkt als de verwerkingsverantwoordelijke in de zin van de wet. Zij handelen bij het uitoefenen van hun functie echter wel namens de instelling. Daarom hebben medewerkers van en onderzoekers verbonden aan een hoger onderwijsinstelling die met studiedata werken wel een rol te spelen in het verantwoord gebruik van studiedata. Wie welke verantwoordelijkheid draagt voor de beslissingen ten aanzien van studiedata binnen een instelling moet door de instelling worden bepaald en vastgelegd.

Hoger onderwijsinstellingen verschillen van elkaar in grootte, cultuur, geschiedenis, ambities en visie. Er is daarom geen o*ne-size-fits-all* oplossing voor de manier van het bepalen en vastleggen van de verantwoordelijkheden van de verschillende betrokken functionarissen. Het is echter wel belangrijk om binnen een instelling duidelijk te hebben wie welke rol speelt bij het maken van de juridische en ethische afwegingen en bij het nemen van beslissingen bij het gebruik van studiedata.

De manier waarop intern de verantwoordelijkheden worden neergelegd, wordt niet nader ingevuld in wet- en regelgeving. Het enige dat wordt geregeld in de AVG, is onder welke omstandigheden een Functionaris voor Gegevensbescherming (FG) moet worden aangesteld en wat diens positie en taken zijn (zie voor meer over de FG paragraaf 5.2.2).

Daarom wordt in dit Referentiekader nader ingegaan op de eindverantwoordelijkheid voor de afwegingen rondom studiedata, de functionarissen die een rol spelen ten aanzien van het verantwoord gebruik van studiedata en tot slot de manieren waarop de verantwoordelijkheden kunnen worden verdeeld.

5.1 Eindverantwoordelijkheid

De eindverantwoordelijkheid voor vrijwel alles dat er binnen een hoger onderwijsinstelling gebeurt, ligt bij het College van Bestuur (CvB), als dagelijks bestuur van de instelling. Dit geldt ook voor het gebruik van studiedata. Via delegatie- of mandaatregelingen kan het CvB wel bepaalde verantwoordelijkheden bij een andere functionaris beleggen, zoals

bij een decaan of directeur.[10] Voor de onderwijssector is het niet ongebruikelijk om van dergelijke regelingen gebruik te maken, al worden deze regelingen vrijwel nooit publiek gemaakt.

In detail: delegatie- en mandaatregelingen
Binnen de Rijksoverheid wordt veel gebruik gemaakt van delegatie- en mandaatregelingen, deze zijn raadpleegbaar op de website van de overheid. Bij delegatie is er sprake van het daadwerkelijk overdragen van bevoegdheden, waaronder verantwoordelijkheden. Bij mandatering wordt de bevoegdheid niet overgedragen en kan de mandaatgever dus altijd nog zijn bevoegdheden blijven uitoefenen.

In de praktijk zal het echter (vaak) niet zo zijn dat het College van Bestuur direct betrokken is bij elk specifiek gebruik van studiedata. Om te borgen dat de hoger onderwijsinstelling wel de verplichtingen uit de wet kan nakomen, zal daarom moeten worden bepaald en vastgelegd wie, dan wel welke functies, binnen de instelling hierin een rol spelen. In de volgende paragraaf worden de betrokken functionarissen genoemd.

5.2 Betrokken functionarissen

Vanwege het feit dat alle hoger onderwijsinstellingen verschillend zijn, kennen ook niet alle instellingen dezelfde inrichting en dezelfde functies. Het zal daarom aan de instelling zelf zijn om in kaart te brengen welke functionarissen betrokken (moeten) zijn bij het gebruik van studiedata. Niettemin wordt in dit Referentiekader een aantal functies benoemd die bij het bepalen en vastleggen van de verantwoordelijkheden vrijwel zeker meegenomen moeten worden.

5.2.1 Eindgebruikers

Allereerst zijn de eindgebruikers een belangrijke categorie functionarissen waar aandacht aan moet worden besteed. Denk dan aan de volgende personen die studiedata kunnen gebruiken voor een specifiek doel:

[10] Bij universiteiten hebben decanen hebben ook zelfstandige (geattribueerde) bevoegdheden op grond van de WHW.

- Lid van het CvB (bijvoorbeeld om inzicht te krijgen op hoofdlijnen van inschrijvingen en afgestudeerden)
- Onderwijsdirecteur of de Directeur Onderwijs (bijvoorbeeld om beleid over doorstroom en studiesucces te kunnen uitstippelen)
- Beleidsmedewerker (bijvoorbeeld om onderbouwd beleidsadvies te kunnen geven)
- Docent (bijvoorbeeld om inzicht in de ontwikkeling van de kwaliteit van het eigen vak te krijgen)
- Ondersteuner (bijvoorbeeld om docenten beter te kunnen ondersteunen bij de inrichting van zijn of haar digitale onderwijs)
- Onderzoeker (bijvoorbeeld om longitudinaal onderzoek te doen naar de impact van een beleidsmaatregel op studeergedrag)
- Opleidingsdirecteur (bijvoorbeeld om inzicht te krijgen in de trend van de afgelopen tijd en verwachtingen voor de toekomst)
- Student (bijvoorbeeld om beter inzicht te krijgen in de eigen ontwikkeling t.o.v. zijn of haar jaargenoten)
- Studiebegeleider (bijvoorbeeld om beter te kunnen bepalen waar of wanneer een student begeleiding nodig heeft)

De eindgebruiker zal in de meeste gevallen bepalen welke data wordt gebruikt als studiedata, voor welk doel studiedata wordt gebruikt en op welke wijze. De eindgebruiker is daarmee bij uitstek degene die moet borgen dat studiedata op verantwoorde wijze wordt benut. Om een eindgebruiker hierbij te helpen, kan een instelling bijvoorbeeld het doen van een (privacy) checklist verplicht stellen voordat studiedata gebruikt mag worden. Deze checklist dwingt de eindgebruiker dan om goed na te denken over de aan privacy en ethiek gerelateerde aspecten.

5.2.2 Functionaris voor Gegevensbescherming

Hoger onderwijsinstellingen zijn verplicht om een Functionaris voor Gegevensbescherming (FG) aan te stellen.[11] De taken van de FG zijn intern toezichthouden op de naleving van de wet- en regelgeving op het gebied van de bescherming van persoonsgegevens en adviseren over de verplichtingen die voortvloeien uit de (U)AVG.

[11] Een FG moet namelijk aangesteld worden ingevolge artikel 37 AVG als de verwerkingsverantwoordelijke een overheidsinstantie of -orgaan betreft, als de verwerkingsverantwoordelijke hoofdzakelijk is belast met verwerkingen die vanwege de aard en de omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen, of als de verwerkingsverantwoordelijke hoofdzakelijk is belast met grootschalige verwerking van bijzondere persoonsgegevens.

Om te borgen dat de FG haar taken adequaat kan uitvoeren, heeft zij een onafhankelijke positie. Dit betekent dat zij geen instructies mag ontvangen over het uitvoeren van de werkzaamheden. De instelling moet er voorts voor zorgen dat de FG voldoende middelen heeft om haar functie uit te oefenen en medewerking krijgt van de instelling om haar taken uit te oefenen. Om te voorkomen dat de FG als een 'slager zijn eigen vlees gaat keuren', neemt een FG geen beslissingen over het verwerken van persoonsgegevens binnen de instelling.

De FG heeft daardoor geen directe verantwoordelijkheid voor het verwerken van persoonsgegevens, maar heeft wel een verantwoordelijkheid om (gevraagd en ongevraagd) advies te geven over verwerkingen van persoonsgegevens en toe te zien op de verwerkingen van persoonsgegevens in de zin van naleving van wet- en regelgeving. Ook kan zij controlerend acteren indien zij situaties treft waarin bewust of onbewust de regels niet of niet volledig worden nageleefd.

De rol van de FG is dus vooral adviserend en controlerend en zij brengt verslag uit aan het hoogste management, dat in de regel (een lid van) het College van Bestuur zal zijn en indien nodig de Raad van Toezicht. Tevens is de FG het contactpunt voor de nationale toezichthouder, de Autoriteit Persoonsgegevens, en moeten betrokkenen altijd contact kunnen opnemen met de FG.

5.2.3 Privacyfunctionaris (Privacy Officer, Privacyjurist, Privacycontactpersoon)

Veel instellingen zullen binnen de faculteiten en diensten een aangewezen privacyfunctionaris hebben die de collega's binnen die faculteit of dienst kan helpen bij vragen over het verwerken van persoonsgegevens of privacy. Aangezien deze functie in de faculteit of dienst is belegd, kent de functionaris de materie waar haar collega's mee werken en kan zij in veel gevallen praktische hulp bieden ten aanzien van een specifieke privacyvraag.

Naast een privacyfunctionaris binnen de dienst of faculteit zal er vaak ook centraal een privacyfunctionaris of -team zijn, denk dan aan een centraal *privacy office* of een of meer privacy juristen. Zij kunnen worden betrokken bij complexere of dienst- of faculteitsoverstijgende privacyvraagstukken. Ook hiervoor geldt dat het aan de instelling zelf is om te bepalen of er een bepaalde verantwoordelijkheid wordt toebedeeld aan deze centrale privacyfunctionaris of -jurist.

Het moet voorkomen worden dat de privacyfunctionarissen slechts een 'verplicht loket' worden om een stempel te halen om verder te kunnen met het gebruik van studiedata. De meerwaarde van deze functionarissen is dat ze de eindgebruiker en andere partijen in de instelling kunnen adviseren en ondersteunen om de juiste afwegingen te maken ten aanzien van het gebruik van studiedata.

5.2.4 (Medisch) Ethische Toetsingscommissie

Met de inwerkingtreding van de Wet medisch-wetenschappelijk onderzoek met mensen (WMO) is het verplicht geworden om voor mens-gebonden medisch-wetenschappelijk onderzoek het onderzoek te laten goedkeuren door een erkende medisch ethische toetsingscommissie (METC). De meeste instellingen met een academisch medisch centrum hebben een erkende METC, die WMO-plichtige onderzoeken moeten goedkeuren. Wanneer niet WMO-plichtige medische onderzoeken worden gedaan, kan het ook zijn dat er (niettemin) goedkeuring van de METC nodig is of dat de METC de verklaring afgeeft dat het onderzoek inderdaad niet WMO-plichtig is.

In de praktijk zal het niet snel voorkomen dat benutting van studiedata valt onder medisch-wetenschappelijk onderzoek. Wanneer studiedata echter wordt gebruikt voor wetenschappelijk onderzoek kan op voorhand niet worden uitgesloten dat het onder omstandigheden toch als een medisch-wetenschappelijk onderzoek wordt aangemerkt. Daarom wordt de METC wel benoemd in dit Referentiekader.

Relevanter is wellicht de trend van de laatste jaren waarbij instellingen niet wettelijk verplichte of erkende ethische toetsingscommissies oprichten. Dit kan gebeuren door de instelling als geheel of door (niet-medische) faculteiten binnen een instelling. Dit gebeurt vaak bij faculteiten waar veel met persoonsgegevens dan wel met proefpersonen wordt gewerkt, bijvoorbeeld bij economische of sociale wetenschappen. Onderzoekers binnen de instelling of betreffende faculteit moeten dan de onderzoeksvoorstellen voorleggen aan deze ethische toetsingscommissie voor advies dan wel goedkeuring.

Ook hiervoor geldt dat dergelijke ethische toetsingscommissies zijn ingericht voor het toetsen van een voorstel voor het doen van wetenschappelijk onderzoek. Wanneer studiedata voor wetenschappelijk onderzoek wordt gebruikt, kan het dus zijn dat dit onderzoek moet worden goedgekeurd door een ethische toetsingscommissie.

Praktijkvoorbeeld: Ethische Toetsingscommissie

Het kan het verantwoorde gebruik van studiedata ten goede komen als onderzoekers die wetenschappelijk onderzoek willen doen met gebruikmaking van studiedata verplicht worden om hun onderzoeksvoorstel voor te leggen aan een Ethische Toetsingscommissie. Dit kan zowel een facultaire als een faculteitsoverstijgende commissie zijn. Zorg er daarbij ook voor dat er voldoende privacy-kennis aanwezig is in deze Ethische Toetsingscommissie.

De Universiteit van Amsterdam heeft bijvoorbeeld bij vijf faculteiten een Ethische Toetsingscommissie, waar onderzoeksvoorstellen aan moeten worden voorgelegd als aan bepaalde criteria wordt voldaan.

De Erasmus Universiteit van Rotterdam heeft een Privacy & Ethics Board ingericht, die voorstellen voor pilots en projecten met studiedata toetst en de voortgang daarvan monitort. In deze Board zitten een lid van de ethische commissie, een student, een docent, een onderzoeker, een beleidsmedewerker, een *data scientist* en de FG.

5.2.5 Het studiedata-team

Vaak zal er binnen een instelling een functionaris of team zijn dat voorziet in het gebruik van studiedata. Dit kan op verschillende manieren, bijvoorbeeld door de data voor te bereiden en zodanig te structureren dat het gebruikt kan worden voor analyses.

Deze functionaris of dit team moet er verder voor zorgen dat het systeem naar behoren werkt, bijvoorbeeld door hiervoor de (technische) tools te (laten) bouwen en beheren. Dit zal ook inhouden te zorgen dat de bronbestanden benaderd kunnen worden op een veilige en betrouwbare manier.

Tot slot zal de functionaris of het team ook vaak de verzoeken om gebruik van studiedata van de eindgebruikers uitvoeren. Daarbij kunnen ze de voorwaarden aangeven waaronder een eindgebruiker studiedata kan gebruiken en zorgen dat hieraan wordt voldaan.

5.2.6 (Chief) Information Security Officer

De (C)ISO ondersteunt een organisatie op het gebied van informatiebeveiliging en heeft kennis over de mogelijke technische en organisatorische beveiligingsmaatregelen die kunnen worden getroffen. De (C)ISO is echter niet verantwoordelijk voor het treffen van de juiste maatregelen, dit is aan de functionaris(sen) die besluiten over het gebruik van bepaalde data dan wel bepaalde systemen.

De (C)ISO kan wel helpen bij het leggen van de juiste relatie tussen dreigingen en risico's en de mogelijke beheer- en beveiligingsmaatregelen die in een specifieke situatie passend zijn. Echter, het blijft aan de verantwoordelijke functionaris om binnen zijn eigen kader de maatregelen al dan niet te treffen.[12]

[12] Handreiking IB profiel CISO van de VNG.

Tot slot helpt de (C)ISO bij het vergroten van het informatiebewustzijn onder medewerkers, al dan niet in samenwerking met andere functionarissen, zoals de FG.

5.3 Wijze van bepalen en vastleggen verantwoordelijkheden

Zoals in het begin van dit hoofdstuk opgemerkt, is er, behalve de verplichting om een FG aan te stellen en diens taken en positie, niet nader geregeld op welke manier de interne verantwoordelijkheidsverdeling wordt vormgegeven door instellingen. Om rechtmatig en zorgvuldig, en daarmee dus verantwoord, studiedata te gebruiken is het echter wel belangrijk dat deze verantwoordelijkheidsverdeling wordt gemaakt en vastgelegd.

Hiervoor kan uiteraard een 'gewoon' beleidsdocument worden gebruikt waarin de verschillende betrokken functionarissen worden benoemd en waarbij wordt aangegeven welke taken en verantwoordelijkheden zij hebben binnen de instelling bij het gebruik van studiedata.

Een andere manier waarop dit kan worden gedaan, is door een RA(S)CI- matrix op te stellen. Hierin worden de betrokken functionarissen genoemd en wordt inzichtelijk gemaakt of zij voor een bepaalde verwerking verantwoordelijk (**R**esponsible), toerekenbaar (**A**ccountable) of ondersteunend (**S**upporting) zijn, of moeten worden geraadpleegd (**C**onsulted) of geïnformeerd (**I**nformed).

RACI matrix

De Europese Toezichthouder voor Gegevensbescherming (EDPS) heeft een basale RACI-matrix opgenomen in zijn richtsnoeren over *accountability on the ground*.

	Responsible	Accountable	Consulted	Informed
Top Management		●		
Business owner	●			
DPO			●	
IT department			●	
Processors, where relevant			●	

Bron: Accountability on the ground Part 1 van de EDPS

6 Transparantie en aanspreekbaarheid

De rode draad in alle voorgaande hoofdstukken, evenals in de (U)AVG en andere gedragscodes en normenkaders, is transparantie en aanspreekbaarheid. Transparantie draagt bij aan het vertrouwen in de manier waarop een instelling omgaat met studiedata, het geeft legitimiteit aan het gebruik van studiedata door instellingen en het helpt medewerkers en onderzoekers bij het maken van de juiste keuzes. In hoofdstuk 2 zijn de uitgangspunten van transparantie en aanspreekbaarheid behandeld.

In dit hoofdstuk wordt ingegaan op de meer praktische kant van het transparantievereiste en het aanspreekbaar zijn. In de AVG wordt namelijk wel bepaald welke informatie moet worden gegeven en op welk moment, maar niet de manier waarop dit moet worden gedaan. In dit Referentiekader wordt daarom nader ingegaan op de vraag waarover instellingen moeten informeren, maar ook wanneer dit in het kader van studiedata het meest gepast is en op welke wijze dit het beste kan worden gedaan. Tot slot worden praktische handvatten gegeven over hoe een instelling aanspreekbaar kan zijn.

6.1 Waarover informeren

Een instelling moet allereerst kenbaar maken dat het gebruik maakt van studiedata, op een manier dat dit voor iedereen duidelijk is. Dit kan op verschillende manieren worden bewerkstelligd, bijvoorbeeld door bij inschrijving bij de instelling aan de (aankomend) student in elk geval duidelijk te maken dat de instelling studiedata gebruikt. Dit kan bijvoorbeeld door op de landingspagina op het intranet of de website dit te benoemen of door regulier alle studenten hierover een e-mail te sturen. Het belangrijkste is dat de informatie op een plek en manier wordt gegeven waarvan mag worden aangenomen dat studenten dit lezen.

Overigens is het niet per se noodzakelijk, en vaak ook niet mogelijk, om op dat moment alle informatie te geven over het gebruik van studiedata door de instelling. Daarom kan gebruik worden gemaakt van een gelaagde manier van informeren, waarbij de belangrijkste zaken direct worden vermeld en de nadere informatie eenvoudig via een link naar een andere pagina of een privacyverklaring kan worden geraadpleegd.[13] In paragraaf 6.3. wordt nader ingegaan op het gelaagd geven van informatie.

[13] Zie ook de Richtsnoeren over Transparantie van de Artikel 29 werkgroep, laatstelijk herzien en goedgekeurd op 11 april 2018, vanaf pagina 22.

Wanneer studiedata door een instelling gebruikt gaat worden, moet ook andere informatie over dat gebruik worden gegeven. Het drieluik – Doel, Grondslag, Zorgvuldigheid – uit hoofdstuk 4 geeft ook hierbij de handvatten om de informatie op een gestructureerde manier te geven.

6.1.1 Doel

Een instelling moet op basis van de AVG duidelijkheid geven over de doelen waarvoor studiedata wordt gebruikt. Zoals in hoofdstuk 4 reeds is gesteld, is het van belang om de doelen waarvoor gegevens worden gebruikt zo welbepaald en specifiek mogelijk te formuleren. Vaak zal het echter niet mogelijk zijn om op voorhand al aan te geven voor welke specifieke doeleinden studiedata gebruikt zal worden. Een oplossing hiervoor is dat op een gelaagde manier informatie kan worden verschaft. Dit betekent dat op een hoger niveau in algemene termen kan worden geïnformeerd over het gebruik van studiedata. Bijvoorbeeld dat de instelling heeft besloten dat studiedata alleen zal worden gebruikt om algemene inzichten te krijgen ter verbetering van het onderwijs of onderwijsbeleid of juist dat het alleen wordt gebruikt voor individuele begeleiding van studenten.

Op een lager niveau moeten dan meer details worden gegeven over het specifieke doel van een bepaalde benutting van studiedata. Bijvoorbeeld als een docent voor zijn eigen vak studiedata gaat gebruiken om inzicht te krijgen in de resultaten over tijd van de studenten of het aantal studenten dat zijn vak heeft gevolgd, moet hij hierover transparant zijn. In paragraaf 6.3. wordt nader ingegaan op het gelaagd geven van informatie.

6.1.2 Grondslag

Naast het doel moet ook worden geïnformeerd over de juridische grondslag die van toepassing is op de verwerking van persoonsgegevens. Ook hiervoor geldt dat op een gelaagde manier kan worden geïnformeerd over de grondslag. Op een hoger niveau kan dan worden aangegeven welke grondslagen mogelijk gebruikt worden voor bepaalde toepassingen van studiedata. Op een lager niveau kan dan worden geïnformeerd welke grondslag daadwerkelijk voor een specifieke toepassing wordt gebruikt, bijvoorbeeld dat een instelling als beleid heeft dat individuele interventies alleen maar op basis van toestemming kunnen plaatsvinden.

Indien de juridische grondslag het 'gerechtvaardigd belang' is, moet over de belangenafweging die in dit kader is gemaakt ook worden geïnformeerd.

6.1.3 Zorgvuldigheid

Naast doel en grondslag moet ook over alle andere overwegingen die zijn gemaakt worden geïnformeerd om te borgen dat het gebruik van studiedata verantwoord en behoorlijk gebeurt. Een aantal hiervan wordt specifiek genoemd in de AVG als elementen waar informatie over moet worden gegeven. Dit betreft informatie over:

- Welke persoonsgegevens worden gebruikt;
- Identiteit en contactgegevens van de verwerkingsverantwoordelijke;
- Of de persoonsgegevens worden gedeeld met (een) andere organisatie(s) en zo ja met welke (type) organisatie(s);
- Of de persoonsgegevens worden doorgegeven naar een land buiten de Europese Economische Ruimte of een internationale organisatie en zo ja, welke waarborgen zijn getroffen dat dit op een rechtmatige manier gebeurt;
- Hoe lang de persoonsgegevens worden bewaard en als dat niet kan in elk geval de criteria om de bewaartermijn te bepalen;
- Dat de betrokkene bepaalde rechten heeft (zie hiervoor ook hoofdstuk 7);
- Dat de betrokkene altijd zijn toestemming mag intrekken, als toestemming de juridische grondslag is geweest op basis waarvan de gegevens worden gebruikt;
- Of het wettelijk verplicht is of een contractuele plicht is voor de betrokkene om de gegevens te verstrekken en wat de gevolgen zijn als de gegevens niet worden verstrekt;
- Of er sprake is van geautomatiseerde besluitvorming en zo ja, nuttige informatie over de onderliggende logica hiervan en de verwachte gevolgen (zie hiervoor paragraaf 7.8);
- Als gegevens van een andere bron/verwerkingsverantwoordelijke worden gebruikt, wat de bron dan is;
- De contactgegevens van de Functionaris voor Gegevensbescherming; en
- Dat de betrokkene een klacht mag indienen bij de instelling zelf of bij de Autoriteit Persoonsgegevens.

Doorgaans hebben (hoger beroeps)instellingen deze informatie vastgelegd in een (algemeen) privacystatement.

6.2 Wanneer informeren

Het uitgangspunt is dat de informatie moet worden gegeven ten tijde van de verzameling van de data. Aangezien studiedata vrijwel altijd persoonsgegevens zal betreffen die oorspronkelijk voor een ander doel zijn verzameld, zal in algemene termen over het gebruik van studiedata moeten worden geïnformeerd op alle plekken waar de gegevens direct van de betrokkene worden verzameld (zie ook paragraaf 6.1.). Dit is echter niet voldoende om tegemoet te komen aan alle transparantie-eisen.

Daarom geldt voor het informeren over het specifieke gebruik van studiedata dat dit het beste kan worden gedaan op het moment dat de gegevens daadwerkelijk als studiedata gebruikt gaan worden. Dat zal in de praktijk vaak zijn nadat is bepaald voor welk specifieke

doel studiedata in gezet gaat worden, wat de grondslag is, welke data hiervoor dan gebruikt moeten worden, op welke manier de data wordt gebruikt en welke maatregelen worden getroffen.

Als de informatie niet gegeven kan worden op het moment van analyse, dan moet dit in ieder geval worden gedaan binnen een redelijke termijn, maar uiterlijk binnen een maand, nadat de gegevens als studiedata gebruikt gaan worden.

Praktijkvoorbeeld: informatieverplichting

Een beleidsmedewerker van de rechtenfaculteit wil inzicht krijgen of er verschil is in cijfermatige resultaten van een vak dat in het Engels wordt gegeven en in het Nederlands. Hiervoor wil hij de cijfers van alle studenten van dit vak van de afgelopen twee jaar betrekken, wat in totaal zo'n 2000 studenten zijn. Hij heeft geen andere informatie over de studenten nodig en gebruikt dit dus ook niet.

Ook bij dergelijk weinig invasieve toepassing van studiedata moet worden voldaan aan de informatieverplichting. Minimaal moet dit mogelijke gebruik worden opgenomen in een algemene privacy verklaring.

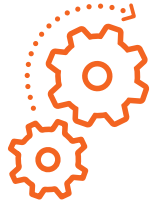
Als het gebruik van studiedata ertoe leidt dat direct contact met de betrokkene wordt opgenomen, bijvoorbeeld bij individuele interventies voor het studiesucces bij een student, moet uiterlijk op het moment van contact worden geïnformeerd over het feit dat studiedata wordt gebruikt.

Praktijkvoorbeeld: studiebegeleiding

Een studentbegeleider ziet dat een student een gesprek heeft aangevraagd bij haar omdat de student tegen problemen aanloopt bij het studeren. Om zich goed voor te bereiden maakt de studentbegeleider gebruik van studiedata om inzicht te krijgen in de ontwikkeling van de student zelf. Hierbij gebruikt ze niet alleen gegevens over cijfers en studiepunten, maar ook informatie over het studiegedrag van de student, bijvoorbeeld op welke momenten hij het meest actief is in het LMS.

De studentbegeleider zal de student bij aanvang van het gesprek moeten informeren over het feit dat ze ook andere informatie dan cijfers en studiepunten heeft opgevraagd. Met het oog op de rechten van de betrokken student (zie ook hoofdstuk 7) moet de student ook in de gelegenheid worden gesteld hierop zijn reactie te geven.

Tot slot, als wordt overwogen om studiedata aan een andere instelling of andere organisatie door te gegeven en de betrokkene(n) zijn nog niet geïnformeerd, dan moet op dat moment hierover worden geïnformeerd.



Praktijkvoorbeeld: delen van data

Een andere instelling vraagt aan hogeschool X om studiedata over het aantal instromers van de middelbare school met het profiel Economie & Maatschappij en er wordt overwogen dit te verstrekken aan die instelling.

Wanneer het herleidbare data van studenten betreft, zal hogeschool X de betreffende studenten hierover voorafgaand moeten informeren. Afhankelijk van hoeveel studenten dit betreft en wat voor soort studiedata , kan dit door een algemene e-mail aan deze studenten of door een algemeen bericht te plaatsen op de (faculteits)webpagina, intranet of nieuwsbrief.

6.2.1 Uitzonderingen

Het is niet noodzakelijk om de informatie te verstrekken als de instelling de betrokkene al heeft geïnformeerd, als het ontvangen of verstrekken van de gegevens uitdrukkelijk door een Europese of Nederlandse wet is voorgeschreven of als de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim of wettelijke geheimhoudingsplicht.

Ook hoeft de in paragraaf 6.1. genoemde informatie niet te worden verstrekt als het onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder wanneer de verdere verwerking voor historisch of wetenschappelijk onderzoek plaatsvindt, of als het behalen van doeleinden hierdoor onmogelijk wordt of ernstig in het gedrang komt. Deze uitzondering moet echter strikt worden uitgelegd. Dit betekent bijvoorbeeld dat wanneer er wel e-mailadressen bekend zijn het niet meer onmogelijk is of onevenredige inspanning kost om de betrokkenen te informeren. Tevens moeten wel passende maatregelen worden genomen om de rechten en belangen van betrokkenen te beschermen.

6.3 Hoe informeren

Zoals meerdere keren aangegeven in dit hoofdstuk hoeft niet alle informatie in één keer te worden gegeven. Dit mag ook op een gelaagde manier worden gedaan, bijvoorbeeld door de zeer algemene informatie te geven op het moment dat gegevens worden verzameld van de betrokkenen, zoals bij de inschrijving. Ook is het goed om dergelijke algemene informatie altijd beschikbaar te maken voor de betrokkenen, bijvoorbeeld op de landingspagina van de website of het intranet. Eventueel kan ook jaarlijks een mailing worden uitgestuurd met de meest relevante informatie.

In de algemene melding kan dan worden verwezen naar een algemene privacyverklaring, waar nadere informatie staat over de wijze waarop persoonsgegevens door de instelling worden gebruikt. Van een dergelijke privacyverklaring kan een deel worden gewijd aan het gebruik van studiedata.

In aanvulling op een algemene privacyverklaring is het ook te overwegen om een privacyverklaring op te stellen specifiek voor het gebruik van studiedata door de instelling. Hierin kan de instelling dan de eigen keuzes en overwegingen opnemen waarvoor binnen de instelling studiedata gebruikt kan en mag worden.

Tot slot, de overwegingen ten aanzien van een specifieke toepassing van studiedata en alle relevante informatie in dat kader kunnen worden gepubliceerd door bijvoorbeeld per faculteit of dienst een (web)pagina beschikbaar te stellen of door op de site van het betreffende onderzoek de vereiste informatie te geven.

Praktijkvoorbeeld: studiedata dashboard

Communiceer op een zo proactief mogelijke manier, bijvoorbeeld met een *studiedata dashboard*, over welke gegevens van studenten worden gebruikt voor welke soorten toepassingen van studiedata.

6.4 Register van verwerkingen

Alle instellingen moeten volgens de AVG een register bijhouden van de verwerkingen van persoonsgegevens die binnen hun organisatie plaatsvinden. Dit register hoeft niet openbaar te worden gemaakt, maar moet desgevraagd wel voor de FG alsook voor de nationale toezichthouder beschikbaar zijn. De volgende gegevens moeten in ieder geval in dit register staan:

- De naam en contactgegevens van de organisatie en van de FG
- Per verwerking:
  - Het verwerkingsdoel
  - Een beschrijving van de categorieën persoonsgegevens en de categorieën betrokkenen
  - De categorieën ontvangers en of de persoonsgegevens, die aan ontvangers buiten de EU worden verstrekt (in dat geval ook de waarborgen die zijn getroffen voor de bescherming van de gegevens)
  - De bewaartermijnen (indien mogelijk)
  - De technische en organisatorische beveiligingsmaatregelen

Er is geen vormvereiste verbonden aan het register van verwerkingen. Voor kleine organisaties zal een excel-bestand een oplossing kunnen zijn, terwijl grotere organisaties meer baat hebben bij een (online) systeem.

De verwerkingen van persoonsgegevens in het kader van studiedata zullen ook in het register van verwerkingen opgenomen moeten worden. De instelling zal het daarom mogelijk moeten maken dat de verwerking in het register kan worden ingevoerd. De wijze waarop dit het beste kan gebeuren, zal per instelling verschillen, omdat het ook afhangt van wie hiervoor intern verantwoordelijk is en op welke wijze het register wordt bijgehouden.

Voorbeeld: register van verwerkingen

De Autoriteit Persoonsgegevens heeft diens register van verwerkingen op hun website gepubliceerd: www.autoriteitpersoonsgegevens.nl

6.5 Aanspreekbaarheid

Zoals in hoofdstuk 2 toegelicht betekent aanspreekbaarheid verantwoordelijkheid nemen. Dit kan een instelling doen door zowel zorgvuldige afwegingen te maken bij conflicterende belangen of uitgangspunten als ook door inzichtelijk te maken wie binnen de organisatie hiervoor verantwoordelijk en aanspreekbaar is. Tevens doet een instelling dit door rekenschap te geven van het feit dat studiedata altijd in een bepaalde maatschappelijke context wordt gebruikt.

Instellingen kunnen zowel *top-down* als *bottom-up* hier nadere invulling aan geven:

- *Top-down*: Instellingen stellen duidelijke processen vast rond het gebruik van studiedata en handelen hier aantoonbaar naar. Hierdoor wordt rekenschap gegeven en verantwoording afgelegd over de afwegingen die zijn gemaakt.

- Instellingen moeten allereerst de afweging maken of een bepaald doel past bij de kernwaarden en maatschappelijke rol van de instelling.
- Daarnaast documenteren instellingen voor alle betrokkenen wat er met welke studiedata wordt gedaan en om welke redenen.
- Deze afwegingen zijn uitlegbaar en toegankelijk voor de betrokkenen.
- Instellingen moeten blijvend toetsen of het nagestreefde doel is bereikt en of aanpassing nodig is (Plan – Do – Check – Act- cyclus).

- *Bottom-up*: Alle betrokkenen moeten kunnen rekenen op de professionaliteit van de medewerkers die met studiedata werken. Deze medewerkers nemen verantwoordelijkheid voor hun handelen en zijn daarop aanspreekbaar. Ook spreken zij – indien nodig – anderen hierop aan.
  - De ethische alsook de juridische afwegingen zijn onderdeel van de dagelijkse praktijk voor iedereen die met studiedata werkt. Het gaat immers om de dagelijkse beslissingen op de werkvloer, waar continu de vraag moet worden gesteld wat ethisch en juridisch verantwoord is en waarbij hierover met elkaar kan worden gesproken.
  - Instellingen kunnen deze dagelijkse praktijk bevorderen door het gesprek over privacy en ethiek onderdeel van het dagelijkse werk te maken. Daarbij is het belangrijk dat de medewerkers die met studiedata werken geen onnodige externe druk ervaren door competitie, werkdruk, prestatiedruk, hiërarchie of regulering.
  - Instellingen maken waar mogelijk en relevant gebruik van een participatief proces door studenten en andere betrokkenen te betrekken bij de ontwikkeling en besluitvorming, bijvoorbeeld bij het introduceren van nieuwe technieken of toepassingen voor het gebruik van studiedata.

7 Rechten van betrokkenen

Zoals in hoofdstuk 4 is uiteengezet, zijn de betrokkenen in het geval van studiedata studenten, aankomend studenten, oud-studenten, docenten, begeleiders en alle andere personen van wie persoonsgegevens worden verwerkt door hoger onderwijsinstellingen. Deze betrokkenen hebben verschillende rechten ten aanzien van hun persoonsgegevens. Instellingen moeten hierin voorzien, ook ten aanzien van het gebruik van studiedata.

Hieronder worden de verschillende rechten van betrokkenen genoemd en wordt uitgewerkt hoe dit in het kader van dit referentiekader kan worden ingevuld.

7.1 Algemeen

Organisaties zijn verplicht het uitoefenen van de rechten door betrokkenen te faciliteren. Dit betekent dat de instelling geen onnodige drempels mag opwerpen voor betrokkenen om hun rechten uit te oefenen en dit niet onnodig mag bemoeilijken.

Daarnaast geldt dat de instelling alle informatie moet geven in begrijpelijke taal en op een makkelijk toegankelijke wijze. Binnen een maand na ontvangst van het verzoek ter uitoefening van een van de rechten van betrokkenen moet hierop worden geantwoord. Als het vanwege de complexiteit van het verzoek nodig is, mag de termijn worden verlengd met maximaal nog een maand. Hierover moet dan wel binnen de eerste maand worden geïnformeerd.

Er is niet bij wet vastgelegd op welke wijze de rechten door betrokkenen kunnen worden uitgeoefend, noch op welke wijze organisaties het uitoefenen ervan moeten faciliteren. Het is aan alle instellingen om hier zelf nader en op passende wijze invulling aan te geven.

In dit Referentiekader

Een voorbeeld van een manier waarop erin kan worden voorzien dat betrokkenen hun rechten kunnen uitoefenen, is via een *self-service-portal*. Via dit portaal kunnen de betrokkenen de gegevens die een instelling van hen heeft tot op zekere hoogte inzien (recht op inzage), kunnen gegevens worden aangepast, bijvoorbeeld een adreswijziging of wijziging in telefoon- of rekeningnummer (recht op rectificatie), en kunnen mogelijk ook niet relevante gegevens verwijderd worden (recht op verwijdering). Voor studenten en medewerkers van een instelling zal dit vaak op een of andere manier al zijn voorzien.

Een *self-service-portal* zal echter niet altijd afdoende zijn om informatie te geven over alle persoonsgegevens die een instelling heeft en alle verwerkingen die een instelling verricht, waaronder het gebruik als studiedata. Ook is dit niet per se voor alle betrokkenen toegankelijk, denk dan aan oud-studenten of andere personen zoals gastdocenten van wie ook persoonsgegevens worden verwerkt die gebruikt worden als studiedata. Vaak is het daarom noodzakelijk om aanvullende voorzieningen te treffen om te voldoen aan het vereiste om het uitoefenen van de rechten van betrokkenen te faciliteren, bijvoorbeeld door een webformulier in te richten via welke betrokkenen hun vragen of verzoeken kunnen indienen of een e-mailadres beschikbaar te stellen waar verzoeken aan gericht kunnen worden.

Het bieden van een webformulier of een specifiek e-mailadres waar verzoeken aan gericht kunnen worden, komt tegemoet aan het faciliteren van de rechten van betrokkenen. Het is echter altijd mogelijk dat een verzoek op een andere manier wordt ingediend en ontvangen. Ook in die gevallen zal het als een verzoek ter uitoefening van de rechten moeten worden aangemerkt en moeten worden beantwoord in overeenstemming met de hierop van toepassing zijnde regels.

7.2 Recht op inzage

Betrokkenen hebben het recht om te weten te komen of persoonsgegevens over hen worden verwerkt en indien dat zo is om inzage te krijgen in deze persoonsgegevens. Uit de rechtspraak blijkt dat het belangrijkste doel van het recht op inzage is om te weten te komen welke persoonsgegevens van iemand worden verwerkt en om vervolgens de rechtmatigheid van die verwerking te kunnen controleren.

Er is tevens een recht op een kopie van de persoonsgegevens. Hierbij is van belang op te merken dat het niet per se gaat om een recht op kopieën van de documenten, maar van de persoonsgegevens. Als de rechten en vrijheden van derden worden geraakt wanneer een kopie van een document zou worden verstrekt, dan is het niet nodig die te verstrekken of kan dergelijke informatie worden weggelakt. Ook kan de betrokkene worden gevraagd om zijn of haar verzoek te specificeren.

In dit Referentiekader

Het recht op inzage zal over het algemeen door een daartoe aangewezen functionaris worden afgehandeld binnen de instelling. Dit kan bijvoorbeeld een privacyjurist of een andere (privacy)functionaris binnen een instelling, dienst of faculteit zijn. Een verzoek om inzage kan echter op alle plekken en in allerlei vormen binnenkomen. Indien het verzoek om inzage wordt ontvangen door een functionaris die betrokken is bij het gebruik van studiedata is het belangrijk eerst afstemming te zoeken met de functionaris die normaliter inzageverzoeken behandelt.

Een instelling kan vervolgens besluiten om na te vragen bij de betrokkene of het inzageverzoek is bedoeld voor alle gegevens binnen de instelling of dat het beperkt is tot inzage in de persoonsgegevens ten aanzien van het specifieke gebruik van studiedata. Op het moment dat iemand inzage vraagt in het gebruik van zijn gegevens voor studiedata zal de relevante informatie hierover moeten worden verstrekt. Met name daar waar studiedata gebruikt wordt voor individuele interventies of in elk geval voor niet-algemene toepassingen zal inzage moeten worden gegeven in de persoonsgegevens die zijn gebruikt voor die specifieke toepassing(en).

7.3 Recht op correctie

In aanvulling op de verplichting dat organisaties moeten zorgen dat de gegevens die ze gebruiken juist zijn (zie paragraaf 4.3.), hebben betrokkenen het recht op correctie. Dit betekent dat zij correctie kunnen vragen van onjuiste gegevens. Dit is geen absoluut recht, er mag worden geverifieerd of de correctie daadwerkelijk een correctie is. Waar het toepasselijk is, kan dit recht ook uitgeoefend worden door een aanvullende verklaring op te nemen. Dit laatste zal met name gebeuren waar het subjectieve beoordelingen over een persoon betreft en de beoordelaar de oorspronkelijke beoordeling juist acht maar de betrokkene hier zelf een andere mening is toegedaan.

In dit Referentiekader

De gegevens die worden gebruikt als studiedata zijn vrijwel allemaal oorspronkelijk voor een ander doel verzameld door de instelling. Enige correctie van onjuiste gegevens zal dan ook veelal bij de bronbestanden moeten gebeuren. Voor zover het subjectieve gegevens betreft, is het bij het gebruik van studiedata van belang om in de gaten te houden dat hierop ook het recht op correctie kan worden uitgeoefend.

7.4 Recht op verwijdering

Een betrokkene kan verzoeken om verwijdering van diens persoonsgegevens. Dit is echter geen absoluut recht. Het recht geldt slechts in de situaties zoals die bij wet zijn voorgeschreven, bijvoorbeeld als de gegevens niet langer nodig zijn, de toestemming wordt ingetrokken (als toestemming de grondslag was) of de gegevens onrechtmatig zijn verwerkt, maar ook als iemand bezwaar heeft gemaakt tegen de verwerking en de organisatie geen prevalerende dwingende gerechtvaardigde gronden heeft om de gegevens te gebruiken.

In dit Referentiekader

Het recht op verwijdering is apart van toepassing op het gebruik van gegevens als studiedata. Een betrokkene kan dus in principe verwijdering vragen van diens gegevens uit de set van gegevens die voor studiedata worden gebruikt, zonder ook om verwijdering van diens gegevens uit de bronbestanden te eisen. Als het wel voor beide wordt gevraagd, moeten in principe beide verzoeken apart worden behandeld.

Praktijkvoorbeeld: recht op verwijdering

Een student heeft met een studieloopbaanbegeleider zijn leerbeperking besproken, maar wil deze niet officieel laten registreren in het systeem van de instelling. Het feit dat dit in het verslag van het SLB-gesprek staat, vindt de student geen probleem, maar zodra hij erachter komt dat het ook voor een studentadviseur bekend is door gebruik van studiedata kan hij daarvan wel verwijdering vragen.

Of een verzoek om verwijdering moet worden gehonoreerd is overigens afhankelijk van de omstandigheden van de verwerking en het verzoek. Indien toestemming de grondslag was voor de verwerking van studiedata zal de intrekking van toestemming ertoe kunnen leiden dat de gegevens verwijderd moeten worden. Als de grondslag is dat het noodzakelijk is voor een taak in algemeen belang of voor het behalen van het gerechtvaardigde belang van de instelling zal moeten worden beoordeeld of er geen prevalerende dwingende gerechtvaardigde gronden meer zijn voor de instelling om de gegevens toch nog te gebruiken als studiedata. Deze afweging zal per geval moeten worden gemaakt.

Wanneer studiedata wordt verwerkt voor wetenschappelijk of historisch onderzoek kan een verzoek om verwijdering worden geweigerd voor zover de verwijdering de verwezenlijking van de doeleinden van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.

7.5 Recht van bezwaar

Betrokkenen hebben het recht van bezwaar tegen het verwerken van hun persoonsgegevens. Dit moeten dan wel verwerkingen betreffen die zijn gebaseerd op de grondslag dat het ‘noodzakelijk is voor een taak in algemeen belang’ of ‘noodzakelijk voor de gerechtvaardigde belangen van de instelling’. Een hoger onderwijsinstelling moet de verwerking van de persoonsgegevens staken tenzij zij dwingende gerechtvaardigde gronden heeft die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband

houden met de instelling, uitoefening of onderbouwing van een rechtsvordering. Een hoger onderwijsinstelling moet in die gevallen zelf een afweging maken.

In dit Referentiekader

Aangezien de meeste verwerkingen van studiedata zullen plaatsvinden op basis van een van de genoemde grondslagen zullen betrokkenen hun recht van bezwaar uit kunnen oefenen. Wanneer een betrokkene bezwaar maakt tegen het gebruik van zijn gegevens als studiedata zal hier gehoor aan moeten worden gegeven, tenzij de instelling van oordeel is dat het dwingende gerechtvaardigde belangen heeft om de gegevens niettemin te verwerken.

Wanneer studiedata wordt gebruikt voor wetenschappelijk of historisch onderzoek heeft de betrokkene ook het recht om bezwaar te maken en moet dit worden gehonoreerd, tenzij het noodzakelijk is voor een taak in algemeen belang om de gegevens toch te (blijven) verwerken.

7.6 Recht op beperking van verwerking

Een betrokkene mag onder bepaalde omstandigheden verzoeken om beperking van het verwerken van zijn persoonsgegevens. Dit mag bijvoorbeeld als:

- de juistheid van de gegevens wordt betwist en de instelling dit controleert; of
- de verwerking onrechtmatig was maar de betrokkene niet wil dat gegevens worden verwijderd; of
- de instelling de gegevens niet meer nodig heeft maar de betrokkene in verband met een rechtsvordering niet wil dat de gegevens worden verwijderd; of
- de betrokkene bezwaar heeft gemaakt en er wordt beoordeeld of de gerechtvaardigde gronden van de instelling zwaarder zouden wegen.

In dit Referentiekader

In de praktijk wordt dit recht slechts heel weinig uitgeoefend. Indien er echter een beperking geldt voor het verwerken van gegevens, bijvoorbeeld omdat de juistheid wordt betwist of wordt onderzocht of de gegevens verwijderd moeten worden, betekent het dat de gegevens niet verder verwerkt mogen worden als studiedata. De instelling moet er daarom, indien een betrokkene het recht op beperking heeft uitgeoefend, voor zorgen dat dit ook wordt gehonoreerd door de gegevens niet meer beschikbaar te stellen voor studiedata-doeleinden.

7.7 Recht op gegevensoverdraagbaarheid

Een betrokkene mag verzoeken om de persoonsgegevens die een instelling van hem heeft in een gestructureerde, gangbare en machine-leesbare vorm te krijgen en om deze vervolgens aan een andere organisatie, bijvoorbeeld een andere instelling, over te dragen, zonder daarbij gehinderd te worden. Wanneer het mogelijk is, heeft de betrokkene zelfs het recht om de instelling te vragen de gegevens rechtstreeks door te geven aan een andere organisatie.

Een betrokkene kan dit recht overigens alleen uitoefenen ten aanzien van gegevens die worden verwerkt op basis van de grondslag van toestemming of wanneer het noodzakelijk is voor de uitvoering van een contract en de verwerking geautomatiseerd gebeurt.

In dit Referentiekader

Met name wanneer studiedata wordt gebruikt voor individuele interventies en de toegepaste grondslag toestemming is, kan de betrokkene het recht op gegevensoverdraagbaarheid uitoefenen, bijvoorbeeld door de uitkomst te delen met een andere instelling of organisatie.

7.8 Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming

Het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming zou ook gelezen kunnen worden als een plicht van organisaties om geen automatische besluiten, waaronder profilering, te nemen als aan dit besluit rechtsgevolgen zijn verbonden of dit anderszins de betrokkene aanmerkelijk treft. Dit betekent dat analyses die worden gemaakt van mensen of groepen mensen ten behoeve van besluitvorming die individuen kan treffen nooit volledig automatisch mogen gebeuren.

Er is een aantal uitzonderingen op dit verbod, bijvoorbeeld als de geautomatiseerde besluitvorming noodzakelijk is voor het aangaan van een contract (denk dan aan het afsluiten van een hypotheek) of als de betrokkene uitdrukkelijke toestemming heeft gegeven. In die gevallen moeten maatregelen worden getroffen, zoals het recht op menselijke tussenkomst, het recht voor de betrokkene om zijn standpunt kenbaar te maken en het recht om een besluit aan te vechten.

In dit Referentiekader

Wanneer studiedata gebruikt gaat worden ten behoeve van de besluitvorming en deze besluiten rechtsgevolgen hebben voor een of meer individuen of hen anderszins significant raakt, dan mag dit dus niet volledig geautomatiseerd gebeuren. De instelling zal dan op z'n minst moeten voorzien in de mogelijkheid van menselijke tussenkomst en het recht voor de betrokkene om zijn standpunt kenbaar te maken of een besluit aan te vechten. Met name ten aanzien van het monitoren of volgen van studenten ten aanzien van hun voortgang is het van belang dat hieruit voorvloeiende rechtsgevolgen of gevolgen die de student anderszins aanmerkelijk treffen hiervan niet volledig geautomatiseerd plaatsvinden. Het hebben van een '*human in the loop*' en menselijke tussenkomst wordt in paragraaf 2.2.4 nader toegelicht. Een belangrijk onderdeel hiervan is dat bij het inzetten van automatisering alsook bij de mogelijke gevolgen ervan de menselijke maat belangrijk is.

7.8.1 Kunstmatige Intelligentie

De opkomst van Kunstmatige Intelligente (*Artificial Intelligence* of *AI*) is een belangrijke ontwikkeling die met name in het licht van geautomatiseerde besluitvorming vaak opkomt maar veel meer beslaat. In toenemende mate wordt kunstmatige intelligentie ingezet voor het analyseren van data. Er zijn verschillende vormen van kunstmatige intelligentie, van relatief simpele algoritmes tot zeer complexe zogeheten zelflerende algoritmes. Welke vorm het meest passend is, zal afhangen van het doel waarvoor het algoritme gebruikt wordt en welke uitkomst(en) ermee bereikt moeten worden.

Als een instelling kunstmatige intelligentie inzet bij het gebruik van studiedata, ongeacht hoe geavanceerd het algoritme is, blijft de instelling verantwoordelijk voor het verantwoord gebruik van studiedata. Dit betekent dus dat alle verplichtingen en vereisten zoals die onder andere in dit Referentiekader worden beschreven onverkort van toepassing zijn, waaronder het drieluik uit hoofdstuk 4.

De instelling moet allereerst bepalen waarom het nodig is om het algoritme te gebruiken. Vervolgens moet bepaald worden en kunnen worden verantwoord wat het doel is van de verwerking door het algoritme, wat de grondslag is en hoe wordt voldaan aan de zorgvuldigheidseisen. Ook de transparantieverplichting is volledig van toepassing. Een instelling moet dus onder andere verantwoorden welke data door het algoritme wordt gebruikt, wat het algoritme daarmee doet, wat de verwachte uitkomst is en hoe de uitkomst(en) worden gebruikt. Bij gebruik van algoritmes moet, zoals in paragraaf 6.1.3. staat beschreven, immers inzicht worden gegeven in het algoritme of tenminste nuttige informatie worden gegeven over de logica ervan.

Een belangrijke voorwaarde voor het gebruik van algoritmes is voorts dat het algoritme 'eerlijk' is en dat dus kan worden uitgelegd en geborgd dat het niet leidt tot onbehoorlijke uitkomsten. Concreet betekent dit dat vooraf goed moet worden nagedacht over het ontwerp: is het gekozen algoritme passend bij het doel? Is de werking van het algoritme voldoende getest? Zijn de maatregelen en waarborgen passend? Wat gebeurt er als de

algoritmes onbedoeld een verkeerde uitkomst geven?[14]

Zoals in paragraaf 7.8. aangegeven mag het gebruik van kunstmatige intelligentie tot slot nooit leiden tot een geautomatiseerd besluit, waaronder profilering, waaraan rechtsgevolgen of andere significante gevolgen voor de betrokkene(n) kleven. Er moet dan altijd in elk geval worden gezorgd voor menselijke tussenkomst.

[14] Zie ook de website van de AP: autoriteitpersoonsgegevens.nl/nl/nieuws/toezicht-op-algoritmes

8 Overige waarborgen en maatregelen

In de voorgaande hoofdstukken zijn de meest essentiële randvoorwaarden behandeld waar een instelling voldoende aandacht aan moet besteden bij het gebruik van studiedata, te weten de verantwoordelijkheden van de instelling, de interne verantwoordelijkheidsverdeling, de transparantieverplichting en de rechten van betrokkenen.

Naast deze essentiële randvoorwaarden is er nog een aantal andere waarborgen en maatregelen waar een instelling nadere aandacht aan moet besteden. Dit zijn:

- Data Protection Impact Assessments (DPIAs)
- Samenwerken met andere partijen
- Beveiliging en Privacy by Design

8.1 Data Protection Impact Assessments (DPIAs)

Een *Data Protection Impact Assessment* (DPIA), in het Nederlands een gegevensbeschermingseffect-beoordeling (GEB) geheten, is een beoordeling van de impact en de risico's op de privacy of beter gezegd de bescherming van gegevens die verbonden zijn aan een (voorgenomen) gebruik van gegevens. Het is natuurlijk altijd goed om een dergelijke beoordeling te doen, maar in een aantal gevallen is het uitvoeren van een DPIA zelfs verplicht. Als een verwerking waarschijnlijk een hoog risico met zich meebrengt voor de betrokkene(n) moet namelijk altijd een DPIA worden uitgevoerd.

Om te bepalen of een verwerking waarschijnlijk een hoog risico met zich meebrengt, moet worden gekeken naar de aard, de omvang, de context en de doeleinden van de verwerking. Er is (gelukkig) al veel nadere invulling gegeven aan wat moet worden verstaan onder een hoog risico en in welke gevallen een DPIA moet worden uitgevoerd. In de volgende gevallen zal volgens de AVG in feite altijd 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 (zie in dit kader ook paragraaf 7.8.).
- Als op grote schaal bijzondere persoonsgegevens worden verwerkt.
- Als op een stelselmatige of grootschalige wijze openbare ruimten worden gemonitord.

In aanvulling op bovenstaande gevallen hebben de Europese privacy-autoriteiten gezamenlijk een lijst van negen criteria opgesteld om te beoordelen of er sprake is van een hoog risico. Denk dan aan criteria als geautomatiseerde besluitvorming (die niet per definitie

leidt tot een besluit met (rechts)gevolgen), bijzondere persoonsgegevens (niet per definitie op grote schaal) en grootschalige verwerking (niet per definitie van bijzondere persoonsgegevens). Als aan twee van de negen criteria wordt voldaan, kan ervan uit worden gegaan dat er waarschijnlijk sprake is van een hoog risico.[15]

Daarnaast hebben alle nationale toezichthouders eigen lijsten opgesteld van situaties waarin een DPIA moet worden uitgevoerd. De Nederlandse toezichthouder heeft een lijst van zeventien soorten verwerkingen opgesteld waarvoor een DPIA moet worden gedaan. Hierop staan zaken zoals het doen van heimelijk onderzoek, het aanleggen van zwarte lijsten, profilering en observatie en beïnvloeding van gedrag.[16]

Een DPIA bestaat altijd uit tenminste vier onderdelen. Ten eerste bevat het een beschrijving van de beoogde verwerkingen, de doeleinden en als de grondslag het 'gerechtvaardigd belang' is ook de belangen van de organisatie. Vervolgens moet er een beoordeling worden gemaakt van de noodzakelijkheid en proportionaliteit van het gebruik van gegevens in relatie tot het doel. Ten derde moet er een beoordeling van de risico's worden gemaakt. Tot slot moeten de maatregelen worden benoemd die worden getroffen om de bescherming van persoonsgegevens te garanderen en aan te tonen dat aan de (wettelijke) eisen wordt voldaan.

In dit Referentiekader

Niet voor alle toepassingen van studiedata zal het verplicht zijn om een DPIA te doen. Per specifiek gebruik van studiedata zal dus moeten worden bepaald of een voorgenomen gebruik van studiedata waarschijnlijk een hoog risico met zich mee zal brengen en dus of een DPIA vereist is. Om hiermee te helpen, hebben veel instellingen een zogeheten pre-DPIA of privacy-checklist ontwikkeld, die moet worden ingevuld voordat met een project of een studiedata-toepassing gestart kan worden. In de pre-DPIA of privacy-checklist staan dan de criteria van de Europese toezichthouders en de verwerking uit de lijst van de AP in vraagvorm opgenomen. Door het invullen van een dergelijke pre-DPIA wordt dan duidelijk of een volwaardige DPIA gedaan moet worden of niet.

[15] Zie de EDPB Guidelines on Data Protection Impact Assessments (WP 248)

[16] De lijst van de AP is vastgelegd in het 'Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens' in de Staatscourant Nr 64418 van 27 november 2019.

Tip!

Zorg dat in een pre-DPIA of privacy-checklist in elk geval de velden moeten worden ingevuld die ook in het Register van Verwerkingen (zie paragraaf 6.9.) moeten worden opgenomen. Daarmee kan aan twee eisen tegelijkertijd worden voldaan.

Er zijn geen vormvereisten verbonden aan een DPIA. Dit kan dus worden gedaan op een manier die het best past bij de instelling, zolang de vier hierboven genoemde punten er maar in staan. In de praktijk is het echter handig om uniformiteit aan te brengen in de wijze waarop binnen een instelling een DPIA wordt uitgevoerd. Dit helpt degene(n) die de DPIA uitvoeren om niet zelf het wiel uit te hoeven vinden en voorkomt dat er een wirwar aan templates ontstaat. Het geeft daarnaast zekerheid dat alle vereiste aspecten worden meegenomen in de beoordeling. Tot slot geeft het ook de mogelijkheid om verschillende DPIA's te vergelijken en om te controleren, bijvoorbeeld door de FG, of het op de juiste manier wordt gedaan. Indien er nog geen eigen DPIA-template is ontwikkeld, zijn er veel voorbeelden beschikbaar die gebruikt kunnen worden.

In detail: DPIA

SURF heeft een template-DPIA beschikbaar op hun website: www.surf.nl/algemene-verordening-gegevensbescherming-avg/impact-en-riskassessment?dst=n1478

Wie de DPIA moet invullen, is aan de instelling zelf om te bepalen, ook met het oog op de verantwoordelijkheidsverdeling die gemaakt wordt zoals beschreven in hoofdstuk 4. Vaak zal het de eindgebruiker van studiedata zijn die dit moet doen of er in ieder geval zeer nauw bij betrokken is. Van belang is echter dat er vanuit meerdere disciplines wordt meegedacht en -gekeken, zodat daadwerkelijk alle risico's en maatregelen de revue passeren. In sommige gevallen kan het ook goed zijn om een technisch expert te betrekken, bijvoorbeeld als een nieuwe techniek wordt gebruikt of als de verwerking met algoritmes of kunstmatige intelligentie zal gebeuren.

8.2 Samenwerken met andere partijen

Een samenwerking tussen een of meer organisaties kan verschillende vormen aannemen. Zo kan het zijn dat een of meer partijen gezamenlijk bepalen dat ze voor een bepaald doel gegevens gaan gebruiken, evenals welke gegevens en op welke wijze dit wordt gedaan. In dat geval spreek je van gezamenlijke verantwoordelijken (zie ook paragraaf 3.4.3). De

gezamenlijke verantwoordelijken moeten onderling afspraken maken over wie welke verantwoordelijkheden draagt binnen de samenwerking. Over de essentie van die afspraken moet open worden gecommuniceerd aan de betrokkenen. Ook moet het duidelijk zijn waar betrokkenen terecht kunnen als zij vragen hebben of hun rechten willen uitoefenen.

Het kan echter ook zijn dat een organisatie een andere organisatie inhuurt, bijvoorbeeld voor het leveren van een IT-dienst, waaronder bijvoorbeeld de leverancier van het LMS. Deze andere partij voert de werkzaamheden uit onder regie van de organisatie in kwestie en beslist niet zelf over wat er met de persoonsgegevens mag gebeuren. In dit geval is er sprake van een verwerkersrelatie. In dergelijke gevallen moeten er afspraken worden gemaakt tussen de verantwoordelijke en de verwerker over onder andere de wijze waarop de verwerker de gegevens verwerkt, welke plichten hij heeft jegens de verantwoordelijke en wat er moet gebeuren na afloop van de verwerking. Hiertoe wordt een zogeheten verwerkersovereenkomst afgesloten.

Tot slot kan een samenwerking ook plaatsvinden tussen twee verantwoordelijken, zonder dat zij als gezamenlijke verantwoordelijken optreden. Denk dan bijvoorbeeld aan een organisatie die van een andere organisatie een set gegevens wil gebruiken, terwijl de laatste verder niets te maken heeft met de daadwerkelijke verwerking. In dat geval kunnen er afspraken worden gemaakt over het gebruik van de gegevens, maar is dit niet verplicht.

In detail: Doel – Grondslag – Zorgvuldigheid bij uitwisseling gegevens

Voor alle verwerkingen geldt het drieluik uit hoofdstuk 4!

Bij het verstrekken van gegeven zal daarom een welbepaald doel, een juridische grondslag en de juiste zorgvuldigheidsmaatregelen moeten worden genomen. Dit geldt ook voor iedere ontvangst van gegevens.

Bij een uitwisseling tussen instelling A en instelling B moeten beide instellingen een doel en een grondslag hebben voor zowel de verstrekking als de ontvangst van de gegevens. Als dit ontbreekt, dan is de uitwisseling niet toegestaan.

Wanneer een instelling met een andere partij gaat samenwerken in het kader van het benutten van studiedata moet deze dus bepalen welke vorm de samenwerking aanneemt. Op basis daarvan zullen de juiste afspraken gemaakt moeten worden.

Veel instellingen zullen voor het maken van de afspraken, zoals een verwerkersovereenkomst of een overeenkomst voor gezamenlijke verantwoordelijken, eigen templates hebben die hiervoor gebruikt moeten of kunnen worden. Wanneer er afspraken moeten worden gemaakt, is het zeer aan te raden en wellicht bij sommige instellingen verplicht om een (privacy)jurist te betrekken.

In detail: verwerkersovereenkomst

SURF heeft een template-verwerkersovereenkomst en een template voor gezamenlijke verwerkingsverantwoordelijken beschikbaar op hun website: www.surf.nl/files/2019-04/SURF-Model-Verwerkersovereenkomst-3.0.pdf en www.surf.nl/files/2019-01/model-gezamenlijk-verantwoordelijkenovk-1.0.pdf.

Tip!

Wanneer wordt samengewerkt met een andere organisatie, vergewis je er dan van dat de uitgangspunten voor het gebruik van studiedata van de eigen instelling ook door de andere organisatie worden onderschreven en gerespecteerd.

8.3 Beveiliging en Privacy by Design

Dit referentiekader gaat slechts beperkt in op de beveiliging van gegevens, omdat hier al veel ander materiaal over beschikbaar is. Het is echter wel van belang om te benoemen, omdat het ook vanuit privacy en ethiek oogpunt belangrijk is om passende technische en organisatorische beveiligingsmaatregelen te treffen.

Het algemene uitgangspunt is dat passende technologische en organisatorische beveiligingsmaatregelen moeten worden genomen, waarbij kan worden gedacht aan het pseudonimiseren en versleutelen van gegevens, het garanderen van de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de systemen en het regelmatig testen en evalueren van de genomen maatregelen.

Al bij het bedenken en ontwikkelen van nieuwe toepassingen of technologieën moet aandacht worden besteed aan de beveiligingsmaatregelen die genomen moeten worden. Dit heet ook wel *privacy by design*. Daarnaast moeten ook de instellingen van toepassingen, applicatie en systemen al standaard zo privacy-vriendelijk mogelijk worden ingesteld. Dit heet ook wel *privacy by default*.

In detail: informatiebeveiliging
SURF heeft veel informatie beschikbaar op hun website, waaronder een informatiebeveiligingsbeleid: www.surf.nl/informatiebeveiliging

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

8.3.1 Pseudonimiseren en anonimiseren

De termen pseudonimiseren en anonimiseren worden veel gebruikt in het kader van privacy en de bescherming van persoonsgegevens. Het belangrijkste verschil tussen deze termen is dat pseudonieme gegevens nog steeds persoonsgegevens zijn, terwijl gegevens alleen anonieme gegevens zijn als deze redelijkerwijs door geen enkele partij (meer) herleidbaar zijn tot een individu. Bijvoorbeeld, op juiste wijze geaggregeerde gegevens kunnen voor derden *wel* anoniem zijn.

Het verwijderen van de naam van een persoon of het vervangen van de naam door een nummer betekent dus niet per definitie dat de overgebleven 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 van in elk geval wetenschappelijk (onderwijs)onderzoek, maar ook bij andere vormen van gebruik van studiedata, zal daarom eerder sprake zijn van pseudonieme gegevens dan van volledig anonieme gegevens.

Wanneer persoonsgegevens gepseudonimiseerd zijn, is er nog steeds sprake van persoonsgegevens en moeten de regels worden nageleefd. Pseudonimiseren is echter wel een zogeheten Privacy Enhancing Technique (PET). In het kader van beveiligen van persoonsgegevens heeft het dus zeker toegevoegde waarde. Het risico voor de betrokkenen als er iets misgaat, bijvoorbeeld als de gegevens in verkeerde handen vallen, is namelijk vele malen kleiner als de gegevens zijn gepseudonimiseerd.

In detail: anonimiseren en pseudonimiseren volgens de AP
De Autoriteit Persoonsgegevens (AP) heeft ook veel aandacht besteed aan het onderscheid tussen pseudonimiseren en anonimiseren, zie hiervoor de website van de AP.

De AP heeft bijvoorbeeld in haar aanbevelingen aan gemeenten over het inzetten van technieken in het kader van Smart Cities aangegeven dat bij bepaalde toepassingen – onterecht – wordt gezegd te worden gewerkt met anonieme gegevens. In dat kader benadrukt de AP dat gegevens pas kunnen worden beschouwd als anoniem als het voor welke partij dan ook, met inzet van (voor het doel) redelijke middelen, onwaarschijnlijk is hieruit personen te identificeren. Ook de juiste toepassing van technologie is noodzakelijk om anonimiteit te waarborgen.

9 Afsluiting

Dit Referentiekader bevat de belangrijkste ethische uitgangspunten en juridische (privacy) kaders waar instellingen voldoende aandacht aan moeten besteden bij het verantwoord gebruik van studiedata. Samenvattend zullen hoger onderwijsinstellingen de volgende vier ethische uitgangspunten in acht nemen bij het gebruik van studiedata:

1. Instellingen zijn aanspreekbaar op en transparant over het gebruik van studiedata en leggen daar rekenschap over af.
2. Instellingen maken bij het gebruik van studiedata een eerlijke afweging tussen de belangen van alle betrokkenen.
3. Instellingen zorgen ervoor dat de analyses betrouwbaar en valide zijn.
4. Er is altijd een plek voor de menselijke maat, ook wanneer instellingen gebruik maken van automatische processen.

Daarnaast besteden hoger onderwijsinstellingen bij het gebruik van studiedata aan de volgende vier juridische privacy-onderdelen specifieke aandacht:

1. De interne verantwoordelijkheidsverdeling is voldoende duidelijk bepaald en vastgelegd.
2. Er wordt voldoende transparant gecommuniceerd over het gebruik van studiedata.
3. Betrokkenen worden gefaciliteerd bij het uitoefenen van hun rechten.
4. Instellingen zorgen ervoor dat bij elk gebruik van studiedata;
   a. Het doel duidelijk is bepaald; en
   b. De grondslag helder is; en
   c. De zorgvuldigheidsnormen goed kunnen worden nageleefd.

9.1 Totstandkoming

In het voortraject is vanuit de Zone Studiedata uitgebreid onderzoek gedaan naar de vraag of er behoefte is aan een landelijk kader voor het verantwoord gebruik van studiedata. Er is met verschillende betrokkenen gesproken, vanuit verschillende organisaties op zowel bestuurlijk en beleidsvormend als uitvoerend niveau.

Uit dat onderzoek is gebleken dat de behoefte aan een landelijk kader breed wordt gedeeld. Hierbij zijn ook enkele randvoorwaarden aangegeven, waaronder dat een landelijk kader vooral richtinggevend moet zijn en niet voorschrijvend. Op die manier kan worden geborgd dat instellingen, die verschillen ten aanzien van hun aard, ambitie, mogelijkheden en wensen, op een passende manier studiedata kunnen gebruiken.

In het voorjaar van 2021 is een zogeheten 0.8-versie van het Referentiekader tot stand gekomen door een samenwerking met een groot aantal stakeholders. Zeven experts van verschillende organisaties zijn intensief betrokken geweest bij het schrijfproces, met een gezamenlijke werksessie eind april 2021. Daarnaast is een klankbordgroep van zeventien personen nauw betrokken geweest, door enkelen ervan persoonlijk te interviewen en ze allemaal gedetailleerder op de hoogte te brengen tijdens een informatiesessie begin mei 2021. Beide groepen, evenals een nog bredere groep stakeholders, is een questionnaire gestuurd met het verzoek te reflecteren op de hierin opgenomen uitgangspunten en principes en de scope van het Referentiekader. Dit tezamen heeft geleid tot de 0.8-versie van het Referentiekader.

In de zomer van 2021 is een gebruikersgroep geformeerd, waarin ongeveer twintig mensen uit verschillende instellingen deelnamen. Zij zijn in de praktijk aan de slag gegaan met het Referentiekader. In het najaar van 2021 is een inspiratiesessie met de gebruikersgroep gehouden, waarin aan de hand van casussen is besproken op welke punten het Referentiekader aangevuld diende te worden Tevens is feedback ontvangen op het Referentiekader van het FG Netwerk VSNU en het FG Netwerk hogescholen (VH).

Al deze input is verwerkt om te komen tot een zogenoemde 0.99-versie, die aan de bestuurders is voorgelegd ter vergadering op 3 december 2021 en daar is omarmd.

9.2 Toekomst

Dit Referentiekader is een levend document. Dit betekent dat het regelmatig een update behoeft om relevant en bruikbaar te blijven. Nieuwe technologische, maatschappelijke of praktische ontwikkelingen kunnen ertoe leiden dat elementen in dit Referentiekader moeten worden aangepast of het Referentiekader moet worden aangevuld. De Zone Studiedata van het Versnellingsplan zal dit proces faciliteren.

Colofon

Projectteam
- Bram Enning (zone studiedata)
- Dominique Campman (zone studiedata)
- Dominique Hagenauw (D.E. Hagenauw)
- George Wurpel (MSG Strategies)
- Mariken Betsema (MSG Strategies)
- Niek Reijmers (MSG Strategies)

Begeleidingsgroep

Experts:
- Miek Krol (UvA)
- Martijn de Hamer (HvA)
- Tom Paffen (VU)
- Joyce Van der Klugt (HSL)
- Bart Karstens (Rathenau instituut)
- Theo Nelissen (Avans Hogeschool)
- Marit Van Ree (NRO)

Klankbordgroep:
- Reinout van Brakel (VSNU)
- Marcel Tillema (VH)
- Germaine Poot en Iris Huis in 't Veld (SURF)
- Leon Van der Neut (ISO)
- Susanne Rijken (IvhO)
- Frits Jacobs (LU)
- Leoniek Wijngaards (UU)
- Janneke Lommertzen (ResearchNed)
- Theo Bakker (De Haagse Hogeschool)
- Gert Douma (Hanze Hogeschool)
- Aramis Jean Pierre (DUO)
- Frederik Zuiderveen Borgesius (RU)
- Martine Baars en Jason Pridmore (EUR)
- Eline Terpstra (LSVb)

Gebruikersgroep:
- Marlon Domingus (EUR)
- Dominique Booms (HR)
- Bert-Jan Klaren (Hanze Hogeschool)
- Jesse Bruins (LU)
- Ineke Stoop (Tilburg University)
- Marjolein Blaauboer (VU)
- Jan Tjeerd Groenewoud (RUG)
- Lex Freund (HR)
- Marco van Leeuwen (BUas)
- Vera Heusschen (HSL)
- Roland Ettema (OU)

Met bijzondere dank aan
Karen Maex (UvA) en Tineke Zweed (HU)
voor de inzichten bij aanvang
van het project.

Het Versnellingsplan Onderwijsinnovatie met ICT is een vierjarig programma van SURF, Vereniging Hogescholen en de VSNU dat inzet op het samenbrengen van initiatieven, kennis en ervaringen en snel en concreet aan de slag gaan met kansen voor het hoger onderwijs. Dit gebeurt in acht verschillende 'zones'. In de zone Studiedata werken 11 instellingen aan de hand van 16 deelprojecten aan het veilig en betrouwbaar benutten van studiedata in hoger onderwijs.

Meer informatie en onze publicaties vind je op
www.versnellingsplan.nl