LEARNING ANALYTICS IN 5 STAPPEN

EEN HANDREIKING VOOR DE AVG

SURF

INHOUD

INLEIDING

Learning analytics is het “het meten, verzamelen, analyseren en rapporteren van data van studenten en hun omgeving met als doel het leren en de leeromgeving te begrijpen en te optimaliseren” (Siemens, 2011). De analyses van deze data kunnen diverse doelgroepen (studenten, docenten, instellingen) waardevolle inzichten geven in verschillende aspecten van het onderwijsproces. Bij het verzamelen en analyseren van gegevens worden in veel gevallen persoonsgegevens verwerkt: gegevens die direct of indirect iets zeggen over individuen, bijvoorbeeld over studenten en docenten. Wanneer een onderwijsinstelling persoonsgegevens verwerkt, is daarop de Algemene Verordening Gegevensbescherming (AVG) van toepassing.

De AVG stelt hoge eisen aan de grondslagen voor de inzet van learning analytics. Het inzetten van learning analytics vraagt om een bewuste overweging van de risico’s voor het individu en het treffen van passende maatregelen. Het is geen kwestie van een keer toestemming vragen en een privacyverklaring opnemen op de site.

Met dit stappenplan wil SURF onderwijsinstellingen op weg helpen om learning analytics vorm te geven onder de AVG. Dit stappenplan is richtinggevend, waarbij iedere onderwijs-instelling zijn eigen privacyoverwegingen zal moeten maken. Het ondersteunt instellingen bij het borgen van de juridische kant van een learning-analyticsproject. Dit draagt bij aan een veilige leeromgeving die de privacy van individuen respecteert.

Let op

Dit stappenplan biedt instellingen een kader voor het introduceren van learning analytics in de eigen instelling. Het is echter geen uitputtend advies hoe je als instelling aan wet- en regelgeving kunt voldoen.

Aan de slag

Wil jouw instelling beginnen met learning analytics en daarvoor een project starten? Doorloop dan samen met het learning-analyticsteam de stappen in dit plan om zo de privacygevolgen van learning analytics direct te kunnen overzien. Sla geen stappen over, maar leg de focus op de stappen die het meest relevant zijn voor jouw project. Bij elke stap lees je over de relevante juridische termen en wat je moet doen. Betrek ook de Functionaris Gegevensbescherming (FG) van je instelling bij het uitvoeren van dit stappenplan.

Tip

Voor meer context van de juridische begrippen kun je:

- **de AVG-handleiding van de Rijksoverheid gebruiken**
- **de SURFwiki met uitleg over de AVG en de interpretatie ervan raadplegen**
- **de online module ‘Privacy in onderzoek’ van SURF volgen**

STAP 1: VOORBEREIDING

Tijdens de voorbereiding van het learning-analyticstraject is het van belang om eerst een projectteam samen te stellen met wie je samen de doeleinden van je traject gaat bepalen. Daarnaast is het van belang om alle stakeholders te identificeren binnen je project. Deze stap beschrijft de voorbereidingen die moet je treffen.

1.1 Bepaal de specifieke doelen die je met learning analytics wilt bereiken

Het is van belang om zo vroeg mogelijk de specifieke doeleinden van het project te bepalen. Tijdens de eerste stap bedenk en beschrijf je daarom wat je instelling daadwerkelijk met learning analytics wil bereiken. Definieer eerst welk resultaat je wilt nastreven om vervolgens te beschrijven hoe learning analytics daarbij kan helpen. De doeleinden die je in deze fase beschrijft, gebruik je ook bij het uitvoeren van het ontwerp in stap 2 en het beoordelen van de rechtmatigheid met een *Data Protection Impact Assessment* (DPIA) in stap 3.

Het omschrijven van de doeleinden is essentieel, omdat het de verwerking van persoonsgegevens eerlijk, transparant en begrijpelijk maakt. Belangrijke uitgangspunten zijn:

- **Doelbinding:** je mag gegevens alleen gebruiken voor specifieke, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Learning analytics is een manier om die doelen te bereiken. Later mogen – onder bepaalde omstandigheden – de verzamelde gegevens ook worden gebruikt voor een ander doel dan waarvoor ze zijn verkregen. Dat mag echter niet gebeuren op een wijze die onverenigbaar is met het doel waarvoor de gegevens zijn verzameld.
- **Dataminimalisatie:** de gegevens moeten toereikend, ter zake dienend en beperkt te zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.
- **Opslagbeperking:** je stelt termijnen vast voor het wissen van gegevens op basis van de doeleinden waarvoor de persoonsgegevens noodzakelijk zijn.
- **Verantwoording:** je moet het gebruik van persoonsgegevens vastleggen en het gebruik in transparante, begrijpelijke en gemakkelijk toegankelijke vorm uitleggen aan individuen. Zie daarvoor ‘Informeren’ in paragraaf 4.3.

Voorbeelden

Bepaal en beschrijf de doeleinden daarom zo specifiek mogelijk. Een algemene doelomschrijving, zoals ‘het leerproces verbeteren’ of ‘het opslaan van de antwoorden bij het maken van een proeftoets’ volstaat niet. De context en de verwachtingen van de individuen bepalen de mate van gedetailleerdheid die nodig is. Werk daarom verder uit wat er onder een algemene beschrijving van het doel wordt verstaan en de wijze waarop de gegevens voor dat doel worden gebruikt:

- **Doel:** ‘Meer aandacht geven tijdens de lessen aan de onderwerpen waar de meeste fouten worden gemaakt’. De volledige doelomschrijving inclusief de wijze waarop learning analytics wordt uitgevoerd is dan bijvoorbeeld: ‘De onderwijscoördinator van het vak ‘*grondslagen van het privacyrecht*’ analyseert de antwoorden in de digitale leeromgeving op groepsniveau gedurende het schooljaar om af te leiden bij welke onderwerpen de meeste fouten worden gemaakt om aan die onderwerpen meer aandacht te geven tijdens de lessen.’
- **Doel:** ‘Excellente studenten de voor hen relevante honoursprogramma’s aanbieden’. De volledige doelomschrijving inclusief wijze waarop learning analytics wordt uitgevoerd, is dan bijvoorbeeld: ‘De coördinatoren van honoursprogramma’s willen excellente studenten herkennen aan de hand van de snelheid en de resultaten van oefentoetsen in de online leeromgeving van relevante vakken aan het einde van een studiejaar, om aan hen relevante programma’s te kunnen aanbieden.’

Een goede, volledige doelomschrijving heeft de volgende structuur: ***'wie' wil 'wat'* doen aan de hand van *'welke'* persoonsgegevens en *'wanneer'* om *'resultaat'* te bereiken.** Denk daarbij aan het SMART-principe: Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdsgebonden. Goed omschreven doeleinden maken het doorlopen van het stappenplan een stuk makkelijker.

1.2 Stel een multidisciplinair projectteam samen

De volgende stap die je bij het uitvoeren van een learning-analyticstraject zet, is het samenstellen van het projectteam. Bedenk wie in de organisatie(s) er belang bij heeft om aan te sluiten bij het project. Is er al eerder een vergelijkbaar projectteam samengesteld? Kijk dan wie er zitting had in die groep.

Betrek mensen met de juiste expertise bij je projectteam. Denk aan de volgende expertises: opdrachtgever, projectleider, ontwerper, functioneel beheerder, jurist en docenten.

Naast het projectteam is het belangrijk om na te denken welke stakeholders er (later) in het project betrokken moeten worden. Een bijzondere rol is daarbij weggelegd voor de Functionaris Gegevensbescherming (FG). Je moet advies van de FG inwinnen bij het beoordelen van de verwerking en het uitvoeren van een *Data Protection Impact Assessment* (DPIA). Daarover meer in stap 3.

Bepaal hoe je draagvlak binnen de instelling en bij de individuen creëert. Hoe kun je studenten van het belang van learning analytics overtuigen? Ga hierover met ze in gesprek. Dit is overigens meteen een belangrijk onderdeel van het uitvoeren van de DPIA.

1.3 Beschrijf de stakeholders

Beschrijf welke specifieke groepen stakeholders een rol spelen bij het inzetten van learning analytics, bepaal wat hun positie is en wat hun verwachtingen of wensen zijn (een stakeholderanalyse). Het gaat hierbij om groepen binnen de instelling, degene die gaan werken met het learning-analytics-systeem en deze beheren, maar ook groepen die helpen met het onderhoud van het systeem, onderaannemers en groepen waarvan gegevens worden verzameld. Denk hierbij aan studenten, docenten, beheerders, projectleiders en management. Wellicht zijn er binnen de instelling procedures om het project voor te leggen aan de medezeggenschapsraad of studentenraad of ook te laten toetsen door een toetsingscommissie of een *Ethics Board*. Als ervaringsdeskundigen binnen of buiten de instelling al learning analytics hebben toegepast, betrek dan deze experts.

Een stakeholderanalyse helpt je met het leren van ervaringen van anderen, het meenemen van focuspunten en risico's waaraan je eerder niet hebt gedacht en het creëren van draagvlak bij belanghebbenden.

STAP 2: ONTWERP

Wanneer je de kaders van het learning-analyticstraject hebt bepaald en beschreven in een eerste versie van je plan van aanpak, werk je vervolgens uit hoe je dit gaat realiseren. De uitkomst van deze stap is een beschrijving van de benodigde systemen om learning analytics mogelijk te maken. Het ontwerp maakt technisch en juridisch duidelijk hoe de instelling learning analytics uitvoert.

De onderstaande ontwerpstappen houden al rekening met juridische principes. Toch maak je in deze fase nog geen afweging of het gehele learning-analytics-systeem rechtmatig is en welke grondslag toepasselijk is. Voor die afweging dient het ontwerp eerst duidelijk te zijn. Daarom beoordeel je de rechtmatigheid pas later. Meer daarover in stap 3.

2.1 Neem privacybescherming mee in het ontwerp

Learning analytics werkt pas echt als je erin slaagt de verzamelde gegevens op de juiste manier te verwerken. Dus denk bij de volgende stappen goed na over welke data verzameld moeten worden om je doeleinden te realiseren en neem de uitkomst op in het ontwerpplan.

Bepaal welke data je minimaal nodig hebt om je doelen te bereiken
Kun je je doel ook bereiken door van minder individuen gegevens te verzamelen? Of door minder gegevens per individu te verzamelen? Bij het ontwerpen van het learning-analytics-systeem ben je namelijk wettelijk verplicht om vanaf het begin privacybescherming mee te nemen in het ontwerp.

Het concept *privacy by design* houdt in dat je al in de ontwerpfase van een product of dienst rekening houdt met privacygevoelige elementen en dat er voldoende privacywaarborgen worden ingebouwd om persoonsgegevens goed te beschermen en te beveiligen.

Hoe minder gegevens je verzamelt van individuen, hoe makkelijker het is om de gegevens te beschermen en hoe minder kans er is op een datalek. Daarnaast kun je gegevens beschermen door ze te splitsen met als doel gegevens uit elkaar te halen en los van elkaar te verwerken, zodat gegevens alleen met een duidelijk doel gecombineerd worden. Ook kun je soms persoonsgegevens beschermen door ze te gebruiken in een abstractere vorm: geaggregeerd in plaats van gedetailleerd. Statistiek is de bekendste vorm van het weergeven van onderzoeksgegevens zonder het openbaar maken van de persoonsgegevens zelf.

Tip

Lees meer over privacy by design en toepasselijke strategieën:
- **op Privacy Designer**
- **in het Blauwe Boekje (pdf) privacyontwerpstrategieën**

2.2 Bepaal de scope van je verwerking

Het is belangrijk om vooraf duidelijk te weten wat de reikwijdte van je project is vanuit privacyperspectief. Het is van belang om vooraf vast te stellen:

1. wat voor persoonsgegevens je gebruikt
2. de gevoeligheid van de persoonsgegevens
3. de hoeveelheid gegevens die je verwerkt, en
4. of er eventueel overige relevante elementen zijn die iets zeggen over de omvang van je verwerkingen, zoals het geografisch gebied.

1. Bepaal welk deel van je dataset uit persoonsgegevens bestaat

De AVG geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Persoonsgegevens zijn dus bijvoorbeeld een naam en adres, maar ook gekoppelde tentamencijfers of gegevens over gedrag. Door deze gegevens verder te combineren (eventueel met andere gegevens) is het namelijk mogelijk om deze gegevens naar personen te herleiden. Het gaat dan om indirect identificeerbare gegevens.

Beschrijf welke persoonsgegevens worden verzameld in het kader van dit project. Zie voor meer informatie de AVG-handleiding van de Rijksoverheid en de SURFwiki met uitleg over de AVG en de interpretatie ervan.

2. Bepaal of je bijzondere persoonsgegevens verwerkt

Bijzondere persoonsgegevens zijn gegevens over zaken als iemands gezondheid, etnische afkomst, seksuele voorkeur, politieke voorkeur of godsdienst. Hiervoor geldt een verwerkingsverbod, tenzij de instelling toestemming heeft van het individu of als het gebruik in een wet is geregeld. Toestemming houdt in dat je apart vraagt naar het relevante gegeven en uitlegt waarom dat is, waarbij het optioneel is om die toestemming te verstrekken.

Voor het verwerken van bijzondere gegevens met learning analytics is het verkrijgen van uitdrukkelijke toestemming de meest voor de hand liggende uitzondering. Zie voor de basiselementen 'Toestemming' in paragraaf 3.1. Als het vragen van toestemming feitelijk onmogelijk blijkt, dan is er wel een mogelijke uitzondering voor wetenschappelijk onderzoek (zie artikel 24 Uitvoeringswet AVG).

Tip

Zie voor meer informatie over het onderscheid tussen uitdrukkelijke toestemming om bijzondere persoonsgegevens te verwerken en daarnaast toestemming als grondslag de Nederlandse vertaling van de richtlijnen over toestemming van de European Data Protection Board (pdf).

Let op

Het burgerservicenummer (BSN) - hetzelfde nummer dat de overheid als onderwijs-nummer gebruikt - is ook een speciaal soort persoonsgegeven. Dit mag je alleen verwerken als in een wet staat dat dat mag en voor welk doel. Denk aan het kopiëren van identiteitsbewijzen: daarbij moet het BSN onleesbaar worden gemaakt.

Je kunt als instelling ook onbedoeld bijzondere persoonsgegevens verwerken. Bijvoorbeeld als de instelling studeergedrag in online-leeromgevingen uitvoerig analyseert met conclusies die specifiek verbonden zijn aan medische (slaap-/leefpatronen) of religieuze (gedrag op godsdienstige dagen) gegevens. Probeer daarom in deze stap zulke eventuele gevolgen van de learning-analytics-analyses op te merken.

3. Bepaal de hoeveelheid gegevens die je verwerkt

Nadat je hebt vastgesteld wat voor (gevoelige) persoonsgegevens je minimaal nodig hebt voor het bereiken van je doel, is het ook van belang om te bepalen hoeveel soorten gegevens je gaat verwerken in het kader van het learning-analyticstraject. Hierbij is het van belang om in ieder geval antwoord te geven op volgende vragen:

- Hoeveel soorten gegevens zijn we van plan om te verwerken?
- Hoe vaak verwerken we deze gegevens?
- Hoe lang zullen de verwerkingen van de gegevens duren (van verzameling tot het verwijderen/anonimiseren van de gegevens)
- Van hoeveel betrokkenen (diegene die onderwerp zijn van het learning-analyticstraject) zullen gegevens worden verwerkt?

4. Bepaal of overige elementen relevant zijn voor de reikwijdte van het traject

In sommige gevallen zijn er nog andere factoren die relevant zijn voor het bepalen van de reikwijdte van de verwerking. Een voorbeeld hiervan is het geografische gebied waarbinnen gegevens verwerkt worden. Zo kan het zijn dat wanneer persoonsgegevens van individuen uit andere (Europese) landen worden verwerkt, bepaalde regels anders zijn. Als je tot de conclusie komt dat dit het geval is, raden we je aan om de FG te raadplegen om te bepalen of er specifieke maatregelen nodig zijn.

2. 3 Beschrijf hoe de verwerking van gegevens plaatsvindt

1. Bepaal welke handelingen je verricht: verwerken van persoonsgegevens

Beschrijf de verschillende handelingen die je verricht met de persoonsgegevens. Verwerken is: alle handelingen die een onderwijsinstelling kan uitvoeren met persoonsgegevens, van verzamelen en opslaan tot en met vernietigen. Beschrijf daarom elke fase van verwerking voor learning analytics, zoals het verzamelen, vervolgens het analyseren en daarna het gebruiken van de resultaten. Bijvoorbeeld bijhouden wat iemand in een leeromgeving doet, is een vorm van persoonsgegevens verwerken. Pseudonimiseren en anonimiseren zijn goede maatregelen om de privacy van individuen te beschermen, maar zijn ook handelingen die onder het begrip verwerken vallen.

2. Beschrijf de databronnen die je gaat gebruiken

Beschrijf de databronnen die je gaat gebruiken (de input) en de oorsprong van deze bronnen. Bepaal welke data die je nodig hebt, al bijgehouden worden binnen de instelling en waar de data vandaan gehaald kunnen worden.

Onderwijsinstellingen beschikken over tal van systemen die relevante data kunnen bevatten. Denk aan je leermanagementsysteem, studentinformatiesysteem, toetssystemen, aanwezigheidsmonitoring, maar ook mobiele applicaties met bijbehorende sensoren (bijvoorbeeld gps-tracking). De kracht van learning analytics is dat je die data samen kunt brengen met behulp van technische standaarden.

Let op

Gebruik niet direct alle al bestaande data voor je learning-analyticstraject. Loop eerst het stappenplan af en hanteer altijd dataminimalisatie.

3. Beschrijf de gebruikte systemen

Breng in kaart welke systemen en diensten binnen en buiten de instelling relevant zijn om het traject uit te voeren. Hoe zet je het learning-analytics-systeem op? Gebruik je een aparte website, of wellicht ook een app? Of wordt er al een bestaand systeem gebruikt om learning analytics toe te passen? Bevat het systeem nieuwe technologieën waarvan de risico's nog niet geheel duidelijk zijn?

Bedenk dat bij de verzameling van gegevens via cookies (en vergelijkbare technologieën, zoals scripts) randvoorwaarden gelden uit de Telecommunicatiewet. Zie hiervoor de regels bij 'Toestemming' in paragraaf 3.1.

4. Beschrijf de betrokken dienstverleners

Voor learning analytics maken onderwijsinstellingen vaak gebruik van dienstverleners, zoals leveranciers. Bepaal wie toegang krijgt tot de gegevens en met wie de instelling de gegevens deelt. Het kan dat dienstverleners via learning-analytics-software toegang hebben tot de gegevens. Voorbeelden hiervan zijn clouddiensten voor studenten of externe systemen die de prestaties bij toetsen meten en daarover rapportages genereren.

Als je software of diensten van derden inzet, zijn er twee zaken waarop je moet letten:

1. De instelling is altijd zelf privacyrechtelijk aansprakelijk voor de kwaliteit van en problemen bij de dienstverlening. Dit geldt dus ook wanneer de softwareleverancier zelf geen aansprakelijkheid wenst te dragen. De instelling kan deze aansprakelijkheid niet ontwijken door bijvoorbeeld een aansprakelijkheidsbeperking op te nemen in een akkoordverklaring van het learning-analyticssysteem of een disclaimer bij het startscherm van de software.
2. Als de externe dienstverlener zelf ook persoonsgegevens ontvangt, zoals bij clouddiensten, moet de instelling aparte afspraken maken over wat de dienstverlener daarmee mag doen. Hiervoor is het van belang om vast te stellen wat de rol is van de dienstverlener. Om te bepalen welke privacyrol een dienstverlener heeft, lees de toelichting in paragraaf 2.5.

Selectie van dienstverleners

Neem bij de selectie de eisen van de AVG mee zoals, beveiligings- en informatieverplichtingen en maatregelen bij verwerking van gegevens buiten Europese Economische Ruimte. Wanneer je een dienstverlener verwerkingsactiviteiten toevertrouwt, mag hij namelijk alleen een beroep doen op dienstverleners die voldoende garanties bieden, met name op het gebied van deskundigheid, betrouwbaarheid en middelen. Zo zorg je ervoor dat de technische en organisatorische maatregelen beantwoorden aan privacyregelgeving, ook gelet op de beveiliging van de verwerking.

2.4 Beschrijf de (beveiligings)maatregelen

Een instelling die persoonsgegevens gebruikt moet deze volgens de AVG beveiligen. Zo verlaag je het risico op datalekken en andere mogelijke inbreuken op de bescherming van persoonsgegevens. Op basis van de AVG moet je hiervoor passende technische maatregelen nemen, zoals het gebruik van moderne techniek om persoonsgegevens te beveiligen. Verder moet je niet alleen naar de techniek kijken, maar ook naar hoe je als organisatie met persoonsgegevens omgaat. Wie heeft er bijvoorbeeld toegang tot welke gegevens?

Neem technische en organisatorische maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens te borgen

Als je persoonsgegevens opslaat, moet je deze adequaat beveiligen. Dit betekent dat je als instelling alle verkregen persoonsgegevens redelijkerwijs beschermt tegen ongeautoriseerde en onrechtmatige kennisname of gebruik. Niet alleen de gegevens waar je om gevraagd hebt, maar ook onbedoeld ontvangen persoonsgegevens moet je beveiligen. Wij raden daarom aan een beleid voor beveiliging en datalekken op te stellen.

Er bestaat nog geen algemeen geldende norm of standaard specifiek voor beveiliging van persoonsgegevens. In bepaalde branches gelden specifieke normen, zoals NEN 7510 in de zorg. SURF heeft een normen en toetsingskader opgesteld over informatiebeveiliging gebaseerd op de NEN 27001.

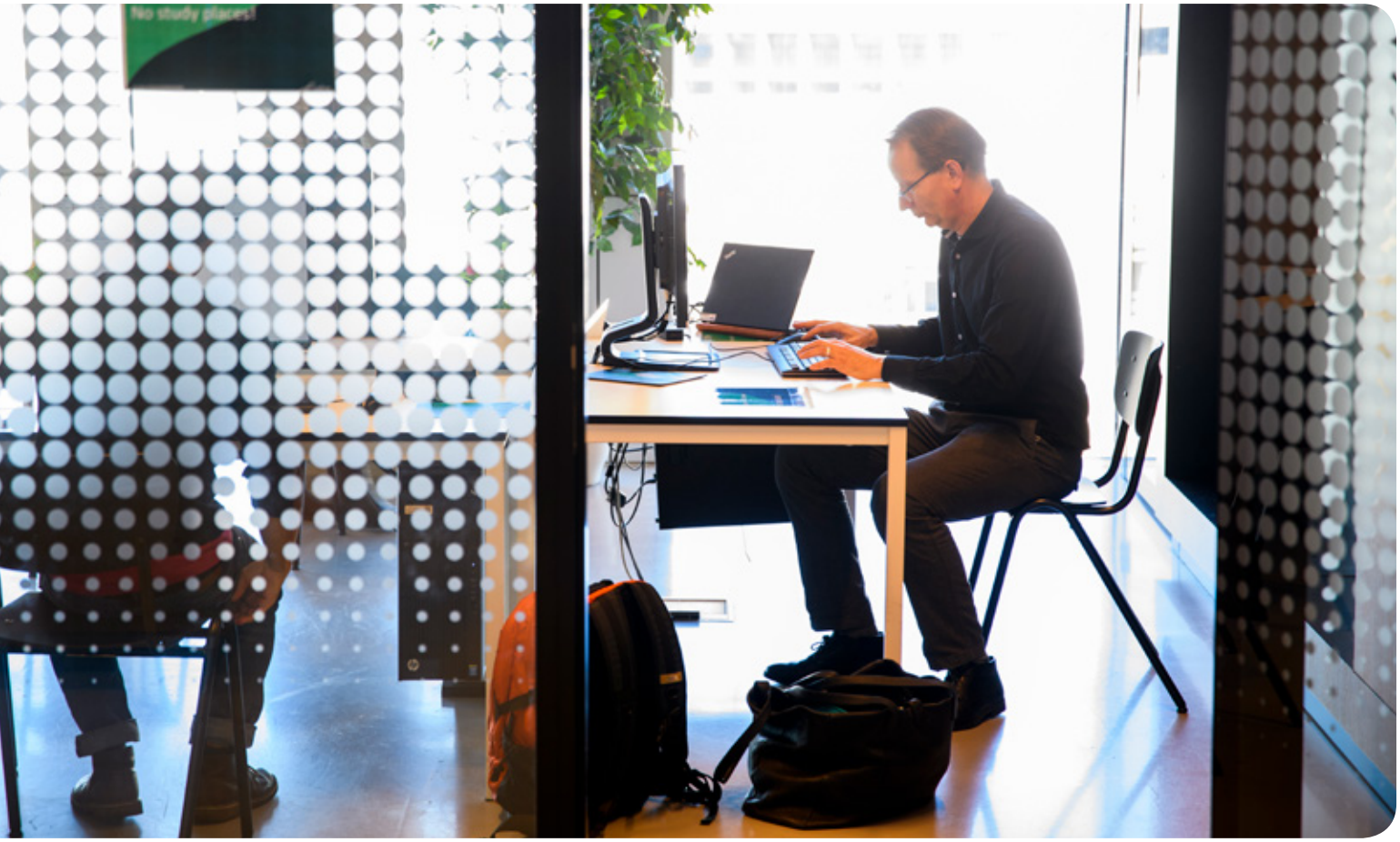
De privacytoezichthouder heeft richtlijnen gepubliceerd over hoe je als instelling kunt voldoen aan de beveiligingseis. Deze richtlijnen geven aan dat beveiliging een integraal onderdeel moet zijn van de ontwikkeling en de verbetering van je diensten en dat je regelmatig moet toetsen (PlanDoCheckAct) of de beveiliging nog wel adequaat is.

Daarnaast moeten de gegevens accuraat en beschikbaar te blijven. Neem daarom maatregelen die aanpassing van gegevens voorkomen en die dreigingen verminderen en wegnemen waardoor gegevens niet langer beschikbaar zijn. Denk bijvoorbeeld aan het nemen van maatregelen om gijzelsoftware en DDoS-aanvallen af te slaan.

Tip

Raadpleeg meer bronnen over beveiliging:

- **de website van de Autoriteit Persoonsgegevens**
- **De handige rapporten van de Franse privacytoezichthouder en ENISA/Teletrust**



Pas aggregatie en pseudonimisatie toe

In sommige gevallen worden maatregelen gebruikt om gegevens beter te beveiligen of te beschermen. Bijvoorbeeld als er gebruik wordt gemaakt van *hashing*, een toepassing waarbij gegevens cryptisch worden bewerkt. Ook in die gevallen blijft volgens de toezichthouder sprake van een verwerking van persoonsgegevens. Alleen het hashen van namen of andere identificerende gegevens, zonder aanvullende maatregelen, leidt er namelijk niet toe dat er geen persoonsgegevens worden verwerkt. Zo is het in die gevallen nog steeds mogelijk om de gegevens terug te herleiden tot individuele personen. Dit wordt ook wel *pseudonimiseren* genoemd. Deze gegevens vallen nog steeds onder de werking van de AVG.

Gegevens zijn pas geanonimiseerd als er geen redelijke manier meer is om de gegevens te herleiden naar een persoon. Bijvoorbeeld als willekeurige unieke nummers zijn toegekend aan de gegevens en vervolgens de lijst met de naamnummerkoppeling is vernietigd. Toch kan ook dan een persoon nog vaak via andere gegevens worden achterhaald, ook als er geen naam of herleidbaar uniek nummer is gekoppeld. Een verzameling van de tentamencijfers en vakken van een student is bijvoorbeeld uniek, geen twee studenten halen namelijk in hetzelfde jaar voor hetzelfde vakkenpakket exact dezelfde cijfers. Die verzameling vormt dan een set persoonsgegevens, ook als de naam of het (unieke) nummer van de student er niet bij staat.

Je kunt gegevens hun status als persoonsgegeven laten verliezen door ze voldoende te aggregeren: je voegt ze dan samen tot uitspraken over meerdere personen. ‘Tachtig procent van de studenten zakt voor deze toets’ is bijvoorbeeld geen persoonsgegeven. Aan dergelijke statistische gegevens stelt de wet geen eisen.

Let op

Met voldoende geaggregeerde gegevens heb je meer mogelijkheden, maar de brongegevens blijven persoonsgegevens waarop de AVG van toepassing is. Alleen verwerkingen waarbij je start met geaggregeerde gegevens geven je meer mogelijkheden. Als een docent bijvoorbeeld bij een online leerplatform meet hoe snel individuele studenten door de stof gaan, is daarvoor een grondslag nodig. Dat geldt ook als hij vervolgens alleen statistische uitspraken doet over zijn bevindingen. Zie voor meer informatie de richtlijnen over onderzoek en het anonimiseren van gegevens gepubliceerd door de voorganger van de European Data Protection Board (EDPB).

Bepaal de organisatorische wistermijnen van de datasets

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van de verwerking. Wanneer de gegevens niet langer noodzakelijk zijn, dan moeten zij worden vernietigd of gewist. Je moet dus van tevoren een wistermijn bepalen voor de verschillende datasets. Dat hangt geheel af de doelen waarvoor je de verschillende datasets bewaart en hoe het systeem de datasets verwerkt.

- Maak een inschatting van hoe lang je datasets nodig hebt om de doelen te bereiken.
- Houd zoveel mogelijk rekening met verdere verwerkingsdoelen, zoals onderbouwing van onderzoeken in rapportages, archiveringsdoelen, academische verantwoording en de richtlijnen van de Autoriteit Persoonsgegevens.

Tip

Zie ook de handreikingen van het Landelijk Coördinatiepunt Research Data Management (LCRDM).

2.5 Bepaal de privacyrollen van de stakeholders

Per gegevensverwerking bepaal je welke privacyrol de betrokken partijen hebben.
De rollen die de AVG onderscheidt, zijn:

- Verwerkingsverantwoordelijke: degene die het doel en de middelen bij verwerking bepaalt
- Gezamenlijk verantwoordelijken: degenen die samen het doel en de middelen van onlosmakelijk verbonden verwerkingen bepalen
- Verwerker: degene die in opdracht van de verwerkingsverantwoordelijke persoons-gegevens verwerkt, en
- Derde: de overige partijen.

Voorbeeld: *Een hogeschool besluit om gegevens van studenten te analyseren om te meten welke vakken ertoe leiden dat leerlingen vaker zakken. Om dit te analyseren gebruikt de hogeschool een cloudtool waarin ze alle cijfers van leerlingen gedurende een jaar invoeren. In dit geval bepaalt de hogeschool welke gegevens ze voor welke doelen analyseren. De leverancier van de cloudoplossing voert slechts analyses uit in opdracht van de hogeschool. De hogeschool is in dit geval dus een verwerkingsverantwoordelijke voor de verwerking en de leverancier van de tool is een verwerker.*

Tip

Gebruik voor meer context van de juridische begrippen de AVG-handleiding van de Rijksoverheid.

STAP 3: BEOORDELING

3.1 Rechtmatigheid van het learning-analyticstraject

Het is van belang om te onderzoeken of de doelen van learning analytics in verhouding staan tot de inbreuk voor de individuen van wie je de gegevens verwerkt (**proportionaliteit**). En of je het doel niet op een voor de betrokken individuen minder nadelige manier kunt bereiken (**subsidiariteit**). Deze afwegingen heb je als het goed is al gedeeltelijk gemaakt tijdens de ontwerpfase van het project (zie stap 2).

Bepaal of de toepassing proportioneel is
Proportionaliteit hangt af of het gebruik van learning analytics evenredig is. Weeg daarom af wat je als instelling nastreeft met learning analytics en bepaal hoe dit doel zich verhoudt tot de mogelijke impact op de individuen. Hoewel het doel de middelen niet heiligt, zal in zijn algemeenheid voor een zwaarder doel meer geoorloofd zijn. De gegevens moeten noodzakelijk zijn voor het doel. Dat is strenger dan 'wenselijk' of 'handig'.

Bepaal of met minder ingrijpende middelen hetzelfde doel te verwezenlijken is
Samen met de proportionaliteit van learning analytics moet de subsidiariteit worden beoordeeld. Dit betekent dat er geen minder ingrijpende manier moet zijn om hetzelfde doel te bereiken. In de context van learning analytics moet dan onder andere worden gekeken naar het overkoepelende doel en of dat doel ook op een andere wijze te verwezenlijken is, zonder het gebruik van learning analytics. Neem daarin de noodzaak van de verwerking van gegevens, de complexiteit en de gevolgen van learning analytics mee.

Zodra het ontwerp van learning analytics is vastgesteld (resultaat van stap 2), en je de proportionaliteit en subsidiariteit hebt vastgesteld kun je de relevante grondslag(en) van de verwerking aanwijzen. Elke verwerking van persoonsgegevens heeft uiteindelijk een grondslag, ofwel een rechtvaardiging nodig. De grondslag geeft de instelling de rechtvaardiging dat persoonsgegevens voor learning analytics mogen worden verwerkt. Voor iedere fase: verzamelen, analyseren en gebruiken, heb je in principe een van de volgende zes grondslagen nodig:

- toestemming
- uitvoering overeenkomst
- wettelijke plicht
- bescherming vitale belangen
- uitvoering publieke taak
- gerechtvaardigd belang

Gegevens gebruiken voor andere doelen dan waarvoor ze oorspronkelijk verzameld zijn
Een instelling kan alleen gegevens verzamelen en verwerken op basis van een van de genoemde grondslagen. Vervolgens kan je als instelling deze gegevens ook gebruiken voor wetenschappelijk onderzoek, statistiek of andere verenigbare doelen, als de instelling de nodige maatregelen heeft getroffen waardoor het zeker is dat de verdere verwerking uitsluitend geschiedt voor deze specifieke doeleinden. Wie een e-mailadres krijgt van een persoon die een vraag stelt, mag die persoon een antwoord sturen maar niet abonneren op de nieuwsbrief. Dat is immers een ander doel. Een ander doel is wel toegestaan als het verenigbaar is met het oorspronkelijke doel.

Een voorbeeld is een enquête sturen over de kwaliteit van de helpdesk naar iemand die hiervan gebruik heeft gemaakt. Omdat de verdere verwerking (hier learning analytics) moet aansluiten bij de specifieke doelen, is doelbinding een lastige eis. Het idee is immers om nieuwe inzichten te verkrijgen, nieuwe vragen te kunnen stellen en vanuit nieuwe hoeken naar de gegevens te kijken.

Per definitie is er vaak dus geen 'bepaald doel'. Daarom raden we aan om zo veel mogelijk concrete doelen te benoemen in de verstrekte informatie en deze regelmatig te herzien. Bij het herzien van doelen waarvoor je als instelling eerder toestemming hebt verkregen, moet je opnieuw toestemming vragen voor de hernieuwde doelen.

Voorbeeld: *Een docent zet een monitoringtool in bij een tentamen om te meten of herkansers anders presteren dan eerstekansers. Hiervoor is de grondslag 'gerechtvaardigd belang' gebruikt. Vervolgens mogen de resultaten worden verwerkt in statistisch onderzoek naar succesfactoren bij dat tentamen. Dat geldt als verdere verwerking voor onderzoek.*

Tip

Zie voor de randvoorwaarden bij wetenschappelijk onderzoek ook de handreikingen van het Landelijk Coördinatiepunt Research Data Management (LCRDM).

Past de instelling learning analytics toe op al eerder **rechtmatig** verzamelde gegevens en zijn de doeleinden van learning analytics verenigbaar met die waarvoor deze persoonsgegevens aanvankelijk zijn verzameld? In dat geval is er geen andere afzonderlijke rechtsgrond vereist dan de grond waarop de aanvankelijke verwerking was toegestaan.

De volgende factoren zijn van belang bij het bepalen of de doeleinden verenigbaar zijn:
- met name **de redelijke verwachtingen van de individuen** op basis van hun verhouding met de instelling over het verdere gebruik ervan
- eventuele koppeling tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking
- de context waarin de gegevens zijn verzameld: wat is de relatie tussen de instelling en het individu?
- het type en de aard van de gegevens: is het gevoelig?
- de mogelijke gevolgen van de voorgenomen verdere verwerking: wat zijn de gevolgen voor het individu?
- het bestaan van passende waarborgen, zoals encryptie, aggregatie of pseudonimisering.

Deze 'verenigbaarheids'-uitzondering is relevant als de individuen kunnen verwachten dat slechts de eerder verzamelde gegevens gebruikt worden voor het specifieke learning-analyticstraject, waarvan de doeleinden lijken op de aanvankelijke doeleinden, en dat de gegevens zich beperken tot niet-gevoelige gegevens die vervolgens in het learning-analytics-traject geen grote gevolgen hebben voor de individuen.

Als de learning analytics (ook) afhankelijk is van nieuwe bronnen of als de doeleinden niet verenigbaar zijn met de oorspronkelijke doeleinden, dan moet de instelling nagaan of een van de zes grondslagen gebruikt kan worden zoals benoemd aan het begin van deze paragraaf.

Grondslag: Bepaal of 'toestemming' nodig is voor (onderdelen van) de verwerking

In sommige gevallen moeten de individuen toestemming geven aan de instelling om hen te mogen volgen met learning analytics. Vanwege de voorwaarden waaraan toestemming moet voldoen is dit juridisch en technisch gezien een uitdaging. Toestemming geven is namelijk niet slechts een formeel vinkje zetten of een pop-up wegklikken, maar toestemming moet een daadwerkelijk vrije instemming van individuen zijn en hen controle te geven over (een onderdeel van) de learning-analytics-verwerking.

Als hoofdregel kun je aanhouden dat in ieder geval de toestemming van individuen nodig is als learning analytics:

- bijzondere persoonsgegevens verwerkt (zie paragraaf 2.2);
- gevoelige persoonsgegevens verwerkt, zoals locatiegegevens. Dat kan in bepaalde gevallen een ernstig risico voor de gegevensbescherming opleveren, waardoor hoge mate van individuele controle passend is;
- cookies of andere gegevens, zoals learning-analytics-scripts, op de computers, laptops of telefoons plaatst of uitleest die de individuen gebruiken; [1] en
- besluiten neemt die uitsluitend zijn gebaseerd op een geautomatiseerde verwerking van persoonsgegevens, als die besluiten rechtsgevolgen hebben of als de individuen anders-zins in aanmerkelijke mate treffen.
- na de belangenafweging en de getroffen maatregelen bij de grondslag 'gerechtvaardigd belang' de belangen van individuen niet voldoende in acht neemt. Deze grondslag is beschreven aan het einde van deze paragraaf.

De wet schrijft niet precies voor hoe je toestemming moet vragen. Maar de manier waarop de instelling toestemming vraagt moet wel voldoen aan de volgende specifieke eisen:

1. **Vrij gegeven**: toestemming moet in vrijheid worden gegeven. Individuen moeten ook 'nee' kunnen zeggen. Dat mag bijvoorbeeld niet tot gevolg hebben dat ze geweigerd worden voor een verplicht vak of geen tentamen mogen doen.
2. **Ondubbelzinnig**: er moet sprake zijn van een duidelijke actieve handeling. Dat betekent geen voor-aangevinkte vakjes.
3. **Geïnformeerd**: als instelling moet je individuen direct en voorafgaand informeren over de belangrijkste onderdelen, zoals het doel van elke verwerking waarvoor je toestemming vraagt, welke persoonsgegevens worden verwerkt en over het intrekken van toestemming. Dat laatste moet net zo makkelijk gaan als het geven ervan.
4. **Specifiek**: toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel. 'Ik geef toestemming voor learning analytics' is niet specifiek. Maak duidelijk wie monitort, welke gegevens verzameld worden en wat daarmee gebeurt. Een voorbeeld: 'Ik geef toestemming voor het volgen en registreren van mijn studieprestaties in de online leeromgeving van dit vak. Hierbij krijg ik studieadvies op maat. De studiebegeleider krijgt deze gegevens om mij proactief te kunnen aanspreken op risico's voor vertraging.'

Als je bij de verwerking voor meerdere doeleinden toestemming vraagt, moet je als instelling de betrokkene hierover informeren en hem voor elk doel afzonderlijk toestemming vragen. Het doel mag ook niet gaandeweg veranderen.

Kortom, maak duidelijk op welke vakken de toestemming betrekking heeft, hoe ver de monitoring gaat per vak en wat per vak de gevolgen zijn. Je kunt ook in enkele zinnen een korte uitleg geven met een link naar een heldere en informatieve privacyverklaring waarin meer specifieke informatie te lezen is. Het is niet toegestaan om toestemming via de gebruiksvoorwaarden, algemene voorwaarden of privacyverklaring te verkrijgen. Wel kun je voor verdere uitleg over de toestemming naar een privacyverklaring verwijzen. Zie verder de stap 'Informeren' in paragraaf 4.3.

Voldoet de toestemming niet aan bovenstaande eisen? Dan is de toestemming niet geldig. Je mag de persoonsgegevens dan (voor dit onderdeel) niet verwerken. Bovendien moet je als instelling kunnen aantonen dat geldige toestemming is verkregen, tijdens en tot 5 jaar na de verwerking. Dit maakt toestemming een kwetsbare en een moeilijk te hanteren grondslag.

[1] *Dit geldt niet voor cookies die noodzakelijk zijn voor de technische werking van de (onderwijs)dienstverlening of voor analytische cookies die slechts een geringe inbreuk maken op de privacy van de individuen (zie ook artikel 11.7a Telecommunicatiewet en de toekomstige ePrivacy Verordening en het stappenplan van de Autoriteit Persoonsgegevens*

Tip

Zie voor meer informatie de Nederlandse vertaling van de AVG-richtlijnen over toestemming van de European Data Protection Board (EDPB).

Grondslag: Uitvoering overeenkomst

Persoonsgegevens mogen worden verwerkt als dit noodzakelijk is voor de uitvoering van een overeenkomst. Als een instelling met iemand een overeenkomst heeft gesloten, mag de instelling de persoonsgegevens van deze persoon verwerken voor zover dit noodzakelijk is om de overeenkomst uit te kunnen voeren. Dit moet dan wel een overeenkomst zijn waarbij het individu zelf ook partij is. De verwerking moet wel een noodzakelijk uitvloeisel van de overeenkomst zijn.

Het enkele feit dat in een overeenkomst met de individuen learning analytics is opgenomen, wil nog niet zeggen dat daarmee is voldaan aan de eis dat deze verwerking ook noodzakelijk is om die overeenkomst uit te voeren. Bij de weging of de gegevensverwerking noodzakelijk is voor de te leveren (onderwijs)prestatie, bepalen uiteindelijk de inhoud en het fundamentele doel van de overeenkomst of de gegevensverwerking daadwerkelijk noodzakelijk is voor de (onderwijs)prestatie. De instelling mag zich dan in dat geval op deze grondslag baseren. De overeenkomst zelf mag echter niet enkel gericht zijn op het verwerken van persoonsgegevens, maar moet een ander (onderwijs)doeleinde hebben. Een onderwijsinstelling heeft over het algemeen geen overeenkomst met studenten. Sommigen zien de inschrijving aan de instelling als een overeenkomst, maar dat is strikt juridisch niet juist.

Als onderwijsinstelling moet je ook voor deze grondslag aantonen dat het noodzakelijk is om learning analytics in te zetten. Omdat dit redelijk nieuw is, kan het snel als niet-noodzakelijk voor onderwijs worden gezien. De gangbare zienswijze is dat onderwijs prima zonder learning analytics kan worden gegeven. Pas als duidelijk is dat onderwijs zonder learning analytics tekortschiet, kan dit als noodzakelijk worden gepresenteerd. Maar dat kan pas als learning analytics zijn waarde over meerdere jaren heeft bewezen. Deze grondslag is daarom mogelijk toe te passen, al is de waarschijnlijke koppeling met specifieke onderwijsdoeleinden minder sterk.

Grondslag: Wettelijke plicht

Als derde grondslag noemt de AVG de wettelijke plicht. Gegevens mogen worden verwerkt als er een wet is die daartoe verplicht. Om verwerkingen van persoonsgegevens op deze grondslag te kunnen baseren, moet het niet mogelijk zijn om aan de plicht te voldoen zonder dat er persoonsgegevens worden verwerkt.

Een instelling kan het standpunt innemen dat zij verplicht de doelen uit wetgeving uitvoeren. Daarvoor is een goed inzicht in studeerprestaties nodig. Learning analytics is een middel om dat inzicht te krijgen. Die redenering zou de inzet van dit middel kunnen rechtvaardigen. Hierbij geldt wel dezelfde kanttekening over noodzakelijkheid als bij de grondslag ‘Uitvoering overeenkomst’.

Grondslag: Algemeen belang of openbaar gezag

Deze grondslag is relevant als de instelling een publieke taak uitoefent voor het algemeen belang of openbaar gezag, zoals uit de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). Het gaat daarbij om taken die in de wet hun basis vinden en die relevant zijn voor de instelling. Net als bij de andere grondslagen geldt dat ‘noodzaak’ een hoge maatstaf is die je moet kunnen onderbouwen. De gegevens moeten niet alleen ‘relevant’ of ‘handig’ zijn.

Een onderwijsinstelling kan bij de onderbouwing van de noodzaak het standpunt innemen dat zij hun publieke taak breed invult. Daarvoor is een goed inzicht in studeerprestaties nodig. Learning analytics is een middel om dat inzicht te krijgen. Die redenering zou de inzet van dit middel kunnen rechtvaardigen. De instelling moet zelf kunnen onderbouwen dat learning analytics echt nodig is voor de publieke taak en dat er geen reëel alternatief (meer) is.

Tip

Loop voor de learning-analytics-verwerkingen die niet onder de publieke taak van de instelling vallen de voorwaarden van de grondslag 'gerechtvaardigd belang' hieronder af. De uitoefening van publieke taken mag een instelling als semi-overheidsinstantie namelijk niet baseren op 'gerechtvaardigd belang'.

Grondslag: Gerechtvaardigd belang

Deze grondslag houdt in dat de verwerking van de persoonsgegevens noodzakelijk is voor het (onderwijs)belang van de instelling, externe partij of individuen én dat er maximaal rekening wordt gehouden met de privacy van de individuen.
Cameratoezicht is een goed voorbeeld: je kunt moeilijk iedereen die door een gebouw wandelt om toestemming vragen, maar de noodzaak voor het specifieke belang "toezicht en beveiliging" is evident. In dat geval volstaat een waarschuwingsbordje en een reglement dat aangeeft wat er gebeurt met de beelden. Bovendien mag dan niet worden gefilmd op locaties waar de privacy zwaar weegt, zoals in kleedruimtes of op toiletten.

De instelling kan zich op de 'gerechtvaardigd belang'-grondslag baseren als:

- de instelling, een externe partij of de individuen een duidelijk omschreven gerechtvaardigd belang heeft, ofwel voordeel;
- de learning-analytics-verwerking noodzakelijk is om dit gerechtvaardigde belang te behartigen. Dat betekent dat, zoals eerder beschreven, je als instelling moet nagaan of het belang van de verwerking in verhouding staat tot de inbreuk op de privacy van de individuen en of de instelling het doel niet op een voor de betrokken personen minder nadelige manier kan bereiken;
- de instelling een afweging heeft gemaakt tussen de (onderwijs)belangen en die van de individuen en deze te documenteren. Ook moet de instelling hierbij eventueel maatregelen treffen om ervoor te zorgen dat de rechten en vrijheden van de individuen niet zwaarder wegen dan het gerechtvaardigd belang. Daarbij moet rekening worden gehouden met de redelijke verwachtingen van de individuen op basis van hun verhouding met de instelling. Aan een beroep op deze grond worden hoge eisen gesteld, een instelling moet bijvoorbeeld de afweging publiceren (bijvoorbeeld op haar website) en individuen in principe altijd een recht van bezwaar (een opt-out) bieden.

Tip

Voer de afweging van belangen voor de grondslag 'gerechtvaardigd belang' uit met hulp van een '*Legitimate Interest Assessment*' of met de uitleg van de Autoriteit Persoonsgegevens.

3.2 Data Protection Impact Assessment (DPIA) voor learning analytics

De AVG bepaalt dat organisaties, naast het toepassen van een grondslag, in bepaalde situaties ook verplicht zijn een gegevensbeschermingseffectbeoordeling of *Data Protection Impact Assessment* (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen, en om daarna maatregelen te kunnen nemen om de risico's te verkleinen. Ook toon je met het documenteren aan dat je als instelling aan de juridische vereisten hebt voldaan voor de verwerking.

Ook al is een DPIA niet in alle gevallen verplicht, het is raadzaam om het in een learning-analytics-traject uit te voeren. Niet alleen draagt een DPIA bij aan bewustwording van de gevolgen van het gebruik van gegevens, er is ook vaak sprake van *profiling* of van een hoog privacyrisico voor de individuen waardoor het uitvoeren verplicht is. SURF adviseert elke instelling die learning analytics inzet een DPIA uit te voeren. Zie ook de uitleg van de Autoriteit Persoonsgegevens over DPIA's.

Let op

In veel gevallen zal het gebruik van learning analytics te categoriseren zijn als *profiling*. Profiling is een van de verplichte verwerkingen op de lijst van de Autoriteit Persoonsgegevens en wordt als volgt omschreven: "*Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering). Bijvoorbeeld beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag.*"

- **Lees meer over een Data Protection Impact Assessment op de website van de Autoriteit Persoonsgegevens**
- **Zie ook de Nederlandse vertaling van de richtlijnen over profiling**

3.3 Hoe voer je een DPIA uit?

Er zijn verschillende methodes om een DPIA uit te voeren. Je kunt er zelf een kiezen, als het maar aan de basisvereisten voldoet, zoals die in de AVG staan beschreven. Die basisvereisten zijn een systematische beschrijving van de gegevensverwerking die je gaat doen, een oordeel over de noodzakelijkheid en evenredigheid van learning analytics met het oog op het vastgestelde doel, een beoordeling van de privacyrisico's voor de individuen en de maatregelen om de risico's aan te pakken. Het is vervolgens aan de instelling om die maatregelen ook daadwerkelijk te treffen. Bovendien moet je het advies van de Functionaris Gegevensbescherming (FG) inwinnen. Dit geeft extra zekerheid dat de DPIA voldoende zicht geeft op de risico's en er voldoende maatregelen worden getroffen om deze af te dekken.

Als uit de DPIA naar voren komt dat learning analytics een hoog risico oplevert én het lukt je als instelling niet om (voldoende) maatregelen te vinden om dit risico te beperken, dan moet je met de Autoriteit Persoonsgegevens overleggen voordat je met learning analytics kunt starten.

Tip

- **Er zijn (Data) Protection Impact Assessment-modellen en risicoformulieren opgesteld door SURF**
- **Daarnaast zijn er voorbeelden van DPIA-templates van toezichthouders te gebruiken of aan te passen (in het Engels):**
  - Commission Nationale de l'Informatique et des Libertés (CNIL)
  - Information Commisioner's Office (ICO)

3.4 Bepaal de impact van learning analytics (risicobeoordeling)

De toepassing van learning analytics moet in lijn zijn met de doelstellingen en de maatschappelijke richtlijnen van de instelling zelf. De waarden die je als instelling nastreeft, de relatie met studenten, duurzaamheid, diversiteit et cetera, moeten gereflecteerd worden in het learning-analytics-systeem. Een belangrijk onderdeel van de DPIA is een risicobeoordeling.

Wanneer je learning analytics inzet voor het realiseren van een bepaald doel, dan is dit met de gedachte om voordelen te realiseren voor de instelling en het individu. Bij voordelen kun je denken aan zaken als vrijheid, welzijn, duurzaamheid, inclusiviteit en diversiteit, gelijkheid, passende dienstverlening, eerlijkheid, efficiëntie en kostenreductie.

Beschrijf de voordelen voor de instelling en het individu
Voordelen van learning analytics kunnen op verschillende niveaus en voor verschillende partijen bestaan. Zo zal de instelling die de learning analytics toepast dit wellicht doen met het oog op het realiseren van het reduceren van kosten, hand in hand gaan met het realiseren van beleids-, onderwijs- of onderzoeksdoelstellingen.

Beschrijf de risico's voor de instelling en het individu
Als instelling ben je verplicht passende maatregelen te treffen om de risico's van learning analytics te beperken. In de praktijk betekent dit dat je de risico's die door learning analytics ontstaan, voortdurend moet beoordelen om te kunnen vaststellen wanneer er privacyrisico's zijn voor individuen. Een "risico" is een scenario dat een gebeurtenis en de gevolgen ervan beschrijft, ingeschat naar de ernst en de waarschijnlijkheid. Als instelling moet je deze risico's beheren door activiteiten te coördineren om de organisatie te sturen en maatregelen te implementeren.

Als onderdeel van de DPIA moet je als instelling onderzoeken of de geplande maatregelen, waarborgen en mechanismen om de belangen van individuen te beschermen voldoende zijn, dan wel of hier nog verbeteringen in kunnen worden doorgevoerd waarmee de risico's voor betrokkene verder worden beperkt. Houd daarom rekening met de mogelijke impact op individuen en eventuele schade die de verwerking kan veroorzaken - hetzij fysiek, emotioneel of materieel. Kijk in het bijzonder of learning analytics een risico vormt voor:

- de onmogelijkheid om rechten uit te oefenen (zoals privacyrechten)
- weigering tot diensten of ontzegging van andere onderwijsmogelijkheden
- verlies van controle over het gebruik van persoonsgegevens
- discriminatie
- identiteitsdiefstal of fraude
- financieel verlies
- reputatieschade
- fysieke schade
- verlies van vertrouwelijkheid
- heridentificatie van gepseudonimiseerde gegevens, of
- ander belangrijk economisch of sociaal nadeel

3.5 Bepaal de risicobeperkende maatregelen

Zodra alle risico's in kaart zijn gebracht moet je als instelling de beoogde maatregelen beschrijven om deze risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan de AVG is voldaan.

Registreer de bron van elk geïdentificeerd risico, of mogelijk nadeel. Overweeg dan de mogelijkheden om dat risico te verminderen. Bijvoorbeeld:

- beslissen om bepaalde soorten gegevens niet te verzamelen
- het beperken van de reikwijdte van de verwerking
- het verkorten van de bewaartermijnen
- het nemen van aanvullende technologische beveiligingsmaatregelen
- het opleiden van het personeel om ervoor te zorgen dat op risico's wordt geanticipeerd en beheerd
- het anonimiseren of pseudonimiseren van gegevens waar mogelijk
- het schrijven van interne richtlijnen of processen om risico's te vermijden
- het gebruik van een andere technologie
- het sluiten van duidelijke afspraken over het delen van gegevens (zie 'Verwerkersovereenkomst')
- het aanbrengen van wijzigingen in privacyverklaringen (zie 'Informeren')
- het geven van een redelijke mate van controle aan individuen over de gegevens die de instelling van hen verwerkt. Wellicht kun je zelfs de vastgestelde doelen bereiken door enkel en alleen de individuen toegang tot de gegevens en de conclusies van learning analytics geven
- individuen de mogelijkheid bieden om, waar nodig, af te zien van deelname aan het project (opt-out), of
- het invoeren van nieuwe systemen om personen te helpen hun rechten uit te oefenen.

Dit is geen uitputtende lijst, meer informatie vind je in de officiële Nederlandse vertaling van de DPIA-guidelines. Vraag ook de Functionaris Gegevensbescherming (FG) om advies. Leg vast of de maatregelen het risico verminderen of wegnemen. Je kunt rekening houden met de kosten en baten van elke maatregel wanneer je beslist of deze wel passend zijn.

3.6 Uitkomst DPIA

Zodra alle informatie is verwerkt in de DPIA is het belangrijk om het advies in te winnen van FG binnen de instelling. Dit geeft extra zekerheid dat de DPIA voldoende zicht geeft op de risico's en er voldoende maatregelen worden getroffen om deze af te dekken. Dat advies moet samen met de beslissing van de instelling om al dan niet door te gaan met het learning-analyticstraject gedocumenteerd worden. Daarnaast is het raadzaam om de individuen, bijvoorbeeld studentenvertegenwoordiging, te vragen naar hun mening over het project.

Tip

Leg de resultaten van de DPIA voor aan de Functionaris Gegevensbescherming (FG) en/of de interne juridische afdeling voor een finale review.

Wanneer uit de DPIA blijkt dat de voorgenomen verwerking een hoog risico voor de individuen inhoudt, en dat dit risico niet wordt weggenomen door het treffen van risicobeperkende maatregelen, dan moet de instelling met de Autoriteit Persoonsgegevens overleggen voordat je met de verwerking start. Dit wordt een 'voorafgaande raadpleging' genoemd. Zie voor meer informatie de website van de Autoriteit Persoonsgegevens.

STAP 4: REALISATIE

Als de uitkomst van de beoordeling positief is, de rechtmatigheid van het learning-analytics-traject is vastgesteld en er geen hoge restrisico's aan het licht zijn gekomen, is het tijd om de nodige juridische, technische en organisatorische maatregelen te treffen.

4.1 Sluit de noodzakelijke contracten af

In de ontwerpende fase (stap 2) heb je in kaart gebracht welke leveranciers en andere derde partijen betrokken zijn bij het learning-analytics-systeem. Direct daarna heb je bepaald welke partijen welke privacyrechtelijke rollen vervullen (verwerkingsverantwoordelijke / verwerker). Aan de hand van die informatie moet je als instelling regelingen treffen en overeenkomsten sluiten.

Gezamenlijke Verantwoordelijkenovereenkomst opstellen

Als je als instelling het doel van en de middelen voor de learning analytics-verwerking samen met anderen bepaalt, is er sprake van gezamenlijke verantwoordelijkheid. Gezamenlijke verantwoordelijken moeten een onderlinge regeling met elkaar treffen waarin zij op transparante wijze hun verantwoordelijkheden vastleggen voor naleving van de AVG. Het gaat daarbij met name om de uitoefening van de rechten van de individuen en om wie er informeert over de learning analytics. De essentie van deze regeling moet ook beschikbaar zijn voor de individuen.

Tip

- SURF heeft een modeldocument voor de Gezamenlijke Verantwoordelijkenovereenkomst.
- Bekijk ook de Impact en Riskassessment-portal van SURF

Verwerkersovereenkomst opstellen

Een verwerkersovereenkomst beschrijft de relatie tussen een dienstverlener (de verwerker) die in opdracht van een ander (de verwerkingsverantwoordelijke) persoonsgegevens verwerkt. Deze overeenkomst is verplicht. Grote leveranciers hebben vaak een eigen model. Een verwerker mag alleen persoonsgegevens verwerken waartoe hij opdracht heeft van de verwerkingsverantwoordelijke op basis van de verwerkersovereenkomst. Let goed op of de learning-analytics-verwerking en de doeleinden helder zijn beschreven in de verwerkersovereenkomst.

Tip

SURF heeft samen met de instellingen een model-Verwerkersovereenkomst opgesteld als onderdeel van het SURF Juridisch Normenkader (Cloud)services. Dit document stelt normen op op het gebied van vertrouwelijkheid, privacy, eigendom en beschikbaarheid voor (cloud)leveranciers.

Toegang tot persoonsgegevens buiten de Europese Economische Ruimte: aanvullende maatregelen

Als instelling ben je niet verplicht om persoonsgegevens bij partijen in Europa op te slaan, maar juridisch is het wel een stuk makkelijker. De AVG garandeert namelijk in ieder land in de Europese Unie dezelfde gegevensbescherming voor individuen. Maar voor de doorgifte

van persoonsgegevens naar partijen buiten Europese Unie - naar entiteiten in zogeheten derde landen - gelden aparte regels. Derde landen zijn alle landen buiten de EU plus Noorwegen, Liechtenstein en IJsland (de Europese Economische Ruimte). Naar waarschijnlijkheid wordt ook het Verenigd Koninkrijk zo'n derde land met aparte regels vanwege Brexit.

De hoofdregel bij derde landen is dat een organisatie persoonsgegevens alleen mag doorgeven als er sprake is van een passend beschermingsniveau. De Europese Commissie heeft een zogenaamde Landenlijst opgesteld van derde landen waarvan besloten is dat deze landen een passend beschermingsniveau bieden. Naast de hierboven genoemde gevallen is internationale doorgifte slechts toegestaan op basis van een wettelijke bepaling uit de AVG, zoals het garanderen van een beschermingsniveau met contractuele bepalingen (modelcontracten ofwel '*Standard Contractual Clauses*') of een aangewezen manier door de Europese Commissie (zoals '*Privacy Shield*', een certificaat voor partijen in de Verenigde Staten die Europese persoonsgegevens ontvangen). Controleer daarom de afspraken met de relevante partijen en bepaal of deze moeten worden verduidelijkt of herzien.

Controleer daarom welke oplossing partijen in derde landen hanteren om de doorgifte van persoonsgegevens mogelijk te maken. Zie meer informatie van de Autoriteit Persoonsgegevens over internationaal verkeer.

4.2 Stel de benodigde beleidsdocumenten en procedures op

Inventariseer bij welk beleid learning analytics kan aansluiten. Bepaal de juiste vervolgstappen als je instelling nog geen relevant beleid heeft.

- Beveiligingsbeleid, waaronder identitymanagement van gebruikers, zie ook de SURF publicaties over beveiliging.
- Procedure voor het omgaan met datalekken om te kunnen voldoen aan de meldingsplicht bij een datalek. Als een datalek optreedt, moet je dit als instelling namelijk in bepaalde gevallen melden. Bepaal of er sprake is van een datalek dat je moet melden bij de toezichthouder en eventueel aan de betrokkenen.
- Procedure voor het omgaan met (inzage- en verwijder)verzoeken van individuen.

4.3 Informeer de individuen over de learning-analytics-verwerking

Wie persoonsgegevens verwerkt, moet de betreffende persoon duidelijk informeren over wat er met de gegevens gebeurt en waarom. Deze informatie moeten de individuen ontvangen voor of op het moment dat de instelling de persoonsgegevens verwerkt.

In een privacyverklaring leg je als instelling uit aan de individuen, zoals de studenten, wat er gebeurt met hun persoonsgegevens. De manieren waarop de instelling de gegevens gebruikt, kunt je daarbij in categorieën verdelen. Beoordeel in welke mate je als instelling transparant kan zijn over learning analytics. Het doel van transparantie is de uitlegbaarheid van het gebruik en de werking van learning analytics. Naast het bestaan en de werking hiervan is het ook relevant om de gevolgen van de toepassing van de learning analytics inzichtelijk te maken. In de privacyverklaring leg je de individuen uit wat learning analytics precies is, welke gegevens de instelling voor dit doel gebruikt en op welke manier learning analytics tot zijn conclusies komt en welke gevolgen dit heeft. Bijvoorbeeld: "We monitoren de tijd die je nodig hebt voor de online-oefeningen. Als die significant langer is dan gemiddeld, dan krijg je extra uitleg en oefeningen die je moet doorlopen voordat je deze module kunt afsluiten."

Het is belangrijk dat een individu de privacyverklaring en, waar nodig, de cookieverklaring, gemakkelijk kan opvragen voordat zijn gegevens worden verwerkt. Kennisname is niet verplicht en je hoeft individuen ook niet te dwingen om de privacyverklaring te lezen. Het is niet nodig om individuen te laten verklaren, bijvoorbeeld met een vinkje, dat zij akkoord zijn met de privacyverklaring.

Wanneer de instelling zich beroept op toestemming als grondslag, dan kan een individu toestemming geven door een toestemmingsverklaring aan te vinken. Die verklaring moet dan wel duidelijk maken waarvoor de student toestemming geeft, zie ook de grondslag 'Toestemming' in paragraaf 3.1.

4.4 Beveiligings- en risicobeperkende maatregelen

Pas de beschreven beveiligingsmaatregelen toe om de vertrouwelijkheid, integriteit en beschikbaarheid van de persoonsgegevens te garanderen. Implementeer ook de aanvullende risicobeperkende maatregelen uit paragraaf 3.5. Controleer vervolgens of de maatregelen het gewenste effect hebben.

4.5 Overige maatregelen

Implementeer een recht op bezwaar bij profiling

Een individu mag altijd een bezwaar indienen wanneer hij onderworpen is aan profiling of getroffen wordt door een maatregel die gebaseerd is op zijn persoonlijkheidsprofiel. De bezwaarmogelijkheid moet je expliciet kenbaar maken aan het individu. De persoon die het bezwaar ontvangt, moet vervolgens de maatregel ongedaan kunnen maken. Als de medewerking van een softwareleverancier nodig is om een actie van het learning-analytics-systeem ongedaan te maken, moet je hiervan tevoren afspraken over hebben gemaakt met de leverancier (in de verwerkersovereenkomst).

Communicatie

Bepaal of je als instelling op basis van learning-analytics nog andere maatregelen moet treffen en voer die uit. Denk aan zaken als het:

- instellen communicatieprocedure of -loket bij vragen van individuen en andere stakeholders
- inrichten van een informatiewebsite met een FAQ
- geven van trainingen aan gebruikers van het learning-analytics-systeem.

4.6 Pilot

Overweeg een pilotfase te organiseren om te testen of alle functionaliteiten correct werken. Na de pilot kun je de werking goed- of afkeuren. Bij acceptatie kan je learning analytics grootschaliger uitrollen als afsluiting de realisatiefase.

STAP 5: EVALUATIE

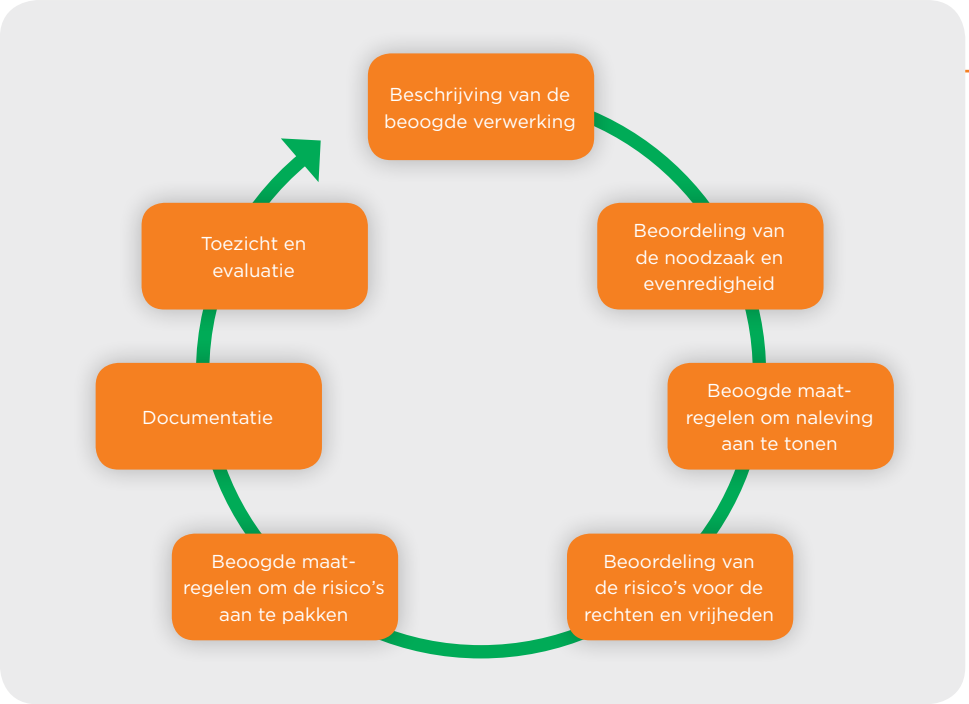
5.1 Evalueer periodiek

Het beoordelen of een learning-analytics-systeem privacyrechtelijk verantwoord is, is geen eenmalig proces. De organisatie en de buitenwereld veranderen. Dat heeft wellicht invloed op de maatschappelijke en juridische kaders van het systeem en daarmee op de legitimiteit. Daarom is het van belang periodiek te evalueren of het systeem nog steeds verantwoord is. Door periodiek te evalueren ontdek je nieuwe risico's op tijd en creëer je een feedbackloop die de toepassing van learning analytics beter en effectiever maakt.

Een evaluatie kan plaatsvinden met een zekere tijdsinterval (bijvoorbeeld elk jaar), maar het is verstandig om ook situaties te herkennen die leiden tot een herevaluatie. Denk bijvoorbeeld aan:

- Het learning-analytics-systeem wordt ingezet voor een ander doel dan waarvoor het oorspronkelijk is bedoeld
- Er worden nieuwe databronnen of nieuwe technologie gebruikt
- Bestaande databronnen worden aangepast of niet meer gebruikt.

Verbeter in zulke situaties het proces en loop dit stappenplan waar nodig opnieuw door. Het stappenplan uitvoeren is namelijk geen eenmalige opdracht, maar een continu proces.



Bron: Visual uit de DPIA-opinie van de EPDB, p. 20.

5.2 Publiceer ervaringen

Denk na over het opslaan en delen van je werkwijze. Hoe zorg je dat docenten de beschrijving het learning-analyticstraject weten te vinden en welke privacy-afwegingen zijn gemaakt? Specialisten maken bijvoorbeeld vaak gebruik van een communityplatform waarop je de werkwijze kunt plaatsen, zoals de Privacy-wiki van SURF. Of gebruik een interne portal van je instelling.

COLOFON

Samenstelling & redactie
Niels Westerlaken, *Project Moore*
Jocelyn Manderveld, *SURF*
Floortje Jorna, *SURF*

Met dank aan
Arnoud Engelfriet, *ICT Recht*
Evelijn Jeunink, *SURF*
Sebas Veeke, *SURF*

Projectleiding
Jocelyn Manderveld, *SURF*
Marieke de Wit, *SURF*

Vormgeving
Vrije Stijl, Utrecht

Drukwerk
Drukkerij Libertas Pascal

Foto omslag
Annemiek van der Kuil, PhotoA.nl

Foto's binnenwerk
p. 10, 21: Sicco van Grieken, Erasmus Universiteit Rotterdam
p. 18: Sicco van Grieken, Wageningen University & Research

Mei 2019

SURF
088 – 787 30 00
www.surf.nl/onderwijs
onderwijsinnovatie@surf.nl

Samen aanjagen van vernieuwing

Universiteiten, hogescholen, mbo-instellingen, onderzoeks-instellingen en universitaire medische centra werken binnen SURF aan ICT-voorzieningen en -innovaties. Met als doel: beter en flexibeler onderwijs en onderzoek. Dat doen we door de best mogelijke digitale diensten te leveren, kennisdeling en -uitwisseling te stimuleren en vooral door steeds te blijven innoveren! Hiermee dragen we bij aan een sterke en duurzame Nederlandse kenniseconomie.

SURF