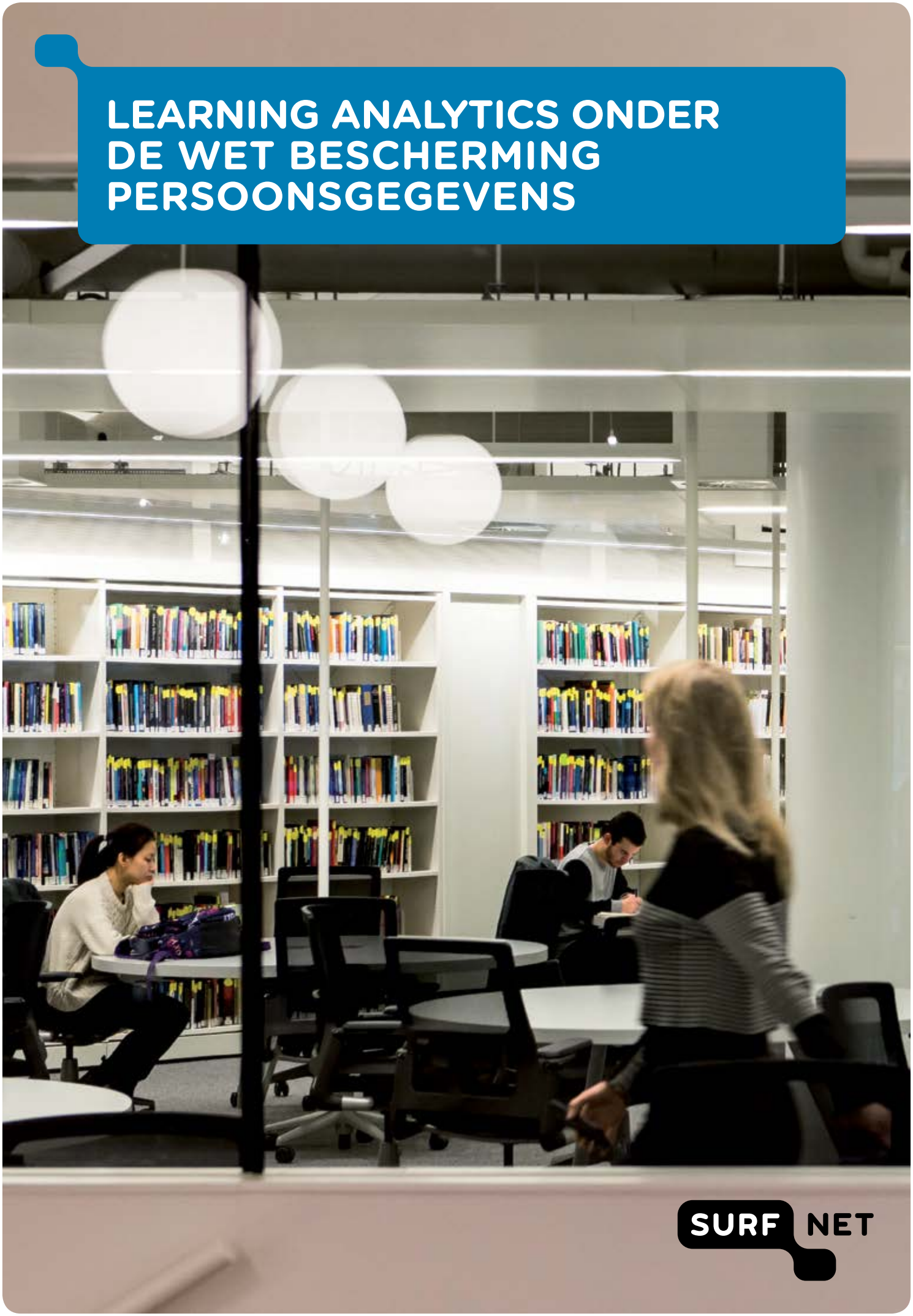
LEARNING ANALYTICS ONDER DE WET BESCHERMING PERSOONSGEGEVENS



SURF NET

INHOUDSOPGAVE

LEARNING ANALYTICS EN PRIVACY

Learning analytics is het verzamelen en analyseren van data uit leeromgevingen om het leerproces van studenten te verbeteren. Deze informatie wordt vervolgens beschikbaar gemaakt voor verschillende stakeholders, zoals de student zelf, de docent of opleidingsmanagement. Daarmee kunt u het onderwijs beter begrijpen en verbeteren. Maar bij het verzamelen en analyseren van gegevens worden persoonsgegevens verwerkt: gegevens die direct of indirect iets zeggen over studenten. Wanneer een onderwijsinstelling persoonsgegevens verwerkt, is daarop de Wet bescherming persoonsgegevens (Wbp) van toepassing. Wat zegt deze wet over learning analytics?

In deze handreiking leest u waarop u moet letten als u studentgegevens verzamelt om het onderwijs te verbeteren. Allereerst maken we duidelijk wat persoonsgegevens zijn en wat u ermee mag doen. Vervolgens gaan we in op de eisen waaraan u moet voldoen als u persoonsgegevens wilt verzamelen. We gaan in op de randvoorwaarden bij verwerking en op uw verplichtingen, bijvoorbeeld de informatieplicht en de beveiliging. Verder leest u waarop u moet letten als u gebruik maakt van de diensten van andere partijen. Ook de eisen aan de gegevensopslag komen aan de orde. Deze handreiking sluit af met een stappenplan.

Het is belangrijk te beseffen dat de inzet van learning analytics juridisch gezien niet eenvoudig is. Het is geen kwestie van een keer toestemming vragen en een privacyverklaring opnemen op de site. De Wbp stelt hoge eisen aan de grondslagen voor inzet van learning analytics en de informatievoorziening; deze moet op maat zijn voor de student gezien de tools die u als onderwijsinstelling wilt inzetten.

WAT ZIJN PERSOONSGEGEVENS?

Persoonsgegevens zijn onder de Wbp alle gegevens die direct of indirect herleidbaar zijn tot een persoon. Een naam of adres is een persoonsgegeven, maar ook gegevens over gedrag vallen hieronder. Bijhouden wat iemand in een leeromgeving doet, is dus een vorm van persoonsgegevens verzamelen. En steeds als u langs elektronische weg persoonsgegevens verzamelt of gebruikt, geldt de Wbp.

Direct of indirect herleidbaar

Als gegevens direct of indirect tot een persoon te herleiden zijn, zijn het persoonsgegevens. Het gaat dus niet alleen om namen of contactgegevens. Een studentnummer is bijvoorbeeld ook een persoonsgegeven, want het is aan een persoon te koppelen. Alleen als de koppeling redelijkerwijs onmogelijk is, zijn de gegevens niet langer persoonsgegevens te noemen. Bijvoorbeeld als willekeurige nummers zijn toegekend en de lijst met naam-nummerkoppeling is vernietigd.

Maar een persoon kan ook vaak via andere gegevens worden achterhaald. Een verzameling van iemands tentamencijfers en vakken is uniek voor die persoon, geen twee studenten halen in hetzelfde jaar voor hetzelfde vakkenpakket dezelfde cijfers. Die verzameling vormt dan een set persoonsgegevens, ook als de naam van de student er niet bij staat.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn gegevens over zaken als iemands gezondheid, etnische afkomst, seksuele voorkeur, politieke voorkeur of godsdienst. Deze gegevens mag u normaal niet verzamelen of gebruiken. Dit mag alleen met uitdrukkelijke aparte toestemming of als het gebruik in een wet is geregeld. Uitdrukkelijke toestemming houdt in dat u apart vraagt naar dit gegeven en uitlegt waarom (met de mogelijkheid nee te zeggen).

Zo mag een studentenkerk vastleggen wie haar diensten bijwoont, hoewel dit een vastlegging van godsdienst is. Maar in een enquête om de studenten beter te leren kennen, mag u deze vraag niet stellen. Dat mag ook niet als u de optie ‘Geen mening/ Weiger te beantwoorden’ opneemt. Is een handicap relevant voor de studie, kan kunt u daar wél naar vragen. Denk aan dyslexie, omdat dan extra tijd voor een tentamen nodig is.

Het BurgerServiceNummer is ook een bijzonder soort persoonsgegeven: dit mag u 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. Maar u kunt ook onbedoeld bijzondere persoonsgegevens vragen. Bijvoorbeeld als u vraagt of studenten op zondag een toets willen maken. Wie daar nee op zegt, kan daar een godsdienstige reden voor hebben.

Wanneer is een gegeven geen persoonsgegeven meer?

U kunt gegevens hun status als persoonsgegeven laten verliezen door ze te aggregeren: u voegt ze dan samen tot uitspraken over meerdere personen. ‘Tachtig procent van de studenten haalde een onvoldoende voor deze toets’ is bijvoorbeeld geen persoonsgegeven. Aan dergelijke statistische gegevens stelt de wet geen eisen. Wanneer wordt een persoonsgegeven een statistisch gegeven? Hiervoor zijn geen harde regels. Een veelgehoorde vuistregel is dat gegevens van minstens vijf personen gecombineerd moeten worden. Andere bronnen (zoals het Centraal Bureau voor de Statistiek) gaan uit van minstens twaalf personen. Waar het om gaat, is dat er écht geen gegevens over individuele personen terug te vinden zijn. Als bijvoorbeeld alle vijf studenten man zijn en eerstejaars Natuurkunde, dan is deze informatie ook na aggregatie nog aanwezig. Wanneer een geaggregeerde uitspraak over nul of honderd procent van de populatie gaat, is deze nog steeds een persoonsgegeven.

Met geaggregeerde gegevens mag u doen wat u wilt. Maar de brongegevens zijn persoonsgegevens waarop de Wbp van toepassing is. Een operatie waarbij men uitkomt bij geaggregeerde gegevens valt dus niet buiten de Wbp. Alleen bewerkingen en analyses waarbij u start met geaggregeerde gegevens vallen buiten deze wet. Als een docent bijvoorbeeld bij een online leerplatform meet hoe snel studenten door de stof gaan, is daarvoor een wettelijke grondslag nodig. Dat geldt ook als hij alleen statistische uitspraken doet over zijn bevindingen.

WANNEER MAG U PERSOONSGEGEVENS VERWERKEN?

Ieder gebruik van persoonsgegevens wordt ‘verwerken’ genoemd in de Wbp. U mag alleen persoonsgegevens verwerken als u aan een of meer eisen in deze wet voldoet: de grondslagen. Hieronder noemen we de grondslagen die van belang zijn bij learning analytics:

- toestemming
- uitvoering overeenkomst
- wettelijke plicht
- uitvoering overheidstaak
- eigen dringende noodzaak

Toestemming

De meest gebruikte grondslag is toestemming van de persoon wiens gegevens u verzamelt. Wilt u daar gebruik van maken? Dan moet u eerst uitleggen wat u gaat doen en waarom. Pas daarna kunt u een student vragen of hij dat wel wil. Voor meer informatie, zie Informatieplicht.

Toestemming moet in vrijheid worden gegeven. Studenten 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. Wilt u in een bepaald vak gebruik maken van een online tool met learning analytics? Vraag dan toestemming vóór de inschrijving. Als de studenten al zijn ingeschreven, is weigeren niet meer realistisch. Zorg dat de toestemming specifiek is geformuleerd. ‘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. Hierbij krijg ik studieadvies op maat. De studiebegeleider krijgt deze gegevens om mij proactief te kunnen aanspreken op risico’s voor vertraging.’

U kunt in één keer toestemming vragen voor meerdere vakken, voor een studiejaar of zelfs voor een opleiding. U hoeft dus geen toestemming per vak te vragen. Wel moet bij zo’n brede toestemming ook breed geïnformeerd worden. Op welke vakken heeft de toestemming betrekking, hoe ver gaat per vak de monitoring en wat zijn per vak de gevolgen? Dit stelt hoge eisen aan de informatieplicht. Studenten kunnen pas toestemming geven nadat adequate informatie is verstrekt. U kunt ook een korte uitleg (enkele zinnen) geven met een link naar de privacyverklaring waarin meer informatie te lezen is. Het is niet voldoende om een zin over de toestemming in gebruiksvoorwaarden, algemene voorwaarden of privacy-verklaringen op te nemen. Wel kunt u voor uitleg over de toestemming naar die documenten verwijzen. Zie verder, Informatieplicht.

De toestemming kan worden ingetrokken. Vanaf dat moment mogen de verwerkingen niet meer worden uitgevoerd. Intrekken van de toestemming kan op ieder moment en zonder opgaaf van redenen, maar het moet wel redelijk zijn om de toestemming in te trekken.

Uitvoering overeenkomst

Als twee partijen een overeenkomst (contract) hebben afgesloten, mogen ze elkaars persoonsgegevens verwerken als dat nodig is voor een goede uitvoering van die overeenkomst. Ze hoeven daar dan niet apart toestemming voor te vragen. Zo mag een webwinkel persoonsgegevens van een klant aan een koerier geven, omdat dat nodig is om de bestelling te bezorgen. Wil de webwinkel de klant ook een nieuwsbrief sturen, dan is daar wél toestemming voor nodig. Die nieuwsbrief is namelijk niet noodzakelijk voor het afhandelen van de bestelling. Deze grond geldt al vanaf het moment dat de partijen onderhandelen over de overeenkomst.

Een onderwijsinstelling heeft over het algemeen geen overeenkomst met de student. Sommigen zien de inschrijving aan de instelling als een overeenkomst, maar dat is strikt juridisch niet juist. U kunt natuurlijk wel studenten overeenkomsten laten aangaan waarin learning analytics is opgenomen. Denk aan een afstudeeropdracht of stage.

De gegevens moeten wel noodzakelijk zijn voor de uitvoering van de overeenkomst. Dat is strenger dan ‘wenselijk’ of ‘handig’. Noodzakelijk houdt in dat de overeenkomst eigenlijk niet kan worden nagekomen zonder gebruik van deze persoonsgegevens. De onderwijsinstelling moet aantonen dat het noodzakelijk is om learning analytics in te zetten. Omdat learning analytics zeer nieuw is, kan het snel als niet noodzakelijk worden gezien. De zienswijze is dan dat onderwijs prima zonder learning analytics kan worden gegeven. Dit is een kip-ei probleem: pas als duidelijk is dat onderwijs zonder learning analytics tekort schiet, kan dit als noodzakelijk worden gepresenteerd. Maar dat kan pas als learning analytics zijn waarde over meerdere jaren heeft bewezen.

Wettelijke plicht

Als derde grondslag noemt de Wbp de wettelijke plicht. Gegevens mogen worden verwerkt als er een wet is die daartoe verplicht. Een onderwijsinstelling kan het standpunt innemen dat zij verplicht is het best mogelijke onderwijs te verzorgen. 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 als bij Uitvoering overeenkomst. Men moet kunnen onderbouwen dat dit nieuwe middel echt nodig is en dat er geen reëel alternatief (meer) is.

Uitvoering overheidstaak

Een instelling voor hoger onderwijs is te zien als een overheidsinstelling. Het leveren van onderwijs zou dan een overheidstaak in de zin van de Wbp zijn. In dat geval mogen persoonsgegevens die nodig zijn voor die onderwijstaak worden verzameld en gebruikt. Ook hier geldt dat ‘noodzaak’ een hoge lat is die u moet kunnen rechtvaardigen.

Dringende noodzaak

Als laatste grondslag noemt de wet de grondslag ‘eigen dringende noodzaak’. Deze grondslag houdt in dat er geen toestemming kan worden gevraagd, dat de verwerking van de gegevens absoluut noodzakelijk is én dat er maximaal rekening wordt gehouden met de privacy.

Een beroep op deze grond is alleen mogelijk als er een duidelijke opt-out is. Wanneer de mogelijkheid bestaat om toestemming te vragen, mag men deze vraag niet omzeilen door een dringende noodzaak aan te dragen. Cameratoezicht is het bekendste voorbeeld: men kan moeilijk iedereen die door een gebouw wandelt om toestemming vragen, maar de noodzaak van 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 toiletten).

Voor learning analytics is een case te maken onder deze grondslag, omdat een instelling immers moet kunnen nagaan hoe studenten presteren. Maar de vraag is wel of het niet mogelijk is om toestemming te vragen. Bovendien gaan veel learning analytics-tools buitengewoon diep in het verzamelen en combineren van data, wat als een zware inbreuk op de privacy gezien kan worden. Dat maakt het niet eenvoudig om een noodzaak aan te tonen die zwaarder weegt dan de privacy. Bovendien is de eis van een opt-out lastig te realiseren.

Wetenschappelijk en statistisch onderzoek: geen grondslag

De verwerking van persoonsgegevens voor wetenschappelijk onderzoek of statistiek is geen wettelijke grondslag. U kunt alleen gegevens verzamelen en verwerken op basis van een van de genoemde vijf grondslagen. Vervolgens kunt deze gegevens ook gebruiken voor wetenschappelijk onderzoek of statistiek. Maar dat onderzoek moet dan wel aansluiten bij het doel waarvoor de gegevens zijn verzameld. Een voorbeeld:

1. Een docent zet een monitoringtool in bij een tentamen om te meten of herkansers anders presteren dan eerstekansers. Hiervoor is toestemming gevraagd. Vervolgens mogen de resultaten worden verwerkt in statistisch onderzoek naar succesfactoren bij dat tentamen. Dat geldt als verdere verwerking voor onderzoek.
2. De docent gebruikt de uitkomsten van het statistisch onderzoek ook om fraudeurs te herkennen. Dit mag niet, want dat gaat het doel van statistisch onderzoek te buiten. Dit zou wel mogen als het vooraf gemeld is en als het noodzakelijk is.

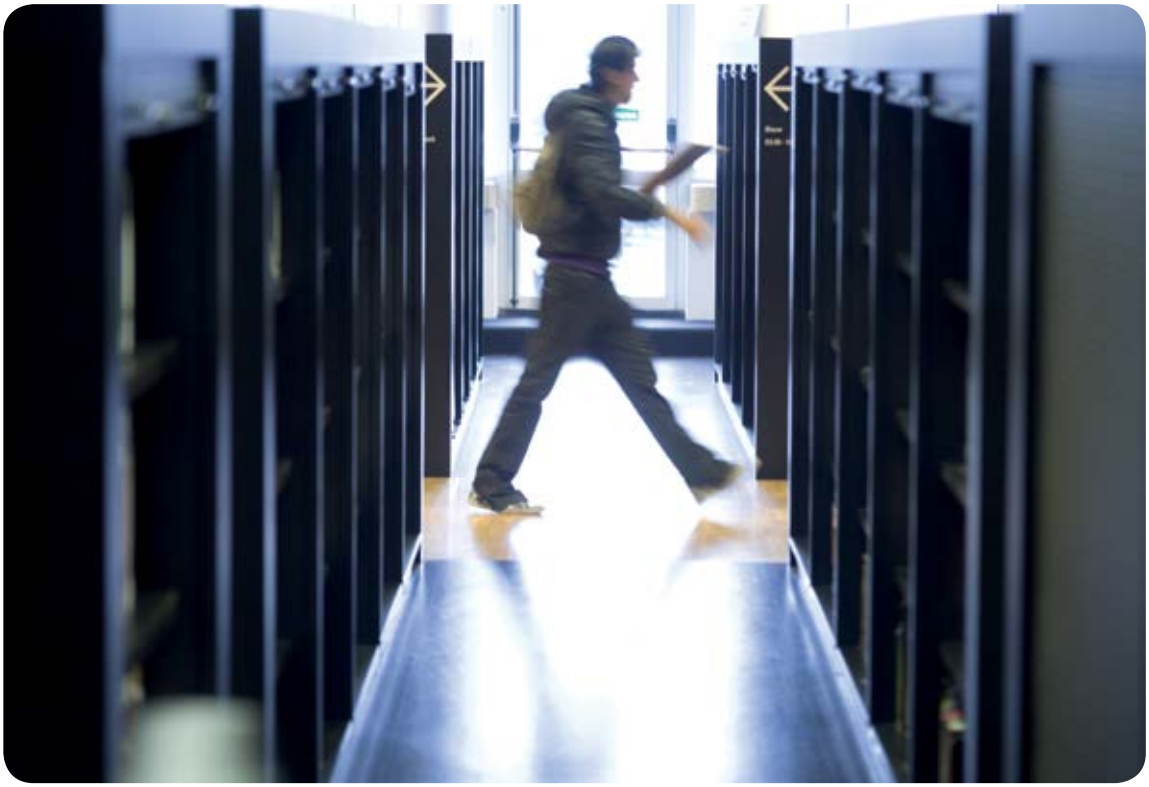
WELKE RANDVOORWAARDEN ZIJN VAN TOEPASSING?

Bij alle verwerkingen van persoonsgegevens stelt de Wbp een aantal randvoorwaarden. Deze zijn erop gericht de verwerking van persoonsgegevens eerlijk, transparant en begrijpelijk te houden. De belangrijkste randvoorwaarden zijn:

- Doelbinding: u mag gegevens alleen gebruiken voor het oorspronkelijke doel.
- Verenigbaarheid: u mag de gegevens alleen voor andere doelen gebruiken als deze verenigbaar zijn met het originele doel.
- Zorgvuldigheid: u moet persoonsgegevens zorgvuldig gebruiken en het gebruik kunnen rechtsvaardigen.
- Welbepaaldheid: u moet het gebruik van persoonsgegevens in detail kunnen uitleggen.

Doelbinding en verenigbaarheid

Doelbinding houdt in dat u gegevens alleen mag gebruiken voor het doel waarvoor ze zijn verkregen. 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 over de kwaliteit van de helpdesk sturen aan iemand die gebruik heeft gemaakt van die helpdesk.



Een doel moet specifiek en duidelijk omschreven zijn. De doelomschrijving moet duidelijk maken wat er gaat gebeuren. Een algemene doelomschrijving zoals 'kwaliteitsdoeleinden' bij opgenomen telefoongesprekken volstaat niet. Wat wordt daaronder verstaan en hoe worden die gegevens gebruikt? Wel correct zou zijn: 'Dit gesprek wordt opgenomen om in geval van conflicten te bewijzen wat er is gezegd'.

U mag informatie niet gebruiken voor een doel dat niet bij verkrijging van de informatie gemeld is. Dit maakt doelbinding een lastige eis bij learning analytics. 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 dus geen 'bepaald doel'. Daarom raden we aan om zo veel mogelijk doelen te benoemen in de verstrekte informatie en deze regelmatig te herzien.

Zorgvuldigheid

Persoonsgegevens moeten in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Het is dus niet toegestaan om onopgemerkt gegevens over personen te verzamelen en verwerken. 'Stiekeme' analytics zijn dus niet toegestaan.

Welbepaaldheid

Persoonsgegevens mag u alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzamelen. Dit houdt onder meer in dat u alle gebruik van persoonsgegevens in detail moet kunnen uitleggen. Bovendien moet die uitleg beschikbaar zijn (zie ook informatieplichten hieronder). Voor elk gebruik is een legitiem doel vereist. Tot slot moet bij het verzamelen al bekend zijn waarom men die gegevens verzamelt.

AAN WELKE VERPLICHTINGEN MOET U VOLDOEN?

Wanneer u gegevens van studenten vastlegt om het onderwijs te verbeteren, dan zijn er bepaalde verplichtingen waaraan u moet voldoen. Ook moet u rekening houden met de rechten van de student. In dit hoofdstuk leest u hier meer over.

Informatieplicht

Wie persoonsgegevens verwerkt, moet de betreffende persoon duidelijk informeren over wat er met de gegevens gebeurt en waarom. Deze informatie moet een student ontvangen voor of op het moment dat hij toestemming geeft om zijn gegevens te verwerken. Internetdiensten verstrekken deze informatie vaak in een privacyverklaring of privacy statement. Een privacyverklaring alleen volstaat niet, maar moet geïntegreerd worden. Een privacyverklaring vormt een aanvulling op de toestemmingsvraag of een toelichting wanneer u zich beroept op een andere grondslag dan toestemming, zoals uitvoering overeenkomst of eigen dringende noodzaak.

Inhoud van een privacyverklaring

In een privacyverklaring legt u aan studenten uit wat er gebeurt met hun persoonsgegevens. De manieren waarop u de gegevens gebruikt, kunt u daarbij in categorieën verdelen. In een privacyverklaring beschrijft u (per categorie):

- welke persoonsgegevens u ontvangt;
- op welke manier u deze gegevens ontvangt;
- welke instantie(s) hier toegang toe krijgen;
- voor welke doel(en) u de gegevens gebruikt;
- hoe dit gebruik in de praktijk verloopt.

Geautomatiseerde verwerking

Als u persoonsgegevens automatisch verwerkt, beschrijf dan in uw privacyverklaring welke logica u hanteert bij de verwerking van de gegevens. In de privacyverklaring voegt u een toelichting toe voor de student over wat learning analytics precies is, welke gegevens u voor dit doel gebruikt en op welke manier de tool tot zijn conclusies komt. 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.”

Kennisname en akkoord

Het is belangrijk dat een student de privacyverklaring gemakkelijk kan opvragen voordat zijn gegevens worden verwerkt. Kennisname is niet verplicht en u hoeft studenten niet te dwingen om de privacyverklaring te lezen. Het volstaat om de privacyverklaring vanaf de startpagina te linken, maar veel instellingen nemen een link naar de privacyverklaring op in de footer van elke webpagina.

Het is niet nodig om studenten te laten verklaren (bijvoorbeeld met een vinkje) dat zij akkoord zijn met de privacyverklaring. Wanneer u zich beroept op toestemming als grondslag, dan kan een student toestemming geven door een zin aan te vinken. Die zin moet dan wel duidelijk maken waarvoor de student toestemming geeft, bijvoorbeeld: “Deel mijn gegevens met de docent” en niet enkel verwijzen naar de privacyverklaring.

Beveiligingsplicht

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

‘Redelijkerwijs’ betekent dat de beveiliging niet perfect moet zijn. Het kan gebeuren dat u aan de wet voldoet en er toch persoonsgegevens worden misbruikt of ontvreemd. Uiteraard heeft u dan wel wat uit te leggen. Per 1 januari is het wettelijk verplicht om inbreuk op de beveiliging te melden bij de toezichthouder als deze inbreuk de betrokkenen ernstig kan benadelen. Onder het kopje ‘Meldingsplicht bij datalek’ leest u hier meer over.

Er bestaat nog geen algemeen geldende norm of standaard voor beveiliging van persoonsgegevens. In bepaalde branches gelden specifieke normen (zoals NEN 7510 in de zorg), maar in het onderwijs nog niet. Normenkaders van brancheorganisaties kunnen u helpen te bepalen of u de persoonsgegevens van studenten adequaat beveiligt, maar deze normenkaders zijn niet zaligmakend.

De privacytoezichthouder College Bescherming Persoonsgegevens heeft zogenoemde richtsnoeren gepubliceerd over hoe bedrijven en instellingen kunnen voldoen aan de beveiligingseis. Deze richtlijnen geven aan dat beveiliging een

integraal deel moet zijn van de ontwikkeling en verbetering van uw diensten en dat u regelmatig moet toetsen (Plan-Do-Check-Act) of de beveiliging nog wel adequaat is. Op https://www.cbpweb.nl vindt u meer informatie over de privacytoezichthouder.

Aansprakelijkheid

Wanneer u software of diensten van derden inzet, blijft de instelling zelf verantwoordelijk en aansprakelijk voor de beveiliging daarvan. Dit geldt ook wanneer de leverancier zijn aansprakelijkheid heeft ingeperkt. Het is dus verstandig om in dit laatste geval de beperking van aansprakelijkheid te weigeren of om deze uit te breiden voor gevallen waarin er schade door privacy-schending ontstaat. Onder het kopje 'Handhaving' leest u hier meer over.

Datalekken

Vanaf 1 januari 2016 bevat de Wbp aanvullende bepalingen voor datalekken. Iedere inbreuk op de beveiliging van persoonsgegevens noemen we een datalek. Het gaat dus niet alleen om grootschalige ontvreemding van persoonsgegevens door externe hackers. Ook ongeautoriseerde toegang tot gegevens is een datalek.

Meldingsplicht bij datalek

Als een datalek optreedt, moet een instelling dit melden. U heeft echter geen meldplicht wanneer de gelekte persoonsgegevens technisch onbegrijpelijk of ontoegankelijk zijn gemaakt voor de hacker. Dit geldt als de persoonsgegevens met versleuteling (encryptie) zijn beveiligd. Wel moet die versleuteling die op het moment van de inbraak onkraakbaar zijn. Natuurlijk kan dit in de toekomst veranderen, maar de wet eist niet van u dat u daar rekening mee houdt.

Bij een datalek heeft u twee verplichtingen:

1. Melding aan de toezichthouder. U moet een datalek melden aan de toezichthouder wanneer er een aanzienlijke of zekere kans is op ernstige nadelige gevolgen voor betrokkenen. Meldingen aan de toezichthouder zijn in principe vertrouwelijk, maar kunnen worden gepubliceerd als daar aanleiding toe is.

2. Melding aan betrokkenen. U moet betrokkenen informeren over een datalek wanneer dit lek waarschijnlijk ongunstige gevolgen zal hebben voor hun persoonlijke levenssfeer.

Vermeld in beide meldingen:

- om wat voor lek gaat;
- waar de betrokkene of toezichthouder meer informatie over het lek kan krijgen;
- wat u aanraadt om de negatieve gevolgen van het datalek te beperken.

Aan de toezichthouder moet u ook melden welke gevolgen het datalek heeft en wat u heeft gedaan (en gaat doen) om het lek te dichten en de gevolgen te beperken.

Rechten van de student

Een student heeft het recht om te weten welke gegevens een onderwijsinstelling verwerkt. De student heeft ook het recht om zijn gegevens te laten corrigeren of te laten verwijderen. Dit kan wanneer hij feitelijke onjuistheden constateert in zijn persoonsgegevens of ziet dat gegevens achterhaald zijn. Hieronder leest u meer over deze rechten.

Recht op inzage

Een student kan een inzageverzoek indienen als hij wil weten welke gegevens een instelling over hem heeft verzameld. Bij zo'n verzoek is een instelling verplicht het

volledige dossier en alle geregistreerde gegevens te verstrekken. Ook aantekeningen en geregistreerde gegevens die niet online staan, vallen in principe onder het inzagerecht.

Een instelling mag slechts in één geval het inzageverzoek weigeren. Dat is wanneer een student excessief veel verzoeken in korte tijd indient. De instelling mag inzage niet weigeren op grond van bedrijfsgeheim of auteursrecht van de leverancier van de tool, of als het onduidelijk is wat de student van plan is met de gegevens. De instelling mag een vergoeding vragen van hoogstens € 5 per inzageverzoek.

Het is lastig om aan een inzageverzoek te voldoen als er geen functie voor inzage is ingebouwd in de learning analytics. Wij raden u daarom aan om bij uw leverancier van de tool te vragen om een dergelijke functie in uw tool in te bouwen.

Recht op correcties

Een student mag een instelling verzoeken zijn gegevens aan te passen als deze onjuist zijn. Het recht van correctie geldt alleen voor overduidelijke onjuistheden, zoals een fout gespelde naam, een onjuiste geboortedatum of een achterhaalde registratie. Het recht van correctie geldt ook voor onterecht verkregen gegevens of gegevens die in strijd met de wet zijn verzameld. Wanneer een student een correctie verzoekt, moet hij zelf de juiste gegevens leveren.

Als een student de gegevens zelf kan corrigeren, kan hij niet eisen dat de instelling dat voor hem doet. Een student kan ook geen correctie of verwijdering afdwingen wanneer een instelling de feiten moeilijk kan verifiëren of als uitgebreid onderzoek naar de juistheid nodig is. Andere gegevens waarbij het recht op correctie niet geldt, zijn: indrukken, meningen, onderzoeksresultaten en conclusies neergelegd in rapporten, conclusies of beoordelingen. Een student kan bijvoorbeeld geen tentamencijfer laten aanpassen door te betogen dat de beoordeling onjuist was.

Bij learning analytics speelt het recht van correctie zelden. De gegevens zijn doorgaans onbetwistbaar: de student deed 23 minuten en 12 seconden over die toets, hij las wel of niet de extra uitleg en bekeek drie van de vijf filmpjes. Het gaat vaak eerder over de conclusies die worden getrokken, maar daarvoor geldt het recht op correctie niet.

Recht op verwijdering

Het recht van verwijdering geldt voor alle gegevens die niet meer relevant of nodig zijn voor de doelen waarvoor zij zijn verzameld. Wanneer van persoonsgegevens geaggregeerde combinaties zijn gemaakt, hoeft u deze combinaties niet te wissen na een verwijderingsverzoek. Deze combinaties bevatten immers geen persoonsgegevens. Als de persoonsgegevens in bronbestanden staan voor wetenschappelijk onderzoek, mogen deze worden behouden, maar alleen voor verificatie van dat onderzoek (dus niet voor ander onderzoek, ook niet als vervolg op het betreffende onderzoek). Wanneer het technisch onmogelijk is om de gegevens te verwijderen, heeft de student het recht de gegevens te laten afschermen zodat ze nergens anders meer voor kunnen worden gebruikt. Dit is bijvoorbeeld het geval als de gegevens op back-ups staan die extern worden opgeslagen. De gegevens op deze back-ups mogen na het verzoek niet meer ingezet worden door uw instelling.

Het verwijderen van learning analytics-brongegevens is verplicht zodra u ze niet meer verwerkt. Wanneer een vak afgelopen is, zijn gegevens over de voortgang van dat vak niet meer nodig en dus mogen ze niet meer worden bewaard. Die gegevens moeten dus zo snel mogelijk na afronding van het vak geanalyseerd worden. De wet noemt hiervoor geen termijnen. Wij raden u wel aan om bij de informatieverstrekking of in uw privacyverklaring aan te geven welke bewaartermijnen de onderwijsinstelling redelijk vindt.

GEAUTOMATISEERDE BESLUITVORMING

De Wbp verbiedt volledig geautomatiseerde besluitvorming of sancties op basis van een persoonlijkheidsprofiel. Het gaat daarbij niet alleen om juridisch bindende besluiten of rechtsgevolgen zoals bij het uitsluiten van een student. Dit verbod geldt bij ieder besluit dat de betrokken persoon 'in aanmerkelijke mate' treft. Als u bijvoorbeeld op basis van een persoonlijkheidsprofiel een student dwingt extra opdrachten te maken, is dit al in strijd zijn met de wet Wbp ook al is zo'n extra opdracht geen juridisch bindend besluit volgens de wet.

Besluitvorming bij learning analytics

Bij learning analytics is al snel sprake van geautomatiseerde besluitvorming. Denk aan analyses die laten zien dat een student zwaar onder de maat presteert of die laten zien dat studenten met vergelijkbare achtergrond een bepaald vak zelden tot nooit in één keer halen. Als u op basis van die analyses een student dwingt om een voorbereidend vak te volgen, overtreedt u de Wbp.

Eis van menselijke tussenkomst

Learning analytics-software mag op basis van opgebouwde profielen conclusies trekken en aanbevelingen doen, maar het systeem mag niets zelfstandig beslissen. Uiteindelijk moet het altijd een mens zijn die de beslissing neemt. De beslissende persoon moet bovendien zelf een inhoudelijke motivatie opstellen. Deze motivatie mag hij baseren op de aanbeveling van de learning analytics-tool.

Een learning analytics-tool mag een student bijvoorbeeld een onvoldoende geven op basis van het aantal gemaakte fouten. Maar de tool mag geen besluiten nemen gebaseerd op (aspecten van) de persoonlijkheid van een student. Het is dus verboden een student automatisch als fraudeur uit te sluiten omdat hij na jaren onvoldoendes opeens zeer goed scoort. Wel mag een learning analytics-systeem deze opmerkelijke verbetering signaleren, waarna een docent nader onderzoek kan doen. De docent moet daarna beargumenteren waarom hij een student uitsluit.

Recht op bezwaar

Een student mag altijd een bezwaar indienen wanneer hij getroffen wordt door een besluit of maatregel die gebaseerd is op zijn persoonlijkheidsprofiel. De bezwaarmogelijkheid moet u bij het besluit of de maatregel expliciet noemen. U kunt de student deze optie bieden nadat de maatregel is opgelegd, als er tijd is om het negatieve gevolg te corrigeren. De persoon die het bezwaar ontvangt, moet vervolgens de maatregel of het besluit ongedaan kunnen maken. Als de medewerking van een softwareleverancier nodig is om een actie van een tool ongedaan te maken, moet u hier van tevoren afspraken over hebben gemaakt met de leverancier.

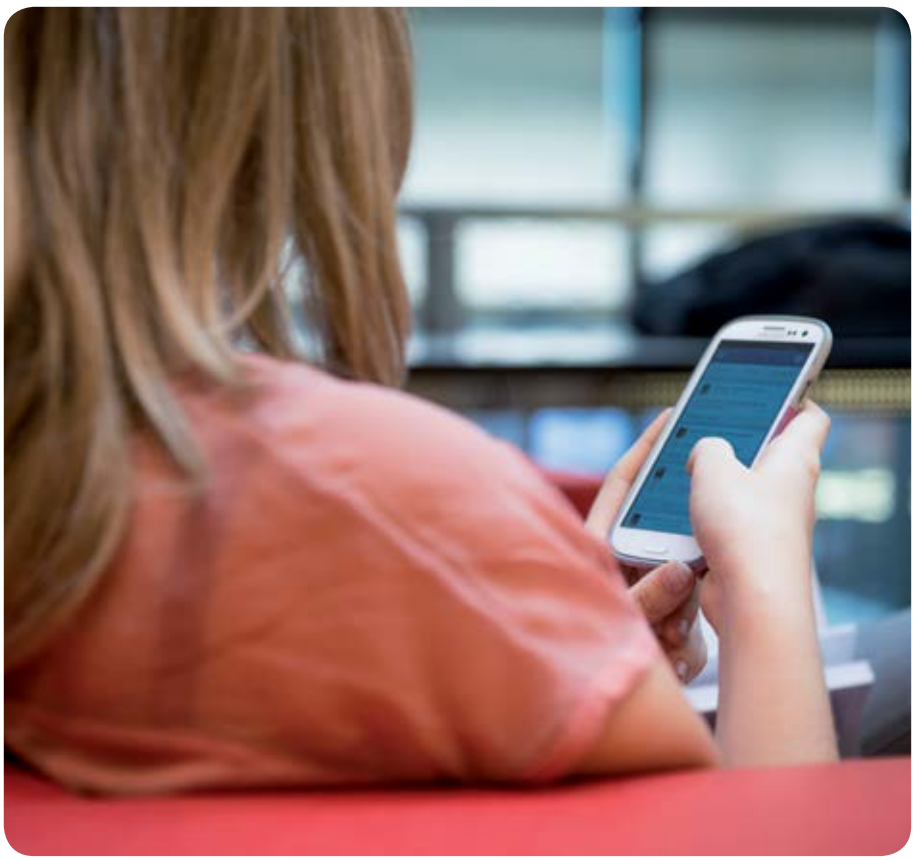
HOE GAAT U OM MET DIENSTEN VAN DERDEN?

Voor Learning Analytics maken onderwijsinstellingen vaak gebruik van diensten van derden. Dit kan door software in te kopen, maar steeds vaker besteden instellingen ook de dienstverlening bij derden uit. Voorbeelden hiervan zijn een clouddienst voor studenten of een externe tool die de prestaties bij een toets meet en daarover rapportages genereert.

Aandachtspunten

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

1. De instelling is altijd zelf 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 de akkoordverklaring van de learning analytics-tool of een disclaimer bij het startscherm van de software.
2. Als de externe dienstverlener zelf ook persoonsgegevens ontvangt zoals bij cloud-diensten, moet de instelling aparte afspraken maken over wat de dienstverlener daarmee mag doen. Dit legt u vast in een bewerkersovereenkomst. De Wbp ziet de dienstverlener namelijk als een ‘bewerker’ van de gegevens. Onder het kopje ‘Bewerkersovereenkomst’ leest u hier meer over.



Clouddiensten

Bij SaaS- en cloud-achtige omgevingen stelt de leverancier van de dienst een applicatie beschikbaar waarbinnen de instelling of de student gegevens uploadt en op de juiste knoppen drukt. De leverancier doet daar niet actief aan mee. Desondanks is het toch de applicatie-leverancier die de bewerker is volgens de Wbp, omdat de verwerkingen onder zijn beheer gebeuren. Maakt uw instelling gebruik van een clouddienst? Dan is het wettelijk verplicht om een bewerkersovereenkomst te sluiten met de leverancier.

Bewerkersovereenkomst

Een bewerkersovereenkomst is de overeenkomst waarbij een partij (de bewerker) in opdracht van een ander (de verantwoordelijke) persoonsgegevens verwerkt. De overeenkomst is verplicht. Europese leveranciers hebben vaak een eigen model. Amerikaanse dienstverleners kennen deze overeenkomst niet en kunnen afwijzend reageren op het verzoek deze af te sluiten. Deze organisaties beschouwen de verkregen gegevens vaak als hun eigendom, maar dit is in strijd met de Wbp. Een bewerker mag alleen bewerkingen op persoonsgegevens uitvoeren waartoe hij opdracht heeft van de verantwoordelijke.

Een bewerkersovereenkomst bevat de volgende elementen:

doeleinden van verwerking	datalekmeldplicht
verplichtingen van bewerker	verzoeken van betrokkenen
doorgifte van persoonsgegevens	vrijwaringen
garanties	geheimhouding
beveiliging	duur, verlenging en opzegging

WAAR MAG U GEGEVENS OPSLAAN?

De Wbp is gebaseerd op Europese regels. In die Europese regels staat dat men persoonsgegevens alleen mag opslaan of laten verwerken in landen waar een ‘adequaat’ niveau van bescherming bestaat. Dat wil zeggen dat het alleen mag in een land met net zulke strenge regels als Europa. Deze regels dwingen andere landen om ook regelgeving over persoonsgegevens aan te nemen.

Een nadere uitwerking vindt u in het ‘Juridisch Normenkader cloud services hoger onderwijs’. Dit document stelt normen voor het hoger onderwijs in Nederland op het gebied van vertrouwelijkheid, privacy, eigendom en beschikbaarheid ten aanzien van cloudleveranciers.

Buiten Europa

U bent niet verplicht om persoonsgegevens in Nederland op te slaan. Ieder ander Europees land is goed. Buiten Europa zijn er eigenlijk geen landen die voldoen aan de Europese eisen. De Verenigde Staten voldoen in ieder geval niet.

Europese dochter

Een bijzondere situatie ontstaat wanneer u persoonsgegevens opslaat in een datacenter in een Europees land dat wordt beheerd door een Amerikaanse partij of een dochtermaatschappij daarvan. Hoewel die partij dan onder Europees recht valt, acht de Amerikaanse overheid zich bevoegd om bij dat Europese datacenter persoonsgegevens op te vragen. Hierover loopt momenteel een rechtszaak tegen Microsoft. In deze zaak kan in hoger beroep worden beslist dat de Amerikaanse Justitie inderdaad gegevens mag vorderen uit Europese datacenters van dochterbedrijven van een Amerikaans bedrijf. Als dit gebeurt, heeft dit gevolgen voor gebruikers van deze datacenters. Het is dan volgens de Wbp niet langer toegestaan om persoonsgegevens op te slaan bij dergelijke datacenters. Houdt u deze ontwikkelingen daarom goed in de gaten als u gebruikmaakt van een datacenter dat beheerd wordt door een Amerikaans bedrijf.

HANDHAVING VAN DE WET

Vanaf 1 januari 2016 staat op overtreding van de Wbp een boete. Deze boete kan oplopen tot € 810.000. De toezichthouder moet nog aangeven welke boetes hij stelt op welke overtredingen.

De toezichthouder mag overtredingen pas beboeten nadat hij een bindende aanwijzing heeft opgelegd en een instelling die niet opvolgt. Wanneer de overtreding echter opzettelijk is begaan of het gevolg is van ernstig verwijtbare nalatigheid, mag de toezichthouder direct een boete opleggen. Wat ernstig verwijtbare nalatigheid precies inhoudt, is nog niet duidelijk. Wanneer een organisatie geen beleid heeft voor datalekken, is er waarschijnlijk sprake van ernstig verwijtbare nalatigheid. We raden u daarom aan uw databeleid zorgvuldig op te zetten en te handhaven, zodat u geen boete riskeert.

STAPPENPLAN

Wilt u gebruikmaken van learning analytics? Dan raden we u aan om de volgende stappen te ondernemen:

1	Bepaal voor welke doelen u learning analytics (LA) wilt inzetten en wat er voor die doelen nodig is.
2	Leg in een aparte privacyverklaring voor LA vast welke doelen dit zijn, welke gegevens u verzamelt en wat daarmee gebeurt.
3	Aggregeer informatie waar mogelijk. Geaggregeerde informatie valt buiten de Wbp. De aggregatie moet onomkeerbaar zijn. Vernietig daarom na aggregatie de brongegevens of scherm deze af.
4	Motiveer welke grondslag(en) de instelling wil gebruiken en waarom de inzet van learning analytics redelijkerwijs noodzakelijk is. Wanneer u wilt werken met toestemming, zorg er dan voor dat: a. de student eerst een duidelijke toelichting kan lezen; b. de student de toestemming op dat moment zonder gevolgen kan weigeren; c. de student uit de toestemmingsvraag kan opmaken waar hij toestemming voor geeft; d. de student expliciet ja of nee kan antwoorden op de toestemmingsvraag.
5	Spreek met de leverancier af dat hij gedetailleerde uitleg verstrekt, die u in de privacyverklaring kan opnemen. Ook bij updates van de tool is dat nodig.
6	Houd toezicht op gebruik van LA-gegevens, in ieder geval als dat buiten de oorspronkelijke doelen valt. Als de gegevens toegankelijk zijn, loopt u het risico dat ze voornieuwe doelen worden ingezet.
7	Zorg ervoor dat studenten LA-gegevens gemakkelijk kunnen downloaden en corrigeren.
8	Ga na welke LA-tools geautomatiseerd beslissingen nemen die studenten in aanmerkelijke mate raken en bied bij deze tools altijd een duidelijke bezwaarmogelijkheid aan.
9	Sluit bewerkersovereenkomsten met de leveranciers van online LA-tools. Leg daarin vast dat: a. zij aansprakelijk zijn voor datalekken; b. zij de gegevens niet voor eigen doeleinden mogen gebruiken; c. zij gedetailleerde informatie aanleveren aan studenten over hoe de tools werken.
10	Stel beleid op tegen datalekken en schendingen van de beveiliging.
11	Reageer positief op privacyzorgen en –bezwaren van studenten en zorg dat u alternatieven heeft waarmee u deze zorgen kunt vermijden.

COLOFON

Auteurs
Arnoud Engelfriet, ICTRecht
Jocelyn Manderveld, SURFnet
Evelijn Jeunink, SURFnet

Projectleiding
Jocelyn Manderveld, SURFnet

Eindredactie
Erik van der Spek, Hendrikx van der Spek

Ontwerp
Vrije Stijl, Utrecht

Fotografie cover
Annemiek van der Kuil

Datum
November 2015

SURF

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 – 787 30 00
www.surf.nl/surfnet