Persoonsgegevens van studenten

Hoe moeten instellingen in het hoger onderwijs op de werkvloer invulling geven aan de normen die de Wbp stelt aan de omgang met persoonsgegevens van studenten?

Colofon

Persoonsgegevens van studenten: Hoe moeten instellingen in het hoger onderwijs op de werkvloer invulling geven aan de normen die de Wbp stelt aan de omgang met persoonsgegevens van studenten?

Dit rapport is geschreven in opdracht van SURFdirect, de digitale rechten Expertise Community van SURF, in samenwerking met het SURFnet/Kennisnet-Innovatieprogramma, door Tina van der Linden, die verbonden is aan de Universiteit van Utrecht.

SURFdirect
Postbus 2290
3500 GG Utrecht
T + 31 30 234 66 00
F + 31 30 233 29 60
E info@surf.nl
W www.surf.nl/surfdirect

Auteur

Mr. T. van der Linden

16 mei 2012

SURF is de ICT-samenwerkingsorganisatie van het hoger onderwijs en onderzoek (www.surf.nl).
Deze publicatie is digitaal beschikbaar via de website van Stichting SURF:
www.surf.nl/publicaties

Inhoudsopgave

Hoofdstuk 1: Inleiding

You love it or you hate it.
Er zijn mensen die privacy een non-issue vinden, zeker anno 2011. Een bekende uitspraak is: *on the internet, there is no privacy - get over it*. Sommige internetgebruikers etaleren hun hele hebben en houden op sociale netwerksites als Facebook of Hyves, bloggen en twitteren erop los. Iedereen wordt constant gemonitord door zichtbare en onzichtbare camera's, en via onze OV-chipkaart en mobiele telefoon zijn sowieso al onze gangen na te gaan. So what? Met het oog op maatchappelijke veiligheid (lees: terrorismebestrijding) is dat maar goed ook. Ik heb niets te verbergen!

Maar soms leidt het feit dat gegevens van mensen ongewild, onbedoeld "op straat liggen" ook tot maatschappelijke verontwaardiging. Creditcardgegevens, vertrouwelijke communicatie (Wikileaks!), computers bij het vuilnis, verloren USB-sticks en in de trein achtergelaten dossiers halen regelmatig het nieuws. Zo ook het bericht in de Elsevier van 2 september 2009,[1] dat gevoelige informatie van studenten aan de Faculteit Communicatie & Journalistiek van de Hogeschool Utrecht al jaren op internet stond. Dat bericht was zelfs aanleiding voor kamervragen aan de toenmalige minister van onderwijs.[2] Het redactioneel van "het Onderwijsblad", het blad van de Algemene Onderwijsbond, van 3 oktober 2009 doet verslag van een onderzoek naar hoe eenvoudig het is om allerlei gegevens van studenten via de onderwijsinstellingen te achterhalen.[3]

Maar of je nou een privacy-lover bent of niet, het recht op privacy is een grondrecht (art. 10 Grondwet), en een mensenrecht (art. 12 Universele Verklaring, art. 17 BUPO, art. 8 EVRM), en is uitgewerkt in Europese regelgeving (Richtlijn 95/46/EG, de privacyrichtlijn). En die is geïmplementeerd in de Nederlandse Wet bescherming persoonsgegevens, de Wbp. Universiteiten en hogescholen in Nederland moeten zich gewoon houden aan de wet.

Dat zegt ook de minister van OCW in zijn antwoord op de kamervragen: [4] een goede naleving van de Wbp is de verantwoordelijkheid van de instellingen voor hoger onderwijs. En verder: "Binnen de universiteiten en hogescholen worden hiertoe ook initiatieven en werkzaamheden ontplooid. Zo zijn medewerkers actief in het beveiligen van informatie die vanuit de instelling wordt verspreid; gegevens die door de studenten zelf openbaar worden gemaakt vallen daar uiteraard niet onder. Verder komen (medewerkers van) de instellingen sinds een aantal jaren bijeen om kennis en ervaringen uit te wisselen over informatiebeveiliging in het kader van Stichting Surf. Er wordt informatie uitgewisseld over beveiligingsinbreuken, er wordt voorlichting gegeven aan de aangesloten instellingen op het gebied van beveiliging, zowel incidenteel (bij calamiteiten) als structureel (bijvoorbeeld in het geval van verspreiding van kennis over beveiligingslekken in software)."

---

[1] Zie bijlage 2.
[2] Zie bijlage 4.
[3] Zie bijlage 3.
[4] Antwoord van minister Plasterk (Onderwijs, Cultuur en Wetenschap) op vragen van de leden Jan Jacob van Dijk en Biskop (beiden CDA) aan de minister van Onderwijs, Cultuur en Wetenschap over het artikel «Gevoelige informatie studenten Utrecht jaren openbaar», Aanhangsel van de Handelingen van de Tweede Kamer der Staten Generaal, vergaderjaar 2009-2010, nummer 356, online beschikbaar op https://zoek.officielebekendmakingen.nl/ah-tk-20092010-356.html.

Om de Wbp na te leven is niet alleen beveiliging in technische zin van belang. Ook bijvoorbeeld de afspraken die gemaakt worden met leveranciers van Cloud-diensten zijn cruciaal voor compliance met de Wbp. Maar zelfs als zowel de technische beveiliging op orde is, èn de privacy-issues met dienstverleners zoals cloud-providers goed geregeld zijn, dan is altijd nog de mens de laatste schakel: ook docenten en onderwijssecretariaten hebben een rol in het zorgvuldig omgaan met studentgegevens

En dát is waar dit rapport zich op richt. De vraag die centraal staat is de volgende:

> *Hoe moeten instellingen in het hoger onderwijs op de werkvloer (docenten, onderwijssecretariaten) invulling geven aan de normen die de Wbp stelt aan de omgang met persoonsgegevens van studenten.*

Dit rapport is dus bestemd voor de instellingen in het hoger onderwijs - zij moeten er immers voor zorgen dat op de werkvloer goed met persoonsgegevens van studenten omgegaan wordt.
Technische beveiliging, en afspraken met dienstverleners blijven uitdrukkelijk buiten beschouwing. In dit rapport wordt ervan uitgegaan dat die op orde zijn. Ook blijft buiten beschouwing wat studenten over zichzelf en over elkaar openbaar maken - daar heeft de instelling geen zicht en geen invloed op.

Het belang van het beantwoorden van de centrale vraag van dit stuk is in de eerste plaats het privacy-belang van studenten. Om opgeleid te worden moeten de instellingen in het hoger onderwijs bepaalde persoonsgegevens van hen verwerken. En dan moeten zij ervan uit kunnen gaan dat hun gegevens bij die instellingen in goede handen zijn, en niet op straat komen te liggen zodat "Jan en alleman" van alles en nog wat over hen te weten kunnen komen. Maar ook de instellingen zèlf hebben een belang bij het voldoen aan de Wbp. Het schaadt het imago van de instellingen die genoemd zijn in de pers natuurlijk als zij op deze manier in het nieuws komen.

De opbouw van dit stuk is als volgt. Hoofdstuk 2 gaat nader in op de vraag wat privacy eigenlijk is, en waarom het belangrijk is. Om de lezer die zichzelf tot de privacy-onverschilligen rekent, misschien toch over te halen naar het andere kamp. Hoofdstuk 3 behandelt de regels van de Wbp, toegespitst op de praktijk van alledag in het hoger onderwijs. De relevante wetsartikelen zijn opgenomen in een bijlage. Veel instellingen hebben regels over hoe omgegaan moet worden met persoonsgegevens van studenten. Deze regels worden geïnventariseerd en besproken in hoofdstuk 4. In hoofdstuk 5 wordt de dagelijkse gang van zaken in het hoger onderwijs bekeken door de bril van de Wbp-compliance. Er wordt een aantal voorbeelden gegeven van hoe het, heel begrijpelijk en soms misschien ook wel gerechtvaardigd, toch vanuit het oogpunt van de Wbp, mis kan gaan. En uiteraard wordt dit stuk afgesloten in hoofdstuk 6 met een conclusie en enkele aanbevelingen.

Hoofdstuk 2: Belang van privacy

Zoals de titel al aangeeft gaat dit hoofdstuk over het antwoord op de vraag waarom het zo belangrijk is om zorgvuldig met persoonsgegevens van studenten om te gaan. Eerst zal uitgelegd worden wat privacy eigenlijk is, waarom privacy belangrijk is, en wat het verband is tussen privacy en persoonsgegevens. Dit leidt tot het begrip informationele privacy. Duidelijk zal worden gemaakt waarom zorgvuldige omgang met persoonsgegevens belangrijk is, ook al heeft de betrokkene (i.e. degene op wie de gegevens betrekking hebben) "niets te verbergen". Tenslotte worden, in aanvulling daarop, enkele voorbeelden gegeven van omstandigheden waarin onzorgvuldige omgang met persoonsgegevens van studenten wel nadelige consequenties kan hebben. Die voorbeelden vallen in twee categorieën uiteen: schade aan iemand's imago in een bepaalde contexten directe schade als gevolg van het bekend worden van bepaalde details.

2.1 Privacy

Bijna iedere verhandeling over privacy begint met een verwijzing naar het historische artikel van Warren en Brandeis uit de Harvard Law Review van 15 december 1890.[5] In "The right to privacy", werd, voor zover bekend, de term privacy voor het eerst werd gebruikt. Zij hebben het over het recht om met rust gelaten te worden.

De kern van het idee van privacy is dat ieder mens een natuurlijke behoefte heeft aan een eigen plek (zowel in letterlijke als in overdrachtelijke zin) waar hij of zij helemaal zichzelf kan zijn. En dus ook zelf mag bepalen wie hij of zij hoe ver daarin toelaat.

De eigen plek is in de eerste plaats het eigen lichaam. Respect voor ieder mens als individu brengt mee dat een ieder zeggenschap heeft over zijn of haar eigen lijf. Die eigen plek is ook de eigen woonomgeving: de studentenkamer of woning. En zelfs buitenshuis, op het werk, in de collegebank en in de openbare ruimte bestaat tot op zekere hoogte recht op bescherming van die eigen plek.

In overdrachtelijke zin gaat het bij de eigen plek over de controle die iemand heeft over wat er over hem of haar bekend is bij anderen. Net zo goed als niet iedereen toegelaten hoeft te worden tot iemands huis – ook al heeft de bewoner niets te verbergen en zit zij gewoon met een kop koffie de krant te lezen – hoeft ook niet iedereen van alles over haar te weten. Niet alleen omdat die persoonlijke details genant zouden zijn of schadelijke gevolgen zouden kunnen hebben, maar omdat het gewoon niemand iets aangaat. Respect voor iemands menselijke waardigheid brengt mee dat niet van alles wat er over iemand te weten is, ook bekend moet zijn bij anderen.

Net zoals een ieder vrij is om bezoek in zijn huis toe te laten, is ook iedereen vrij om informatie over zichzelf met anderen te delen – of niet! Zaken als leeftijd, vrijetijdsbesteding, talenten en voorkeuren: het recht op een overdrachtelijke "eigen plek" brengt mee dat een mens zelf zou moeten mogen bepalen wie wat

[5] Eenvoudig op internet te vinden: http://www.abolish-alimony.org/content/privacy/Right-to-Privacy-Brandeis-Warren-1890.pdf.

over hem of haar weet. Dát is wat bedoeld wordt met "informationele zelfbeschikking".[6]

Het is meteen duidelijk dat het recht op een eigen plek niet absoluut is; er zijn allerlei beperkingen op mogelijk. Zelfs op de lichamelijke integriteit: in sommige gevallen kan iemand tegen zijn of haar wil worden onderworpen aan onderzoek aan en zelfs in het lichaam.[7] Ook de eigen woning kan tegen de wil van de bewoner in bepaalde omstandigheden betreden en doorzocht worden.[8]

Het recht op informationele zelfbeschikking zoals hierboven omschreven, bestaat in het Nederlandse recht niet in zijn onverkorte vorm. Iedere legaal in Nederland verblijvende persoon staat geregistreerd in de bestanden van de overheid met een aantal basisgegevens. Om aan het maatschappelijk leven deel te kunnen nemen moeten overeenkomsten gesloten worden, waarvoor het bekend maken van bepaalde persoonsgegevens vaak noodzakelijk is. Ook in de intermenselijke omgang worden voortdurend persoonsgegevens uitgewisseld. Van belang is dan wel dat iemand zelf bepaalt wat zij wel of niet vertelt. De mate waarin een burger met de wet in de hand invloed kan uitoefenen op wie wat over hem weet wordt in dit stuk aangeduid met "informationele privacy". Dus: informationele zelfbeschikking is de uiterste vorm, informationele privacy is wat de wet beoogt te regelen.
De kern, de belangrijkste reden waarom zorgvuldig met gegevens van studenten omgegaan moet worden is, kort en bot gezegd: "Nobody's business". Als een student zelf niet wil vertellen aan iemand dat zij studeert, wat zij studeert, welke cijfers ze gehaald heeft, waar ze woont, etc. dan is dat haar goed recht. En dan mag het niet zo zijn dat een derde (haar moeder, haar ex-vriend, een potentiële werkgever, of de buurvrouw) daar toch, buiten haar om, via de onderwijsinstelling achter kan komen.

2.2 Beeldvorming

Behalve het "nobody's business"-argument zijn er wel meer redenen waarom iemand niet zou willen dat zijn persoonsgegevens publiek bekend zijn. Eigenlijk zou de vraag niet moeten zijn wat iemand te verbergen heeft, maar wat iemand aan een ander wil vertellen.[9]

In het contact tussen mensen, en zeker tussen mensen die elkaar niet zo goed kennen, is imago enorm belangrijk. Imago, het beeld dat van iemand bestaat, wordt bepaald door hoe iemand eruit ziet, hoe hij zich kleedt, hoe hij praat en wat hij zegt, en wat er over hem bekend is.
Individuen leven over het algemeen niet alleen, maar ze delen hun leven met anderen in verschillende rollen. Zo woont een student misschien samen met andere studenten in een studentenhuis, is ze lid van een sportvereniging, zit ze in een werkgroep bij een bepaald vak, en maakt ze ook nog deel uit van haar familie. Het is een bekend en normaal verschijnsel dat mensen zich soms in een an-

[6] Westin, A.F. 'Science, Privacy and Freedom: Issues and Proposals for the 1970's, Part II, Balancing the Conflicting demands of Privacy, Disclosure and Surveillance', in: Columbia Law Review, 1966, online beschikbaar via http://www.jstor.org/pss/1120983.
[7] Art. 56 Sv.
[8] Zie de bepalingen in de Algemene wet op het binnentreden.
[9] Zie Daniel J. Solove, 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, San Diego Law Review, Vol. 44, p. 745, 2007, online beschikbaar op http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565&rec=1&srcabs=174508.

dere rol anders gedragen. Maar ook dat andere dingen belangrijk zijn, eigenschappen anders gewaardeerd worden, resultaten in de ene rol wel en in een andere rol niet positief gewaardeerd worden. Iemand kan op het werk een heel andere kant van zichzelf laten zien dan thuis, en weer een andere op de sportclub of in het café. En natuurlijk veranderen rollen en groepen waar iemand deel van uitmaakt in de loop der tijd. In een vriendenclub op een middelbare school maakte iemand met andere dingen indruk dan later bij collega's op het werk.

Dat kan dus betekenen dat iemand er een belang bij heeft om die rollen ook gescheiden te houden, met name als wetenswaardigheden uit de ene rol negatief uitwerken op het imago in een andere rol … ook al zijn die wetenswaardigheden an sich misschien niet eens relevant voor die andere rol. Zo is een goede reputatie als escort-girl tijdens iemands studententijd wellicht geen pre voor een functie later als longarts. En misschien wil iemand niet dat zijn drinkbroeders in de kroeg weten dat hij een opleiding volgt tot professioneel balletdanser.
We hebben het dan eigenlijk over vooroordelen, over groepskenmerken die klakkeloos op een individu van toepassing verklaard worden. En over jeugdzonden, die iemand tot in lengte van jaren nagedragen kunnen worden. Ook daarom is informationele privacy dus van belang. Niet alleen voor dingen die anderen niets aangaan, maar ook om verschillende werelden, verschillende delen van iemands leven van elkaar gescheiden te houden. Als iemand zelf bepaalt wie wat over hem mag weten, dan kunnen irrelevante dingen uit een andere rol, die wel negatief kunnen uitwerken op zijn imago in een andere rol onbekend blijven.[10]

Ook dat kan spelen bij persoonsgegevens over studenten. Misschien wil een student niet dat in de omgeving waar hij vrijwilligerswerk doet, bijvoorbeeld bij daken thuislozen, bekend is dat hij geneeskunde studeert – puur omdat hij dan met andere ogen bekeken wordt. Of iemand wil niet dat zijn medestudenten weten dat hij uit Limburg komt – of uit Friesland. Of dat hij de zoon is van een bekende Nederlander. Of dat hij de bekende Nederlander zelf is!

2.3 Schadelijke wetenswaardigheden

Tenslotte zijn er nog voorbeelden denkbaar dat het bekend worden van bepaalde details direct schadelijke gevolgen heeft voor de betrokkene, los van imagoschade zoals hiervoor bedoeld.
Een voorbeeld is een student die gestalked wordt door zijn ex-vriendin. Via zijn studentnummer kan ze zijn rooster achterhalen, en ze kan hem dus lastigvallen bij colleges en werkgroepen. Of een boze vader, die achter de slechte studieresultaten van zijn dochter komt. Of een journalist, die de afstudeerscriptie van een inmiddels bekende strafpleiter in handen krijgt en diens vroegere standpunten onthult.

Het punt is dat gegevens die op het eerste oog onschuldig lijken, in een bepaalde context toch heel schadelijk voor een betrokkene uit kunnen pakken.

[10] Zie over imago en digitaal identiteitsmanagement uitgebreider: Tina van der Linden, Tijmen Wisman, Image-building op het internet: Houd greep op je digitale identiteit, geschreven in opdracht van SurfDirect, de DIgitale Rechten Expertise Community van SURF, maart 2010, online beschikbaar op http://www.surffoundation.nl/SiteCollectionDocuments/SURFdirect_Image-building%20op%20het%20internet_mrt2010_DEF.pdf.

2.4 Conclusie

Het is belangrijk dat niet alleen op instellingsniveau maar ook op de werkvloer van het hoger onderwijs, door docenten en onderwijssecretariaten, zorgvuldig omgegaan wordt met persoonsgegevens van studenten.

Hoofdstuk 3. De regels: Wet

Iedereen die in zijn of haar werk met persoonsgegevens van anderen werkt, moet zich houden aan regels. Die regels staan in de wet, de Wet bescherming persoonsgegevens. En die wet is een uitvoering van een bepaling in de Grondwet, die stelt: "*De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.*" (art. 10 lid 3 Gw.).

Vooraf is het natuurlijk van belang om te weten wanneer het precies gaat om persoonsgegevens; met andere woorden, wanneer de regels van toepassing zijn. Persoonsgegevens zijn al die gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon. Dus: alles wat iets zegt over iemand, en je weet of kunt erachter komen wie dat is. Die persoon, op wie de gegevens betrekking hebben, wordt in de Wbp de "betrokkene" genoemd.

Bij studenten zal het dan bijvoorbeeld gaan om naam, adres, woonplaats (de zogenaamde NAW-gegevens), geboortedatum, eventueel het adres van zijn of haar ouders, welke opleiding iemand volgt, welke vakken, cijfers, rooster, aanwezigheid, ziekte, ingeleverde werkstukken etcetera.

Identificeerbaar is een student in de eerste plaats aan de hand van zijn of haar naam. Omdat namen niet gegarandeerd uniek zijn, krijgen studenten een studentnummer, aan de hand waarvan iedere student uniek geïdentificeerd kan worden. Anonieme gegevens, bijvoorbeeld wetenschappelijke bijdragen die aan (double)blind peer review worden onderworpen waarbij de peers elkaar identiteit ècht niet kunnen achterhalen, vallen dus niet onder de Wbp (wèl onder het auteursrecht). Ook geaggregeerde gegevens, bijvoorbeeld statistische gegevens die niet meer terug te voeren zijn op individuele studenten, zijn geen persoonsgegevens in de zin van de wet.

Het normatieve uitgangspunt (gebaseerd op het idee van informationele privacy dat in het vorige hoofdstuk aan de orde is geweest) is dat zorgvuldig moet worden omgegaan met persoonsgegevens. De wettelijke regels zijn te beschouwen en te begrijpen als een concrete uitwerking van deze eis van zorgvuldigheid.

Instellingen in het hoger onderwijs zijn vrijgesteld van de verpliching om hun verwerkingen van persoonsgegevens te melden bij het College Bescherming Persoonsgegevens, mits ze voldoen aan de vereisten van art. 19 van het Vrijstellingsbesluit (zie Bijlage I).

3.1 Doelbinding

Het eerste punt is dat niet méér gegevens gevraagd en opgeslagen mogen worden dan strikt noodzakelijk is voor het doel waarvoor de gegevens nodig zijn.[11] Dat betekent dat dus eerst vastgesteld moet worden wat het doel van de gegevensverwerking precies is. Degene die het doel bepaalt waarvoor gegevens verzameld worden, wordt in de Wbp de "verantwoordelijke" genoemd.

[11] Art. 7 en art. 9 Wbp.

Dat doel wordt in eerste instantie op instellingsniveau bepaald, en daar wordt ook aangegeven welke gegevens van studenten dus nodig zijn. In het hoger onderwijs zijn dus de instellingen in ieder geval aan te merken als verantwoordelijken. Maar ook individuele docenten kunnen "verantwoordelijken" in de zin van de Wbp zijn, namelijk als zij ook eigen doelen hebben met het verwerken van de persoonsgegevens van studenten. Voor zover docenten en medewerkers van onderwijssecretariaten alleen uitvoering geven aan de doelstellingen die op instellingsnivo zijn bepaald zijn zij aan te merken als "bewerkers" in de zin van de Wbp. Dat betekent dat zij zich, voor wat betreft de gegevens die aan hen worden toevertrouwd, moeten houden aan de regels van de Wbp. En dat de instelling daarvoor verantwoordelijk is! Veel instellingen hebben daarom eigen interne regels voor de omgang met persoonsgegevens van studenten. Die regels komen in het volgende hoofdstuk aan de orde.

Docenten en onderwijssecretariaten houden studentgegevens bij, zoals cijfers en presentielijsten. Van tevoren moet dan nagedacht zijn voor welk doel die gegevens verzameld en bewaard worden, en welke gegevens dus nodig zijn - en welke niet. Alleen gegevens die nodig zijn voor een van te voren bepaald, legitiem doel, mogen verzameld en bewaard worden. Zo is het duidelijk dat cijfers voor deeltoetsen opgeslagen moeten worden, die bepalen immers het eindcijfer voor een cursus - maar welke studenten altijd samen optrekken niet.

Belangrijk is voorts dat gegevens niet voor een ander doel gebruikt mogen worden dan het doel waarvoor zij verzameld zijn - tenzij dat andere doel niet onverenigbaar is met het oorspronkelijke doel. Een adres van een student mag bijvoorbeeld wel gebruikt worden om een nagekeken maar niet door de student opgehaald werkstuk per post aan hem terug te sturen. Maar het mag niet, zonder toestemming van de betrokken student, aan een headhunter doorgespeeld worden!

3.2 Grondslagen voor verwerking

Het tweede punt is dat er maar een beperkt aantal gronden is waarop verwerking van persoonsgegevens gebaseerd mag worden. Het begrip "verwerken" omvat al het denkbare dat met persoonsgegevens gedaan zou kunnen worden, met name: opslaan, gebruiken, bewaren en doorgeven aan anderen ("derden"). Hier worden alleen de grondslagen besproken die voor de relatie student - docent - instelling van belang zijn.

Studenten hebben een overeenkomst gesloten met de onderwijsinstelling waar ze studeren door zich in te schrijven voor een bepaalde opleiding. Om die overeenkomst uit te kunnen voeren (te weten: die student op te leiden voor een bepaald diploma) moeten nou eenmaal persoonsgegevens van die student verwerkt worden. Dat is prima, en dat mag natuurlijk. Ook mogen gegevens met toestemming van de betrokkene (dat is: degene op wie de gegevens betrekking hebben, in dit geval de student) verwerkt worden. Als er bijvoorbeeld een excursie georganiseerd wordt dan kan het handig zijn om mobiele telefoonnummers van de deelnemers te hebben. Als deelnemende studenten hun mobiele telefoonnummer voor dat doel geven aan een docent, dan mag daaruit afgeleid worden dat die studenten voor gebruik voor dat doel toestemming hebben gegeven. Volgens de regels moet de docent dan na die excursie die telefoonummers weer wissen, tenzij hij of zij apart toestemming krijgt om die gegevens ("altijd handig") te mogen bewaren.

In bijzondere gevallen kan het zijn dat gegevens toch zonder expliciete toestemming (en zonder dat verwerking noodzakelijk is voor de opleiding) verwerkt mogen worden. In dat geval moet een belangenafweging gemaakt worden tussen het belang waarvoor de gegevens dan nodig zijn (zoals bijvoorbeeld bij een student die ergens van beschuldigd wordt) en het privacy-belang van de student. Het moge duidelijk zijn dat bij zo'n belangenafweging het niet altijd evident is welk belang het zwaarste weegt. In voorkomende gevallen doet een docent er goed aan om die belangenafweging niet zelf te maken maar over te laten aan bijvoorbeeld een bestuur of een studie-adviseur.

Ook als een "vitaal belang" van de student in het geding is mogen gegevens verwerkt worden. Een voor de hand liggend voorbeeld is het geval dat een student tijdens de les een buiten bewustzijn raakt en per ambulance afgevoerd wordt - waarbij de docent dan wel aan het ambulancepersoneel naam en andere relevante gegevens van deze student door mag geven.
Concreet betekent dit dus onder meer dat gegevens van een student niet zonder diens toestemming meegedeeld mogen worden aan anderen, onder wie: ouders (tenzij de betrokken student minderjarig is en de ouders wettelijke vertegenwoordigers zijn), mede-studenten, collega's, potentiële werkgevers, commerciële partijen, etc. Met toestemming mag het wel, bijvoorbeeld als een docent gevraagd is door een student om als referentie op te treden bij een sollicitatie.

3.3 Bijzondere persoonsgegevens

Het derde punt betreft de zogenaamde bijzondere persoonsgegevens. Bijzondere persoonsgegevens gaan onder andere over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en strafrechtelijke verleden. De hoofdregel is dat deze gegevens helemaal niet verwerkt mogen worden, behoudens de in de wet genoemde uitzonderingen. Een van deze uitzonderingen betreft “scholen voor zover dat met het oog op de speciale begeleiding van leerlingen of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is”. Als dus een student met dyslexie extra tentamentijd nodig heeft, dan mag wel vastgelegd worden dat die student dyslexie heeft en op basis daarvan recht heeft op extra tijd. Maar het is docenten dus niet toegestaan om bijvoorbeeld geloof of politieke voorkeur, als die terug te voeren zijn tot identificeerbare studenten, te registreren.

3.4 Bewaartermijn

Ten vierde mogen gegevens niet tot in lengte van dagen bewaard blijven. Uit de eis van doelbinding volgt eigenlijk al dat gegevens niet langer bewaard mogen worden dan nodig is voor de verwerkelijking van de doeleinden waarvoor ze verzameld en verwerkt zijn – tenzij uiteraard die gegevens geanonimiseerd worden.

Concreet betekent dit dat presentielijsten, tentamens en dergelijke in elk geval niet langer bewaard mogen worden dan de termijn waarop behaalde studieresultaten verlopen, tien jaar. Het vrijstellingsbesluit bepaalt dat uiterlijk nadat de studie is beëindigd, de persoonsgegevens worden verwijderd. Het is dus goed om regelmatig op te ruimen en oude stapels (werkstukken, presentielijsten, evaluatieformulieren, tentamens) te vernietigen. Dat geldt ook voor elektronische bestanden die meer dan tien jaar oud zijn (hoewel die wellicht door het voort-

schrijden der techniek toch al niet meer leesbaar zijn) of die betrekking hebben op studenten die al twee jaar of langer afgestudeerd zijn. Scripties die met toestemming van de betrokken studenten in de bibliotheek (fysiek en/of elektronisch) opgenomen worden mogen uiteraard wel beschikbaar blijven, omdat er dan een ander doel is (te weten: informatie-ontsluiting). Hetzelfde geldt voor documenten die opgenomen worden in de database van het plagiaatdetectiesysteem.

3.5 Beveiliging

Tenslotte moeten gegevens op een adequate manier beveiligd worden, zodat niet iedereen zomaar bij de persoonsgegevens van studenten kan. Die adequate beveiliging zal als regel wel in de gehanteerde procedures en de gebruikte software ingebakken zitten - maar dan is wel van belang dat die ook goed gehanteerd worden. Dus: geen presentielijsten laten slingeren, uitgeprinte gegevens niet bij de printer op de gang laten liggen maar meteen ophalen, zorgvuldig omspringen met inloggegevens, en geen ingelogde computers onbeheerd achterlaten.

3.6 Andere wetten

Behalve de Wbp zijn in enkele bijzondere gevallen ook andere wetten relevant. Het kan namelijk zijn dat een overheidsorgaan een wettelijke bevoegdheid heeft om gegevens te vorderen – en de verantwoordelijke (lees: instelling voor hoger onderwijs) kan dan via de zijdeur van art. 8 sub c ("gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is") verplicht zijn om aan die vordering te voldoen. Te denken valt aan verzoeken van de AIVD op grond van art. 17 van de Wet op de inlichtingen- en veiligheidsdiensten 2002, aan verzoeken van de politie op grond van artt. 126nc/u Sv. (onderdeel van de zgn. de Wet bevoegdheid vorderen gegevens) en aan verzoeken van de IND/Vreemdelingenpolitie op grond van art. 107 Vreemdelingenwet 2000.

Hoofdstuk 4. De regels: de instellingen zelf

De wettelijke regels, met name die van de Wbp, worden door veel instellingen "vertaald" naar privacyreglementen, studentenstatuten, en dergelijke. In het kader van dit onderzoek is een brief gestuurd naar alle 53 instellingen voor hoger onderwijs die bij SURFnet aangesloten zijn. De vraag was of de instelling regels (richtlijnen, reglementen, statuut o.i.d.) heeft die zich richten tot docenten en/of onderwijssecretariaten, over hoe zij met gegevens van studenten om moeten gaan. Er is expliciet bij vermeld dat het gaat om een inventarisatie, en dat in het onderzoeksrapport niet vermeld zal worden welke instelling welke regels (of geen regels) hanteert. Dat is tevens de reden waarom bij de hierna opgenomen citaten geen bron is vermeld.

Van 16 instellingen werd een antwoord ontvangen. Een enkeling gaf aan "helemaal niets te hebben", een paar wilden niet meedoen aan het onderzoek, sommigen gaven kort aan regels te hebben, en 11 instellingen stuurden spontaan ook hun eigen regels mee.

In dit hoofdstuk wordt verslag gedaan van de inventarisatie van die regels, aan de hand van dezelfde punten die in het vorige hoofdstuk over de Wbp besproken zijn: doelbinding, grondslagen voor verwerking, bijzondere persoonsgegevens, bewaartermijn en beveiliging. Steeds wordt weergegeven wat zoal in de reglementen aan bepalingen gevonden is, gevolgd door een kort evaluerend commentaar. Het hoofdstuk wordt afgesloten met enige observaties over de kenbaarheid en bruikbaarheid van de instellingsregels.

4.1 Doelbinding

Doelen die in de reglementen zoal genoemd worden zijn:

a. de organisatie en de invulling van het onderwijs;
b. de diplomering en de administratie van de studievoortgang;
c. de begeleiding en ondersteuning van studenten;
d. het geven van studieadviezen;
e. de werkzaamheden van de aan de instelling verbonden instanties die zich richten op het studentenwelzijn;
f. het verstrekken of ter beschikking stellen van leermiddelen;
g. het berekenen, vastleggen of innen van college- en examengelden en andere bijdragen voor leermiddelen en activiteiten, waaronder begrepen het in handen van derden stellen van deze vorderingen;
h. het verzenden van voor studenten relevante informatie;
i. het behandelen van geschillen;
j. het doen uitoefenen van accountantscontrole;
k. het beheer en de beveiliging van gebouwen en voorzieningen van de instelling;
l. het samenstellen van de kiesregisters;
m. de uitvoering of toepassing van een wettelijke verplichting;
n. adequaat kunnen voldoen aan de vraag gegevens te verstrekken aan personen of instanties met een publiekrechtelijke taak;
o. het kunnen beschikken over zowel individuele als collectieve studenteninformatie ten behoeve van ontwikkelingen, studenten-, onderwijs- of marketing-

beleid, of andere beleid/ontwikkeling in verband met de bedrijfsvoering van de instelling.

Eén instelling gooit alles op een hoop: "De verwerking van persoonsgegevens heeft tot doel het vastleggen van persoonsgegevens, het bieden van individuele informatie en het verstrekken van gegeven ten behoeve van officiële instellingen (cfi; IB-groep, inspectie; ABP; ARBO) aan artsen, logopedisten, psychologen, opvoedkundigen, leerkrachten en andere personen, voor zover dit noodzakelijk is voor de bedrijfsvoering van [de instelling]".

Twee instellingen verwijzen naar afzonderlijke regels per verwerking van persoonsgegevens, waarin dan per verwerking wordt aangegeven
- wie de verantwoordelijke is, wie de beheerder en wie de bewerker;
- welke doeleinden de verwerking heeft;
- van welke categorieën van personen persoonsgegevens worden verwerkt;
- welke soorten van persoonsgegevens ten hoogste worden verwerkt en op welke wijze deze gegevens worden verkregen;
- aan welke personen binnen en buiten de organisatie welke persoonsgegevens kunnen worden verstrekt, gelet op het doel en de grondslag van de verwerking.

Commentaar: Het is goed (en ook wettelijk vereist natuurlijk) dat instellingen nagedacht hebben over de doelen waarvoor ze gegevens verzamelen, en dat ze die doelen geëxpliciteerd hebben. Echter, gegevensverstrekking aan derden ligt altijd een beetje problematisch, en het criterium "voor zover noodzakelijk voor de bedrijfsvoering van de instelling" is erg vaag. Is het noodzakelijk voor de bedrijfsvoering van een instelling van hoger onderwijs om gegevens (zoals studieresultaten of presentie) over een student met psychische problemen door te spelen aan een psycholoog? En wie bepaalt dat?
Ook het "kunnen beschikken over zowel individuele als collectieve studenteninformatie ten behoeve van ontwikkelingen, studenten-, onderwijs- of marketingbeleid, of andere beleid/ontwikkeling in verband met de bedrijfsvoering van de instelling" is buitengewoon vaag en ruim geformuleerd, en is niet opgenomen bij de doelen die in het Vrijstellingsbesluit genoemd zijn.

4.2 Grondslagen voor verwerking

Alle onderzochte reglementen nemen de regeling van de artt. 8 en 9 Wbp (zie bijlage) over. Sommige instellingen laten het daarbij, anderen proberen de grondslagen te concretiseren voor de specifieke situatie van studenten in het hoger onderwijs.

Zo heeft een universiteit een "naslagwerk" met betrekking tot vragen van instanties als AIVD, politie/justitie, sociale dienst, OPTA en dergelijke. Het gaat dan om de invulling van de belangenafweging van art. 8 sub f Wbp. Het dringende advies aan de medewerker is om die belangenafweging vooral niet zelf te maken, maar vragende instanties door te verwijzen naar hogere niveaus (CvB, directeur studentenservice en hoofd juridische zaken).

Een hogeschool heeft een Gedragscode Gegevensverstrekking aan derden. De algemene regel van die Gedragscode luidt als volgt:
"Algemene persoonsgegevens worden niet aan derden verstrekt, tenzij er sprake is van één van de onderstaande uitzonderingen:

- Wij zijn verplicht tot het verstrekken van de gegevens op grond van een wettelijk voorschrift;
- De student heeft toestemming gegeven om gegevens door te geven;
- In noodsituaties, in het belang van de betrokken student.

Vertrouwelijke gegevens worden nooit aan anderen (ook niet binnen de instelling) doorgegeven, tenzij met toestemming van de student."

4.3 Bijzondere persoonsgegevens

Een drietal instellingen vermeldt expliciet welke persoonsgegevens binnen de onderwijsinstelling verwerkt worden. De een neemt de volgende gegevens op:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, alsmede bank/gironummer van betrokkene;
b. dezelfde gegevens van de ouders, voogden of verzorgers van betrokkene,
c. nationaliteit en geboorteplaats;
d. inschrijvingsvorm;
e. correspondentienummer;
f. een administratie/studentnummer dat geen andere informatiebevat dan bedoeld onder a;
g. jaren van inschrijving als student;
h. student debiteurengegevens;
i. in geval van inschrijving aan meer dan één instelling: eerste instelling;
j. eerste jaar van inschrijving aan de desbetreffende instelling(en);
k. opleiding(en), opleidingsdeel of –delen, opleiding(en) van de vervolgfase, cursus(en) HBO;
l. studiefase (propedeutische fase, bachelor of masterfase);
m. voltijdse/deeltijdse, AD of duale studie;
n. gegevens studiefinanciering;
o. eventuele getuigschriften;
p. beslissing omtrent beëindiging van de inschrijving;
q. datum waarop degene aan wie geen getuigschrift van het afsluitend examen is uitgereikt, de instelling hebben verlaten;
r. datum van het behalen van het getuigschrift van het afsluitend examen;
s. laatst gevolgde vooropleiding die toegang geeft tot het hoger onderwijs met vermelding van vakkenpakket, alsmede het middelbaar beroepsonderwijs,alsmede waar vereist het al dan niet voldaan hebben aan aanvullende eisen;
t. jaar waarin het aan de vooropleiding verbonden diploma is behaald;
u. in voorkomende gevallen de datum van overlijden
v. andere gegevens waarvan de verwerking wordt vereist met het oog op de toepassing van een andere wet.

Een tweede wil ook:

- een gedigitaliseerd opgeslagen pasfoto;
- nationaliteit en geboorteplaats, geboorteland van ouders en grootouders;
- gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de betrokkene;
- school van herkomst van betrokkene, diploma vooropleiding;
- andere gegevens, verzameld via een camera die zichtbaar is of waarvan de aanwezigheid kenbaar is gemaakt;
- andere gegevens, verzameld via een verborgen camera, indien er sprake is van een vermoeden van strafbaar of onrechtmatig handelen door studenten,

waarbij het proportionaliteits- en subsidiariteitsbeginsel in acht wordt genomen.

En daarbij wordt aangegeven dat deze lijst niet limitatief is. Als gevolg van onder andere wijzigingen in de (onderwijs)organisatie of in wetgeving kunnen er veranderingen optreden.

Een derde school slaat nog veel meer op, naast de gegevens zoals vermeld op het aanmeldingsformulier, "voor zover nodig" ook:

- gegevens betreffende godsdienst en/of levensovertuiging;
- gegevens betreffende de gezondheid;
- gegevens betreffende vooropleiding en actueel studieverloop (portfolio);
- gegevens aangaande de financiële situatie van de student.

Commentaar: Er worden dus ook bijzondere gegevens in termen van de Wbp opgeslagen, namelijk: godsdienst/levensovertuiging en gezondheid. Voor godsdienst/levensovertuiging geldt art. 17 van de Wbp, dat bepaalt dat instellingen op godsdienstige of levensbeschouwelijke grondslag die gegevens inderdaad mogen verwerken, voor zover dit gelet op het doel van de instelling en voor de verwezenlijking van haar grondslag noodzakelijk is. Voor gezondheid geldt de eerder genoemde uitzondering voor scholen, voor zover dat met het oog op de speciale begeleiding van leerlingen of het treffende van bijzondere voorzieningen in verband met hun gezondheidstoestand noodzakelijk is. Het is op het eerste gezicht niet duidelijk voor welk doel nationaliteit en geboorteplaats, geboorteland van ouders en grootouders verwerkt zou moeten worden. Dat zou alleen mogen met het doel personen van een bepaalde etnische of culturele minderheidsgroep een bevoorrechte positie toe te kennen ten einde feitelijke nadelen vanband houdende met de grond ras op te heffen of te vermindering, dit voor dat doel noodzakelijk is en de betrokkene daartegen geen schriftelijk bezwaar heeft gemaakt (art. 18 Wbp).

4.4 Bewaartermijn

De meeste regels nemen gewoon de hoofdregel van art. 10 Wbp over: Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld en verwerkt. Dat is ontegenzeggelijk niet onjuist, maar weinig informatief voor bijvoorbeeld een docent die graag wil weten hoe lang zij gegevens mag of moet bewaren.
Een hogeschool maakt een mooi onderscheid tussen soorten gegevens en de daaraan verbonden bewaartermijnen:

- gegevens betreffende toelating tot de opleiding en examens, de inschrijving en het al dan niet behalen van getuigschrift(en) moeten 50 jaar bewaard worden;
- gegevens over de aard en het verloop van het onderwijs, studievoortgangsresultaten en studiebegeleiding worden uiterlijk 4 jaren nadat de studie is beëindigd, verwijderd;
- gegevens van persoonlijke en individuele aard, al dan niet rechtstreeks verbonden met het onderwijsproces, die verwerkt worden door studentendecanen en andere vertrouwenspersonen, worden uiterlijk 5 jaar na het einde van de studie verwijderd, afhankelijk van de doelbestemming en ter beoordeling aan de betrokken studentendecaan en/of vertrouwenspersoon.
- Gegevens verzameld door camera's worden niet langer bewaard dan noodzakelijk voor het doel waarvoor ze verzameld zijn: maximaal 14 dagen, dan wel tot een geconstateerd incident afgehandeld is.

Een andere hogeschool bepaalt daarnaast nog dat persoonsgegevens van aspirant-studenten die niet bij de hogeschool worden ingeschreven uiterlijk twee jaar na aanvang van het nieuwe studiejaar uit het bestand worden verwijderd.

4.5 Beveiliging

Veelal wordt in het privacyreglement een bepaling opgenomen in de trant van: er zijn passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking – waarbij die technische en organisatorische maatregelen vervolgens uitgewerkt zijn in andere reglementen, bv. het reglement ICT-gebruik, het beveiligingsbeleid, etc.

4.5 Kenbaarheid en bruikbaarheid

Niet alle instellingen hebben regels, en de regels van de instellingen die ze wel hebben verschillen nogal in kwaliteit en abstractieniveau. Sommige instellingen hebben zich beperkt tot, eigenlijk, het overnemen van de Wbp, anderen hebben zich wat meer moeite getroost en hebben geprobeerd de Wbp te vertalen naar de eigen onderwijssituatie. Maar het mooiste reglement heeft slechts een zeer beperkte waarde als het niet kenbaar en bruikbaar is voor de docenten en secretariaatsmedewerkers die in de dagelijkse praktijk, heel af en toe, met kwesties rond persoonsgegevens van studenten geconfronteerd worden.

Om te beginnen is natuurlijk bewustzijn het allerbelangrijkst. Iedereen die in het hoger onderwijs met persoonsgegevens van studenten werkt, moet zich ervan bewust zijn dat hiervoor privacyregels gelden, en dat naleving van die regels belangrijk is. Zowel om het recht op privacy van studenten niet in gevaar te brengen, als om de reputatie van de instelling te beschermen. Als dat bewustzijn er niet is, hebben regels ook niet zoveel zin.

Als dat bewustzijn er wèl is, dan is het belangrijk dat medewerkers die een vraag hebben (bijvoorbeeld of ze nou wel of geen studieresultaten aan een klasgenoot of een ouder mogen verstrekken) het antwoord op die vraag snel en gemakkelijk in een reglement kunnen vinden – of dat ze die vraag aan iemand kunnen voorleggen die een antwoord weet. Hoewel dit punt niet systematisch onderzocht is, lijkt hier (op basis van een rondgang langs enkele docenten in het hoger onderwijs) wel ruimte voor verbetering te zijn. Bijvoorbeeld: het bestaan bij een universiteit van een prachtig naslagwerk over hoe met vragen om informatie over studenten om te gaan is bij velen "op de werkvloer" niet bekend, en zo kan het als nog misgaan.

En als dan er bewustzijn is, en het is bekend dat er regels zijn (en die regels kunnen ook gevonden worden, bijvoorbeeld op het intranet) – dan is nog de vraag of die regels ook voldoende duidelijk geformuleerd zijn om echt een handvat te bieden voor de praktijk. Zou een docent, die zijn kast wil opruimen en dozen met oude tentamens wil weggooien, wel iets hebben aan een bepaling als: "Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld en verwerkt"? Weet die docent of tentamens persoonsgegevens zijn, voor welk doel die verzameld zijn, of dat doel inmiddels verwezenlijkt is, en of ze, dus, weggegooid moeten of mogen worden? En zou een secretaresse die bezoek krijgt van de politie, de

moed hebben om niet het adres of het rooster van een bepaalde student mede te delen?

Hoofdstuk 5. Praktijk van alledag

Hoewel in het voorgaande al wel steeds met concrete voorbeelden geprobeerd is de materie wat minder abstract te maken, maakt dit hoofdstuk echt de overstap van de theorie naar de praktijk. Een aantal alledaagse voorbeelden zal aan de orde komen, waar, bezien vanuit de eerder genoemde bril van de Wbp-compliance, vraagtekens gezet kunnen worden. De voorbeelden zijn heel divers, en ontleend aan eigen ervaringen en gesprekken met docenten en secretariaatsmedewerkers, en aan het redactioneel van "het Onderwijsblad", in de inleiding genoemd.

5.1 Oude websites

Zeker in de tijd van voor de elektronische leeromgevingen zoals Blackboard werden er nog wel eens ad-hoc websites opgezet voor een bepaald doel: bij een vak (als ELO avant la lettre), voor een evenement, of om aan een gemeenschappelijk project te werken. Deze sites zijn soms niet echt weggehaald, vaak zijn ze alleen niet meer via een link bereikbaar – maar nog wel als de URL gewoon ingetikt wordt. En het kan zijn dat zo'n site ook nog steeds opduikt bij de zoekresultaten van Google, als bijvoorbeeld gezocht wordt op de naam van een student wiens naam op die site voorkomt.

Datzelfde probleem schijnt zich voorgedaan te hebben als veiligheidslek van cloud-toepassingen als Blackboard en Medusa, volgens Het Onderwijsblad en Elsevier.nl,[12] de berichten die mede aanleiding waren voor dit rapport.

Niet alleen informatie die als webpagina (.html) beschikbaar is gesteld, maar ook "gewone" bestanden (zoals Word, Excel en pdf-bestanden) kunnen via een rechtstreekse URL voor iedereen beschikbaar zijn – ook al is dat niet altijd de bedoeling en is men zich daar wellicht misschien niet eens van bewust. Plaatsing op een (mede) extern toegankelijke netwerkschijf kan in sommige gevallen al voldoende zijn.

Die gegevens zijn niet meer nodig voor het doel waar ze ooit voor verzameld waren (vereiste van doelbinding), en ze worden aan de buitenwereld via internet beschikbaar gesteld, terwijl daar geen reden (meer) voor is. Weghalen dus, en zorgen dat niets meer voor buitenstaanders via internet te zien is.

5.2 Cijferlijsten

Vroeger was het gebruikelijk om lijsten met cijfers op prikborden op te hangen. Soms gewoon alfabetisch op naam, soms nog steeds in alfabetische volgorde maar dan zonder naam maar met alleen een studentnummer, en soms zonder naam en gesorteerd op studentnummer. Dat was dan vanwege de "privacy". Uiteraard een nobel streven, en natuurlijk "helpt" het wel iets, maar de vraag is of

[12] A. Kersten, Help, mijn privacy lekt weg! Vertrouwelijke gegevens van onderwijsinstellingen op straat, redactioneel "het Onderwijsblad", 3 oktober 2010 en "Gevoelige informatie studenten Utrecht jaren openbaar", Elsevier.nl van 2 september 2009.

het voor een ”derde” mogelijk is om aan de hand van een studentnummer achter de identiteit van de betrokken student te komen. In de praktijk was dat vaak niet zo heel lastig.

Uiteraard is een prikbord in de hal van een universiteitsgebouw openbaar – maar toch op een andere manier dan het internet openbaar is. Je kunt er gevoeglijk van uit gaan dat op het moment dat het lijstje door de docent verwijderd wordt, de cijfers ook echt niet meer te vinden zijn. En omdat iemand, om de cijfers te raadplegen, fysiek naar de plek toe moet waar ze hangen (en dan moet zij ook nog weten dat ze daar hangen) is een geanonimiseerde, op studentnummer gesorteerde cijferlijst op een prikbord toch een ander verhaal dan exact datzelfde lijstje op het openbare internet (of een besloten intranet of cloud-toepassing die een lek blijkt te bevatten).

Want dan zijn die cijfers wellicht op studentnummer te vinden via een zoekmachine. En zijn ze misschien voor onbepaalde tijd vindbaar (via de cache van de zoekmachine, via iemand die het lijstje gekopieerd en hergepubliceerd heeft, of domweg via zoiets als archive.org). Via diezelfde zoekmachine is wellicht ook wel een naam bij een studentnummer te vinden en vice versa; bijvoorbeeld omdat een mede-student een groepspaper op zijn blog zet, waar de namen en studentnummers van de auteurs op het titelblad prijken.

ELO’s hebben over het algemeen wel een faciliteit om cijfers aan een student te communiceren op een manier dat alleen de student zelf (althans iemand die haar inloggegevens weet) die cijfers kan zien; bijvoorbeeld het GradeBook op WebCT. Toch komt het regelmatig voor dat de complete lijst op de beginpagina van een vak gezet wordt. Waarom? Omdat de betreffende docent of onderwijssecretariaatsmedewerker geen weet heeft van de GradeBook faciliteit, omdat het gemakkelijker en sneller is om de hele lijst erop te zetten, èn omdat men zich niet voldoende bewust is van het belang van het recht op informationele privacy van studenten. Een student hoort zelf te kunnen bepalen wie zij op de hoogte wil brengen van haar studieresultaten – en wie niet.

Persoonsgegevens van studenten (cijfers) worden dus zonder grondslag beschikbaar gesteld aan derden (andere studenten, en anderen die toegang hebben tot de ELO), in strijd met de Wbp.

5.3 Elektronische leeromgeving

Los nog van de hiervoor besproken kwestie van de cijferlijsten in de ELO, moet een onderwijsinstelling in het algemeen ook bij gebruik van een ELO zorgvuldig omgaan met studentgegevens. Het is dan wel zo dat in een ELO per cursus een afgeschermde omgeving gecreeerd wordt (kan worden) – maar het is soms ook mogelijk om met een gastaccount, of als demo-student binnen te komen. En soms zitten er wel heel veel studenten in een cursus. Kortom: zet zo min mogelijk persoonsgegevens van studenten in de ELO, en haal ze er weer af als ze niet meer nodig zijn.

5.4 Studieverenigingen / sociale netwerksites / alumninetwerk

Instellingen doen er goed aan om zich bewust te zijn van de gevaren die allerlei op sociaal verkeer gerichte initiatieven met zich brengen voor de privacy van hun studenten. Natuurlijk is het leuk als de rugbyvereniging een oudledenevenement wil organiseren. Maar als de instelling dan gaat helpen bij het opsporen van uit het oog verloren oudleden, door de namenlijst te vergelijken met wat bij haar bekend is over haar eigen alumni en dan de contactgegevens doorspeelt – dan handelt zij in strijd met de Wbp. Tenzij natuurlijk de betrokken alumni, bij gelegenheid van hun opname in het alumniregister, ondubbelzinnig toestemming hebben gegeven voor dit soort verstrekking.

Meer in het algemeen geldt dat instellingen best social-networking kunnen stimuleren en faciliteren, maar altijd uitsluitend met toestemming van de betrokkenen.

5.5 Contacten met de buitenwereld

Docenten en onderwijssecretariaten worden nog wel eens benaderd door "derden" die iets willen. Een biochemisch bedrijf wil een leuke activiteit organiseren voor bijna afgestudeerden met bepaalde specialistische kennis, een bezorgde vader wil weten of zijn dochter niet vastgelopen is met haar scriptie, een student wil graag weten of er nog meer studenten zijn wiens ouders in Gaasterland wonen.

Ook als er geen enkele reden is om te twijfelen aan de goede bedoelingen van deze "derden" is het belangrijk om geen details over studenten bekend te maken aan deze derden. Ook niet aan ouders! Tenzij met uitdrukkelijke toestemming van de betrokken student. Wat wel kan (maar vaak meer werk oplevert) is zelf het verzoek doorspelen aan de betrokkenen, zodat zij, indien gewenst, contact op kunnen nemen.

5.6 Onderling

Eigenlijk geldt dat ook binnen de onderwijsinstelling, tussen bijvoorbeeld collegadocenten. Het gaat niet aan (is een inbreuk op de informationele privacy van de betrokken student) om bij de koffie-automaat gedrag of cijfers van een met name genoemde student met collega's te bespreken – tenzij daar een objectief gerechtvaardigde reden voor is.

Een mooi voorbeeld daarvan is brief die aan een student gestuurd werd – en in afschrift (met naam en adres van de betrokken student in het briefhoofd en de aanhef) aan alle docenten:

> "*U stelt ons echter keer op keer voor problemen, bijvoorbeeld door te laat te verschijnen bij afspraken en onderwijs, onvoldoende inzet te tonen, bovengemiddeld vaak in beroep te gaan, vaak te zakken of te verzuimen bij toetsen of tentamens, onevenredig veel e-mails te sturen, verzoeken in te dienen bij verkeerde instanties, geen of onjuiste keuzes te maken t.a.v. de studie, enz. Al met al levert u het departement buitensporig veel werk op en is een situatie ontstaan die niet op deze wijze voort mag duren*."
>
> Er wordt aangegeven welke vakken hij nog moet doen, en vervolgens:

> "*U besteedt absoluut geen tijd en aandacht aan onderdelen die in bovenstaand overzicht niet voorkomen, niet binnen het departement en ook niet daarbuiten; u doet derhalve ook geen verzoeken inzake dergelijke onderdelen.*
> *U doet vanaf heden geen enkel verzoek meer voor bijzondere voorzieningen of voor afwijkingen va de bovenstaande regels, behoudens in de situaties van aantoonbare overmacht of medische noodzaak, zoals hieronder nader omschreven.*
> *U stuurt geen brieven of e-mails aan docenten, Examencommissie of andere instanties, anders dan waar nodig in de hieronder genoemde situaties van aantoonbare overmacht of medische noodzaak.*
> *U gaat ook niet meer in beroep tegen tentamenuitslagen, beslissingen van de Examencommissie of andere beslissingen.*
> *Zou u dit, ondanks dit bericht, toch doen, dan mag u daarop geen reactie verwachten.*
> *(…)*
> *Tenslotte berichten wij u dat over dit schrijven niet wordt gecorrespondeerd*. "

Dit was blijkbaar een extreem voorbeeld, waarin naar het lijkt wel een objectief gerechtvaardigde reden was voor het verspreiden van dit bericht onder alle docenten. Normaal gesproken moet echter iedere student ervan uit kunnen gaan dat een docent hem "blanco" tegemoet treedt, en niet al allerlei details over hem weet.

5.7 Toespraken

Bij gelegenheid van buluitreikingen worden studenten soms in het openbaar individueel toegesproken. Dat is natuurlijk vooral bedoeld om de student in het zonnetje te zetten. Een persoonlijke noot is dan bedoeld om de student, en zijn ouders en andere genodigden in de zaal, het gevoel te geven dat het ook echt over deze student gaat en niet een algemeen praatje is wat voor alle studenten geldt. Het wordt over het algemeen gewaardeerd door ouders als zij hun kind kunnen herkennen in de toespraak, dat maakt het persoonlijker, minder afstandelijk.
Aan die toespraken zit natuurlijk ook een keerzijde. De zitting is openbaar, in principe kan iedereen naar binnen. Soms worden in die toespraken persoonlijke details vermeld, waarvan niet meteen voor de hand ligt dat de betrokken student wil dat iedereen dat weet. Bijvoorbeeld zoiets als: "Je hebt het een tijd erg moeilijk gehad na de dood van je vader/moeder/vriend, maar het is je toch gelukt om je studie zonder al te veel vertraging af te ronden." Nou geldt voor die toespraken natuurlijk in zekere zin hetzelfde als voor de papieren cijferlijsten op het prikbord: in principe moet je fysiek aanwezig zijn om er kennis van te kunnen nemen. Toch weet de instelling niet wie er in de zaal zitten, wie aantekeningen maakt of filmt, en wat er met die aantekeningen of films gebeurt.

Een oplossing zou zijn om de toespraak vooraf voor te leggen aan de student en hem om toestemming te vragen – maar dan is het verrassingselement voor de student van de toespraak af, en daarmee een deel van de feestelijkheid. Docenten die toespraken schrijven en houden moeten zich hier wel van bewust zijn, en zich afvragen of de betrokken student geen bezwaar zou hebben tegen het noemen van bepaalde persoonlijke details.

5.8 Plagiaatcontrole

Ook via plagiaatcontrolesoftware zoals Urkund kunnen persoonsgegevens van studenten bij anderen terechtkomen. Als er een "match" is tussen een nieuw document en een document dat al in de Urkund-database is opgeslagen, dan kan de "nieuwe" docent dat opgeslagen document inzien - inclusief de gegevens die de auteur over zichzelf, bv. op het titelblad, heeft vermeld. Belangrijk is wel dat de student die het nieuwe document instuurt, die gegevens niet te zien krijgt.

Natuurlijk is er in dit geval een gerechtvaardigd doel (namelijk: preventie van plagiaat), en het lijkt ook duidelijk dat de docent het document moet kunnen vergelijken met het document waaruit zou zijn overgenomen. Maar het is misschien wel goed om studenten erop te wijzen, dat als zij (verplicht) documenten ter controle naar zo'n plagiaatcontrole-applicatie sturen, die documenten door die applicatie opgeslagen worden en aan andere docenten ter beschikking gesteld worden als er een verdenking is dat een andere student iets uit dat document heeft overgenomen.

Overigens wordt bij het insturen van een document de student er wel op gewezen dat hij ervoor kan kiezen om zijn document niet in de database van het plagiaatcontrolesysteem op te laten nemen. Dat is dan meer met het oog op auteursrecht; opname in dat systeem is immers een vorm van verveelvoudiging waar de auteur toestemming voor moet geven.[13] Maar als bij-effect heeft het niet geven van toestemming ook tot gevolg dat de persoonsgegevens van de auteur niet opgeslagen worden.

5.9 Universiteitsblad, instellingskrant

Sommige studenten halen het instellingsnieuws, door een sportprestatie, een ingezonden brief, een advertentie. Net als "gewone" kranten zijn ook instellingskranten tegenwoordig in digitale archieven beschikbaar - en die archieven zijn doorzoekbaar, onder meer op naam. Ook op die manier zijn dus persoonsgegevens van studenten te achterhalen.

Advertenties (met telefoonnummers en emailadressen) staan over het algemeen niet in de digitale archieven. Voor wat betreft artikelen en ingezonden stukken: als indertijd publicatie in een krant toegestaan was, dan is ook archivering van de kranten toegestaan. Zie hierover bijvoorbeeld de uitspraak van de Raad van State van 8 september 2010 met betrekking tot het archief van het Universiteitsblad Groningen, LJN BN6172.[14] De Raad oordeelde dat de universiteit als "verantwoordelijke" in de zin van de Wbp is aan te merken. Het belang van een betrouwbaar en representatief archief rechtvaardigde in dit geval de verwerking van persoonsgegevens. In de belangenafweging tussen het privacybelang van de betrokkene en het belang van vrijheid van meningsuiting en de betrouwbaarheid en representativiteit van het archief, woog laatstgenoemd belang zwaarder – maar wel: "gezien de beperkte aard van de mededeling" die over de betrokkene is gedaan, en het feit dat hij indertijd met het artikel in de Universiteitskrant ingestemd had.

[13] art. 1 Aw.
[14] Uitspraak is te vinden door het LJN-nummer in te tikken op www.rechtspraak.nl.

5.10 Conclusie

Ook als een instelling de technische beveiliging op orde heeft, goede afspraken gemaakt heeft met dienstverleners en een deugdelijk reglement heeft, dan nog kan het voorkomen dat persoonsgegevens van studenten bij anderen terechtkomen op een manier die in strijd is met de wet. Privacy-bewustzijn is een belangrijke schakel, de docent en de secretariaatsmedewerker spelen hierbij een cruciale rol.

Hoofdstuk 6: Conclusie en aanbevelingen

Hoe moeten instellingen in het hoger onderwijs op de werkvloer invulling geven aan de normen die de Wbp stelt aan de omgang met persoonsgegevens van studenten? Het algemene antwoord is: Door vanuit een instellingsbreed gedragen privacybewustzijn op de werkvloer zorgvuldig met die gegevens om te gaan, aan de hand van bruikbare en kenbare regels.

De inventarisatie die in het kader van dit onderzoek bij de instellingen voor hoger onderwijs gedaan is, leert dat de instellingen in het algemeen best veel geregeld en ook opgeschreven hebben. Hiervan is verslag gedaan in hoofdstuk 4. Het probleem is dat deze regels op de werkvloer niet altijd kenbaar en bruikbaar zijn.

Kenbaar: Als de docenten en secretariaatsmedewerkers niet van het bestaan van de regels afweten, of ze niet snel en gemakkelijk kunnen vinden, dan hebben de regels slechts een zeer beperkte waarde. Kenbaarheid van de regels is in dit onderzoek niet systematisch onderzocht, maar het lijkt erop dat er wel ruimte is voor verbetering. Een link naar de regels, op een voor de hand liggende plaats op het intranet voor medewerkers is een goede oplossing. En er moet een toegankelijke vraagbaak zijn voor medewerkers: iemand van kennis van zaken, die vragen kan beantwoorden en kan helpen.

Bruikbaar: De regels moeten daarnaast voldoende duidelijk geformuleerd zijn om echt en handvat te bieden voor de praktijk. Dat betekent dat het letterlijk overnemen van de regels van de Wbp niet voldoet; de regels moeten ingevuld en toegespitst worden, zodat een docent met een vraag in die regels een duidelijk antwoord vindt.

Die kenbare en bruikbare regels moeten aangeven dat bijvoorbeeld het volgende moet gebeuren: oude websites moeten verwijderd worden, cijfers mogen alleen aan de betreffende student zelf gecommuniceerd worden, gegevens mogen niet voor andere doelen gebruikt worden, aan derden mogen geen inlichtingen over studenten gegeven, oude bestanden moeten worden verwijderd en dozen met oude tentamens, werkstukken en presentielijsten moeten vernietigd worden. Dit soort zaken moet in een beleid vastgelegd zijn, en er moet op worden toegezien dat dit beleid ook uitgevoerd wordt.

Het belangrijkste is privacybewustzijn bij hen, die met studentgegevens omgaan. En dan niet een bewustzijn in de zin van: er zijn allerlei lastige en vervelende regeltjes die ons beperken in ons dagelijks werk. Maar: inzicht in waarom privacy belangrijk is: omdat respect voor een student als persoon meebrengt dat die student zelf moet kunnen bepalen wie wat over hem of haar weet. Voorlichting en educatie dus, met de nadruk op het waarom. Misschien iets om tijdens een onderwijsevenement voor docenten, of bij bijscholing, eens aan de orde te stellen.

Het doel van dit alles is: het waarborgen van het recht op privacy van studenten, en het beschermen van de reputatie van de instelling.

Bijlage 1: De relevante bepalingen uit de Wet bescherming persoonsgegevens en Vrijstellingsbesluit

Vrijstellingsbesluit: Artikel 19. Leerlingen, deelnemers en studenten

1. Artikel 27 van de wet is niet van toepassing op verwerkingen van instellingen voor onderwijs betreffende hun leerlingen, deelnemers of studenten, voor zover deze verwerkingen voldoen aan de in dit artikel vermelde eisen.
2. De verwerking geschiedt slechts voor:
   a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, deelnemers of studenten, dan wel het geven van studieadviezen;
   b. het verstrekken of ter beschikking stellen van leermiddelen;
   c. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen;
   d. het behandelen van geschillen en het doen uitoefenen van accountantscontrole;
   e. de uitvoering of toepassing van een andere wet.
3. Geen andere persoonsgegevens worden verwerkt dan:
   a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, alsmede bank- en girorekeningnummer van de betrokkene;
   b. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
   c. nationaliteit en geboorteplaats;
   d. gegevens als bedoeld onder a, van de ouders, voogden of verzorgers van leerlingen, deelnemers of studenten;
   e. gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de betrokkene;
   f. gegevens betreffende de godsdienst of levensovertuiging van de betrokkene, voor zover die noodzakelijk zijn voor het onderwijs;
   g. gegevens betreffende de aard en het verloop van het onderwijs, alsmede de behaalde studieresultaten;
   h. gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen;
   i. gegevens met het oog op het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten;
   j. andere dan de onder a tot en met i bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.
4. De persoonsgegevens worden slechts verstrekt aan:
   a. degenen, waaronder begrepen derden, die leiding geven aan of belast zijn met de in het tweede lid bedoelde activiteiten of die daarbij noodzakelijk zijn betrokken;

b. anderen, in de gevallen bedoeld in artikel 8, onder a, c en d, of artikel 9, derde lid, van de wet;
c. anderen, in de gevallen bedoeld in artikel 8, onder e en f, van de wet, voor zover het slechts gegevens betreft als bedoeld in het derde lid, onder a, en nadat het voornemen daartoe aan de betrokkene of diens wettelijk vertegenwoordiger is medegedeeld en deze gedurende een redelijke termijn in de gelegenheid is geweest het recht als bedoeld in artikel 40 of 41 van de wet uit te oefenen.

5. De persoonsgegevens worden verwijderd uiterlijk twee jaren nadat de studie is beëindigd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.