Bijlagen

Bijlage A – Inventarisatieschema gegevensverwerkingen DARO

	Toelichting	Antwoord (in te vullen door intern verantwoordelijke afdeling, evt. in overleg met de IT-afdeling)
Naam systeem		The Raiser's Edge
Onderdeel	A	-
Doel systeem	B	Gestructureerd opslaan van o.a. NAW gegevens ter ondersteuning van het doel van de afdeling Development & Alumni Relations: "een zodanige band realiseren, onderhouden en versterken met alumni, bedrijven en fondsen overeenkomstig de missie en ambities van onze universiteit, zodat die partijen de universiteit financieel danwel in natura willen ondersteunen om de universiteit te laten excelleren en promoten". In het dagelijks leven zorgt Raiser's Edge voor ondersteuning bij zowel fondsenwerving als alumni-relatiebeheer. Ten aanzien van de fondsenwerving leggen wij vast hoe hoog de donatie is, over welke termijnen die wordt afgeschreven en van welke bankrekening. Verder leggen wij nauwkeurig vast wie wanneer gevraagd is om een donatie, om "over-solliciting" te voorkomen. Ook wordt bijgehouden wie er niet voor fondsenwerving, maar wel voor alumnirelaties wil worden benaderd (of welke combinatie dan ook). Ten aanzien van alumni relaties (het betrekken van alumni in onderwijs via mentorprogramma, voorzien van stages door alumni, en gastcolleges) houden wij NAW gegevens en ook werkgevegevens bij. Alumni hebben een belangrijke rol te vervullen in de realisering van het Tilburgs Onderwijs Profiel, vandaar dat werkgevergegevens relevant zijn. Daarnaast worden werkgevergegens gebruikt voor accreditatie doeleinden: waar komen onze studenten terecht en hoe relevant is de opleiding geweest in het bereiken van de arbeidsmarktpositie? Tevens kan de informatie gebruikt worden voor het bereiken van de internationaliseringsagenda: welke alumni werken in welk land, bij welke organisatie en zijn zij bereid Tilburg University te helpen bij het leggen van contacten in die landen/met die organisaties.
Is er een PIA uitgevoerd voor dit systeem en de verwerkingen?	C	Nee (niet dat wij weten - misschien wel naar aanleiding van vorige Inventarisatie Verwerking Persoonsgegevens, 2 jaar geleden)
Verantwoordelijke	D	Tilburg University
Intern verantwoordelijke	E	Hoofd Development en Alumnirelaties
Functioneel Beheerder	F	Functioneel Beheerder Development en Alumnirelaties
Technisch	G	LIS (teamleider OA)
Gebruiker(s)	H	Medewerkers van Development en Alumnirelaties, ERM, Career Services
Categorieen personen/ betrokkenen waarvan persoonsgegevens worden verzameld	I	Alumni (inclusief medewerkers) Corporate Relaties Non-Corporate Relaties: partijen (geen alumni, geen medewerker, geen corporate relatie) die met onze afdeling een relatie aangaan (bv studenten die doneren, crowdfunding donateurs)

Informatie over de persoonsgegevens	J	1. Soort gegevens	2. Grondslag verwerking	3. Aard gegevens/ Risico Klasse	4. Standaard verstrekkingen + doel verstrekking	5. Rechtstreekse toegang	6. Vrijstellingsbesluit	7. Herkomst gegevens
		ANR/UID medewerker/alumnus/relati	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris
		Intern adres medewerker	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		SAP
		(oud)Lidmaatschap TiU/alumni/studie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Titelatuur alumnus/relatie/relatie	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Voorletters alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Roepnaam alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Doopnaam alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Tussenvoegsels alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Achternaam alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Geboortedatum alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Geboorteplaats alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Geboorteland alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Geslacht alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Nationaliteit alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Adres alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Postcode alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Woonplaats alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Land alumnus/relatie	4. Vitaal belang	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Huis Telefoonnummers alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Mobiele telefoonnummers alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Bedrijfs telefoonnummers	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Emailadres alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Oud adres alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris / alumnus / relatie
		Afgeronde studies TiU alumnus/relatie (ba/ma, faculteit, beoordeling, studierichting, datum)	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris
		Vooropleiding alumnus/relatie	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		Osiris
		Bankrekening alumnus/relatie (innen	1. toestemming	1	Geen	Functioneel beheer		alumnus / relatie
		Donatiegegevens	1. toestemming	1	Geen	Functioneel beheer		alumnus / relatie
		Donatiegegevens in natura/Volunteerjobs tbv TiU of alumnirelaties (mentor, gastcolleges etc)	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		alumnus / relatie
		(persoonlijke) contactinformatie met alumnus / medewerker / relatie (mailings, email, telefoon, post)	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		Mailplus. Mailbox relatiemanager/alumnimail box. Alumnus/relatie
		contactvoorkeuren alumnus / relaties	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		alumnus / relatie
		Aanmeldingen en aanwezigheid TiU	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		alumnus / relatie
		werkgever - gegevens (naam functie, naam werkgever, contactgegevens werkgever, evt. linkedin link)	6. Gerechtvaardigd belang,relatiebeheer	0	Geen	Functioneel beheer		LinkedIn / alumnus
		relaties tussen alumni/relatie (bv	6. Gerechtvaardigd belang,relatiebeheer	1	Geen	Functioneel beheer		alumnus / relatie

Derde(n)	K	-
Beveiliging van het systeem	L	**Wat betreft het systeem**: Blackbaud is de leverancier van het software pakket (welke een Nasdaq listed bedrijf is). Er komen regelmatig updates voor het pakket beschikbaar. Deze updates worden altijd uitgevoerd, het pakket is gehost door LIS op een Windows server, gebruiker hiervoor de standaard security van de software.
Bewerker	M	-
Voorgenomen buitenlandse verstrekkingen + omschrijving doel	N	-
Looptijd/ bewaartermijn (+	O	Oneindig

Bijlage B – Privacyreglement TiU

Regelement bescherming persoonsgegevens relaties Universiteit van Tilburg

Dit reglement bevat, conform de Wet bescherming persoonsgegevens, regels voor een zorgvuldige omgang met het verzamelen en verwerken van persoonsgegevens van relaties van de universiteit. De bijlage bevat een korte toelichting.

1 Begripsbepalingen

In dit reglement wordt in aansluiting bij en in aanvulling op de Wet bescherming persoonsgegevens, hierna te noemen de Wet, verstaan onder:
a. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare betrokkene;
b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
c. bestand: elk gestructureerd geheel van persoonsgegevens, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
d. verantwoordelijke: College van bestuur van de Universiteit van Tilburg, hierna te noemen College;
e. gebruiker: de door het College aangewezen functionaris die geautoriseerd is persoonsgegevens in een bestand in te voeren en/of te muteren, dan wel van de uitvoer van het bestand kennis te nemen;
f. beheerder: de door het College aangewezen functionaris die belast is met de dagelijkse zorg voor de verwerking van persoonsgegevens, voor de juistheid van de ingevoerde gegevens, alsmede voor het bewaren, verwijderen en verstrekken van gegevens;
g. bewerker: degene die ten behoeve van het College persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
h. toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de geregistreerde aanvaardt dat hem betreffende persoonsgegevens worden verwerkt;
i .verstrekken van persoonsgegevens uit het bestand: het bekend maken of ter beschikking stellen van persoonsgegevens.

2. Reikwijdte van het reglement

Dit reglement is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens van relaties van de Universiteit van Tilburg, alsmede op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

3 Algemeen toetsingskader

3.1 Doelbinding en rechtmatige grondslag
Persoonsgegevens van relaties worden slechts verzameld, verwerkt en gebruikt voor een bepaald, uitdrukkelijk omschreven en gerechtvaardigd doel en op een rechtmatige grondslag. Per afzonderlijke verwerking of samenhangende verwerkingen zijn in de bijlage bij dit reglement de doelen en grondslagen geformuleerd.
3.2 Gebruik van de persoonsgegevens
Persoonsgegevens worden alleen verwerkt op een wijze die verenigbaar is met de doeleinden waarvoor ze zijn verkregen.
3.3 Beoordeling verenigbaarheid
Bij de beoordeling of een verwerking verenigbaar is, als bedoeld in artikel 3.2, wordt in elk geval rekening gehouden met:
1. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
2. de aard van de betreffende gegevens;
3. de gevolgen van de beoogde verwerking voor de betrokkene;
4. de wijze waarop de gegevens zijn verkregen;
5. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.

4 Regels voor de verwerking van persoonsgegevens

4.1 Volgens algemeen toetsingskader
De verwerking van persoonsgegevens dient te voldoen aan het algemeen toetsingskader zoals genoemd in dit reglement.
4.2 Verwerking voor historische, statistische en wetenschappelijke doeleinden

Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden wordt als verenigbaar beschouwd, indien de nodige voorzieningen zijn getroffen ter verzekering dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden.

5 Beveiliging en bewaring van gegevens
5.1 Beveiliging
Het College treft de nodige maatregelen van technische en organisatorische aard om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.
5.2 Beperkte toegang
Uitsluitend de beheerder en geautoriseerde gebruikers hebben toegang tot (delen van) de vastgelegde gegevens, voor zover dat noodzakelijk is voor de uitoefening van de functie.Deze personen zijn gebonden aan een geheimhoudingsplicht, tenzij enig wettelijk voorschrift tot mededeling verplicht.
5.3 Bewaartermijn
Persoonsgegevens, die niet langer voor het doel noodzakelijk zijn, worden zo spoedig mogelijk verwijderd.
5.4 Bewaartermijn voor historische, statistische en wetenschappelijke doeleinden
Persoonsgegevens mogen langer worden bewaard dan bepaald in het vorige artikel voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard en de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

6 Verstrekking van persoonsgegevens
6.1 Verstrekking binnen en buiten de Universiteit van Tilburg
Per afzonderlijke verwerking of samenhangende verwerkingen is in het handboek “Inventarisaties verwerkingen persoonsgegevens” aangegeven aan welke personen binnen en buiten de organisatie welke persoonsgegevens worden verstrekt, gelet op het doel en de grondslag van de verwerking.

7 Kennisgeving
7.1 Algemene mededeling
Het College zal een relatie door middel van een algemene kennisgeving het bestaan van dit reglement meedelen, alsmede daarin aangeven op welke wijze het reglement kan worden ingezien en verkregen.

8 Rechten van betrokkenen
8.1 Algemeen
Iedere relatie heeft recht op inzage, verbetering, aanvulling, verwijdering of afscherming van vastgelegde persoonsgegevens, alsmede het recht van verzet zoals geformuleerd in deze paragraaf.

8.2 Recht op inzage
Een relatie heeft recht op inzage in haar betreffende verwerkte persoonsgegevens. Een verzoek hiertoe wordt schriftelijk ingediend bij het College.

8.2.1 Termijn
Op het verzoek wordt zo spoedig mogelijk, maar uiterlijk binnen vier weken na indiening schriftelijk gereageerd.

8.2.2 Afschrift
Elke relatie heeft op verzoek ten hoogste twee keer per jaar recht op een afschrift van de over haar opgenomen persoonsgegevens

8.2.3 Vergoeding van kosten
Voor het in 8.2.2 genoemde afschrift zal een vergoeding van administratieve kosten verlangd worden, welke bij vooruitbetaling dient te worden voldaan.

8.3 Verbetering, aanvulling, verwijdering of afscherming van vastgelegde persoonsgegevens

8.3.1 Verzoek tot verbetering, aanvulling, verwijdering of afscherming

Elke relatie kan met betrekking tot over haar opgenomen persoonsgegevens de beheerder van deze gegevens verzoeken deze te verbeteren, aan te vullen, te verwijderen, of af te schermen.

8.3.2 Kennisgeving aan betrokkene en aan derden

Indien de opgenomen persoonsgegevens van betrokkene feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn verwerkt, verbetert de beheerder deze gegevens. De beheerder deelt dat binnen vier weken na ontvangst van het in 8.3.1 genoemde verzoek schriftelijk aan de relatie mee. Bovendien worden derden aan wie de gegevens, voorafgaand aan de correctie, zijn verstrekt hiervan in kennis gesteld, tenzij dit onmogelijk is of een onevenredige inspanning kost.

8.3.3 Termijn voor uitvoering

De beheerder draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

8.4 Verzet

8.4.1 Gronden voor verzet

Indien gegevens worden verwerkt op grond van artikel 8, onder e en f van de Wet, kan de betrokkene daartegen bij het College te allen tijde verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.

8.4.2 Beslistermijn

Het College beoordeelt binnen vier weken na ontvangst van het verzet of het gerechtvaardigd is. Indien het verzet gerechtvaardigd is, treft het College maatregelen die nodig zijn om de verwerking te beëindigen.

8.4.3 Vergoeding van kosten

Het College zal voor het in behandeling nemen van een verzet een vergoeding van administratieve kosten verlangen, overeenkomstig lid 8.2.3 van dit reglement.

9 Rechtsbescherming

9.1 Algemene klachten

Indien een relatie van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit reglement jegens haar niet worden nageleefd, kan zij een schriftelijke klacht indienen bij het College.

De algemene klachtenregeling van de universiteit, opgenomen in hoofdstuk 4 van het ‘Bestuurs- en beheersreglement’, is van toepassing.

9.2 Bezwaarmogelijkheden na het indienen van een algemene klacht

Indien het antwoord van het College voor betrokkene niet leidt tot een voor hem acceptabel resultaat, heeft betrokkene de mogelijkheid bezwaar aan te tekenen conform de Wet.

9.3 Bezwaarmogelijkheden na afwijzing van een verzoek

Indien de verantwoordelijke afwijzend heeft beslist op een verzoek als bedoeld in de artikelen 8.2, of 8.3.1 of de verantwoordelijke het verzet van betrokkene zoals bedoeld in artikel 8.4.1 heeft afgewezen, kan betrokkene bezwaar aantekenen conform de Wet.

10 Overgangs- en slotbepalingen

10.1 Looptijd

Onverminderd eventuele wettelijke bepalingen is dit reglement voor onbepaalde tijd van kracht.

10.2 Wijziging van het reglement

Het College is bevoegd dit reglement te wijzigen of aan te vullen. Eveneens zal de bijlage van tijd tot tijd, indien nodig, gewijzigd of aangevuld worden.

10.3 Inwerkingtreding

Dit reglement treedt per 1 maart 2003 in werking.

Bijlage 1

Bijlage 1 bij: Reglement bescherming persoonsgegevens relaties Universiteit van Tilburg
Op 1 september 2001 is de Wet bescherming persoonsgegevens in werking getreden. Elke verwerking van een persoonsgegeven moet aan bepaalde voorwaarden voldoen en in overeenstemming zijn met de wettelijke gegevens.
Van relaties worden persoonsgegevens verwerkt in het kader van beheersactiviteiten. Een inventarisatie hiervan is opgenomen in het rapport 'Inventarisaties verwerkingen persoonsgegevens', dat ter inzage ligt op kamer A 161. In het algemeen dient hierbij gedacht te worden aan de volgende categorieën van bestanden:
*Studiekiezers (scholieren VWO 4,5,6)
Het doel hiervan is:
1. het organiseren van de ontvangst en verzending van documenten
2. de behandeling, de aanmaak, de afdoening en archivering van documenten
3. de communicatie met betrokkenen
4. het verzenden van informatie over de producten en diensten van de organisatie van de verantwoordelijke
5. het bijhouden van een overzicht van de verzonden informatie
6. het onderhouden van contact met betrokkenen

*Telefoon- en adressenlijst
Het doel hiervan is:
1. Communicatie met betrokkenen;
2. Onderhouden van contacten met betrokkenen

*Toegangsregistratie
Het doel hiervan is:
1. Intern beheer;
2. Bedrijfsbeveiliging;
3. Beveiliging van de toegang tot gebouwen en terreinen

*Cameratoezicht
Het doel hiervan is:
1. Bedrijfsbeveiliging;
2. Bescherming van de veiligheid en gezondheid van een of meer natuurlijke personen;
3. Beveiliging van de toegang tot gebouwen en terreinen;
4. Bewaking van zaken die zich in gebouwen of op bedrijventerrein bevinden;
5. Vastleggen van incidenten.

*Afnemers- en leveranciersbestand
Het doel hiervan is:
1. Berekenen en vastleggen van inkomsten en uitgaven;
2. Doen van betalingen of innen van vorderingen;
3. Onderhouden van contacten met afnemers en leveranciers

*Debiteuren- en crediteurenbestand
Het doel hiervan is:
1. Berekenen en vastleggen van inkomsten en uitgaven;
2. Doen van betalingen of innen van vorderingen;
3. Onderhouden van contacten met debiteuren en crediteuren.

*Administratie van gastsprekers
Het doel hiervan is:
1. Een overzicht van de gastsprekers die komen of geweest zijn;
2. Latere raadpleging voor bijvoorbeeld wederom een verzoek tot spreken bij Studium Generale.
3. Betaling van onkostenvergoeding aan de gastspreker.

*Database verzending nieuwsbrief Wetenschapswinkel
Het doel hiervan is:

1. Het bijhouden van een verzendlijst voor de nieuwsbrief aan klanten van de Wetenschapswinkel en andere geïnteresseerden.
*Alumnidatabase
Het doel hiervan is:
1. het onderhouden van contacten met betrokkenen;
2. het verzenden van informatie aan de betrokkenen;
3. het berekenen, vastleggen en innen van bijdragen en giften;
4. het bijhouden van een overzicht van de verzonden informatie;

Vergoeding van kosten
Iedere relatie heeft recht op inzage, verbetering, aanvulling, verwijdering of afscherming van vastgelegde persoonsgegevens alsmede het recht van verzet zoals geformuleerd bij de 'rechten van betrokkenen' in paragraaf 8 van het reglement.
Voor de administratieve kosten zal de UvT een vergoeding vragen overeenkomstig het in het 'Besluit kostenvergoeding rechten betrokkene' vastgelegde tarief. Dit tarief bedraagt momenteel voor een verzoek om inzage, respectievelijk het in behandeling nemen van een verzet 4.50 Euro.

Bijlage C – Protocol Datalekken TiU

Protocol meldplicht datalekken

Meldplicht datalekken

Op 1 januari 2016 gaat de Wet meldplicht datalekken in. Deze meldplicht houdt in dat organisaties die persoonsgegevens verwerken onmiddellijk een melding moeten doen bij de Autoriteit Persoonsgegevens (voorheen College bescherming persoonsgegevens) zodra er sprake is van een datalek. Of een datalek gemeld moet worden is afhankelijk van de (potentiële) impact van het datalek op de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van betrokkenen. In een aantal gevallen moet het datalek ook gemeld worden aan de betrokkenen van wie de persoonsgegevens zijn gelekt.

Bij een datalek is sprake van een inbreuk op de beveiliging waardoor persoonsgegevens verloren gaan of onrechtmatig worden verwerkt. Voorbeelden van (mogelijke) datalekken zijn bijvoorbeeld een kwijtgeraakte USB-stick waarop persoonsgegevens waren opgeslagen, een gestolen laptop of telefoon, het achterlaten van tentamenuitwerkingen in de trein, een harde schijf die wordt weggegooid zonder dat de onderzoeksdata die daarop stonden op de juiste wijze zijn gewist, een virus op een computer dat toegang heeft tot persoonsgegevens, een inbraak in een databestand door een hacker en een fout in een website waardoor persoonsgegevens van persoon A aan persoon B worden getoond.

In sommige gevallen zal de IT-afdeling kunnen zien dat er sprake is van een beveiligingsincident (bijvoorbeeld in het geval van een virus of hack), maar dat is natuurlijk niet altijd het geval. Daarom heeft TiU een Protocol meldplicht datalekken opgesteld, dat naar alle medewerkers wordt gecommuniceerd. Het is immers van belang dat iedere medewerker zo spoedig mogelijk intern een melding maakt van een mogelijk datalek, zodat door LIS en Legal Affairs beoordeeld kan worden wat de ernst is van het incident. Een datalek moet gemeld worden binnen 72 uur. Als er ten onrechte geen (tijdige) melding wordt gemaakt van een datalek, kan er een bestuurlijke boete worden opgelegd van (maximaal) 820.000 euro. Per 1 januari 2016 heeft Tilburg University een Functionaris voor de Gegevensbescherming aangesteld, die toezicht houdt op de naleving van de Wet bescherming persoonsgegevens.

Protocol meldplicht datalekken

Let op: bij twijfel, altijd een interne melding doen! Ga er in principe vanuit dat er sprake is van een meldenswaardig incident. Intern kan er beter teveel dan te weinig gemeld worden. De verantwoordelijke medewerkers bij LIS en Legal Affairs zullen beoordelen of er sprake is van een datalek dat bij de Autoriteit Persoonsgegevens gemeld moet worden.

In geval van diefstal of verlies van een gegevensdrager (laptop, gsm, usb-stick, externe harde schijf, etc.) dient u dit altijd te melden. Dit geldt ook voor hacking, digitale bedreiging, virussen, crypto-ware.

1. Is er sprake van verwerking van persoonsgegevens?

Voor wat betreft de interne melding van datalekken moet er al snel vanuit worden gegaan dat er sprake is van een verwerking van persoonsgegevens. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare persoon. Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden. Alle gegevens die met een persoon in verband gebracht kunnen worden zijn persoonsgegevens.

Voor de hand liggende gegevens zijn iemands naam, adres, postcodes met huisnummers, woonplaats en e-mailadres. Een administratienummer is een persoonsgegeven. Gevoelige gegevens als iemands ras (bijvoorbeeld een foto), godsdienst of gezondheid (bijvoorbeeld onderzoekdata met medische gegevens) worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd.

Als er sprake is van de verwerking van persoonsgegevens, ga naar stap 2.

2. Is er sprake van een (mogelijk) datalek?

Bij een datalek moet u denken aan alle (ook kleine) verzamelingen van persoonsgegevens die verloren gaan of in verkeerde handen kunnen vallen (bijvoorbeeld een kwijtgeraakte USB-stick waarop persoonsgegevens waren opgeslagen, een gestolen laptop of telefoon, het achterlaten van tentamenuitwerkingen in de trein, een harde schijf die wordt weggegooid zonder dat de onderzoeksdata die daarop stonden op de juiste wijze zijn gewist, een virus op een computer dat toegang heeft tot persoonsgegevens, een inbraak in een databestand door een hacker en een fout in een website waardoor persoonsgegevens van persoon A aan persoon B worden getoond). Niet ieder beveiligingsincident is een meldenswaardig datalek; deze beoordeling zal gedaan worden door LIS en Legal Affairs. Als er sprake is van de kans dat er persoonsgegevens verloren zijn geraakt, zijn gewist of in verkeerde handen zijn gevallen dan is er sprake van een beveiligingsincident, ga naar stap 3.

3. Intern melden

Doe per ommegaande intern melding van het incident, via datalek@tilburguniversity.edu. Geef hierbij een zo uitgebreid mogelijke beschrijving van het incident. Berichten die u stuurt naar deze mailbox komen terecht bij de security officer, het CERT-team, informatiebeveiliging, de functionaris voor de gegevensbescherming en Legal Affairs. Deze medewerkers zullen zo snel mogelijk na de melding contact met de melder opnemen en gezamenlijk en met u beoordelen of er sprake is van een datalek dat bij de Autoriteit Persoonsgegevens, en eventueel betrokkenen, moet worden gemeld. Bij deze beoordeling wordt gebruik gemaakt van de Beleidsregels van de Autoriteit Persoonsgegevens. Deze medewerkers zullen ook de eventuele melding bij de Autoriteit Persoonsgegevens verzorgen. Indien betrokkenen geïnformeerd moeten worden over een datalek, zal dat gebeuren in overleg met het verantwoordelijke organisatieonderdeel.
Als u contacten hebt met een externe bewerker van persoonsgegevens (bijvoorbeeld een derde partij die een systeem waar persoonsgegevens in zijn opgeslagen voor de universiteit host) en de bewerker meldt aan u dat er sprake is van een beveiligingsincident, dient u dit ook te melden via datalek@tilburguniversity.edu.
Vragen? Neem contact op met datalek@tilburguniversity.edu.

Bijlage D – Verwerkersovereenkomst TiU

DE ONDERGETEKENDEN:

- **Tilburg University[1],** gevestigd aan de Warandelaan 2 te Tilburg, Kamer van Koophandel nummer 41095855 en rechtsgeldig vertegenwoordigd door **[VERTEGENWOORDIGER]** (hierna: **"Verwerkingsverantwoordelijke"**);

- **[NAAM VERWERKER],** gevestigd aan het [ADRES] te [PLAATS], Kamer van Koophandel nummer [KVK] en rechtsgeldig vertegenwoordigd door **[VERTEGENWOORDIGER]** (hierna: **"Verwerker"**);

Hierna gezamenlijk te noemen: "**Partijen**" en individueel te noemen "**Partij**";

NEMEN HET VOLGENDE IN AANMERKING:

- Partijen hebben op <DATUM> een overeenkomst gesloten met kenmerk <KENMERK VAN DE OVEREENKOMST> met betrekking tot <ONDERWERP VAN DE OVEREENKOMST>. Ter uitvoering van de Overeenkomst verwerkt Verwerker ten behoeve van Verwerkingsverantwoordelijke Persoonsgegevens;
- In het kader van het uitvoeren van de Overeenkomst is <NAAM VERWERKER> aan te merken als Verwerker in de zin van de AVG en is Tilburg University aan te merken als Verwerkingsverantwoordelijke in de zin van de AVG;
- Partijen wensen zorgvuldig en in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens om te gaan met de Persoonsgegevens die ter uitvoering van de Overeenkomst verwerkt (zullen) worden;
- Partijen wensen in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens hun rechten en plichten ten aanzien van de Verwerking van Persoonsgegevens van Betrokkenen Schriftelijk vast te leggen in deze Verwerkersovereenkomst.

EN ZIJN ALS VOLGT OVEREENGEKOMEN:

ARTIKEL 1. DEFINITIES

In deze Verwerkersovereenkomst hebben de met hoofdletter geschreven begrippen de in dit artikel opgenomen betekenis. Waar de definitie in dit artikel in het enkelvoud is opgenomen, wordt ook het meervoud daaronder begrepen en vice versa, tenzij uitdrukkelijk anders vermeld of uit de context anders blijkt.

1.1 AVG: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de Verwerking van Persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.2 Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon op wie de Persoonsgegevens betrekking hebben, zoals bedoeld in artikel 4 onder 1) AVG.

1.3 Bijlage: een bijlage bij deze Verwerkersovereenkomst, die een integraal onderdeel vormt van deze Verwerkersovereenkomst.

1.4 Bijzondere categorieën Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een

[1] Tilburg University gaat uit van de Stichting Katholieke Universiteit Brabant

vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG.

1.5 Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om Persoonsgegevens te verwerken, zoals bedoeld in artikel 4 onder 10) AVG.

1.6 Dienst: de op grond van de Overeenkomst te leveren dienst(en) door Verwerker aan Verwerkingsverantwoordelijke.

1.7 Inbreuk in verband met Persoonsgegevens: een (vermoeden van een) inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, zoals bedoeld in artikel 4 onder 12) AVG.

1.8 Medewerker: de door Verwerker ingeschakelde werknemers en andere personen waarvan de werkzaamheden onder zijn verantwoordelijkheid vallen en die worden ingeschakeld door Verwerker ter uitvoering van de Overeenkomst.

1.9 Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een Derde, aan wie/waaraan de Persoonsgegevens worden verstrekt, zoals bedoeld in artikel 4 onder 9) AVG.

1.10 Overeenkomst: de overeenkomst die tussen Verwerkingsverantwoordelijke en Verwerker is gesloten en op grond waarvan Verwerker Persoonsgegevens ten behoeve van de uitvoering van deze overeenkomst voor Verwerkingsverantwoordelijke verwerkt.

1.11 Persoonsgegeven: alle informatie over een Betrokkene; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon, zoals bedoeld in artikel 4 onder 1) AVG.

1.12 DPIA: de gegevensbeschermingseffectbeoordeling (data protection impact assessment) die vóór de Verwerking ten aanzien van het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens wordt uitgevoerd, zoals bedoeld in artikel 35 AVG.

1.13 Schriftelijk: op schrift gesteld of langs de elektronische weg, zoals bedoeld in artikel 6:227a van het Burgerlijk Wetboek.

1.14 Sub-verwerker: een andere verwerker, waaronder maar niet beperkt tot groepsmaatschappijen, zustermaatschappijen, dochtermaatschappijen en hulpleveranciers, die Verwerker inschakelt om voor rekening van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten.

1.15 Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

1.16 Toezichthoudende autoriteit: één of meer onafhankelijke overheidsinstanties die verantwoordelijk is of zijn voor het toezicht op de toepassing van de AVG, teneinde de grondrechten en fundamentele

vrijheden van natuurlijke personen in verband met de Verwerking van hun Persoonsgegevens te beschermen en het vrije verkeer van Persoonsgegevens binnen de Unie te vergemakkelijken, zoals bedoeld in artikel 4 onder 21) en artikel 51 AVG. In Nederland is dit de Autoriteit Persoonsgegevens.

1.17 Verwerkersovereenkomst: de onderhavige overeenkomst inclusief Bijlagen, zoals bedoeld in artikel 28 lid 3 AVG.

1.18 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens, zoals bedoeld in artikel 4 onder 2) AVG.

ARTIKEL 2. VOORWERP VAN DE VERWERKERSOVEREENKOMST

2.1 De Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst. Bij tegenstrijdigheid tussen de bepalingen uit de Verwerkersovereenkomst en de Overeenkomst, prevaleren de bepalingen uit de Verwerkersovereenkomst.

2.2 De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen die plaatsvinden ter uitvoering van de Overeenkomst. Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

2.3 Verwerkingsverantwoordelijke geeft Verwerker opdracht en instructies om de Persoonsgegevens te verwerken namens de Verwerkingsverantwoordelijke. De instructies van Verwerkingsverantwoordelijke zijn nader omschreven in de Verwerkersovereenkomst en de Overeenkomst. Verwerkingsverantwoordelijke kan naar redelijkheid Schriftelijk aanvullende of afwijkende instructies geven.

2.4 Verwerker verwerkt de Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke en op basis van de instructies van Verwerkingsverantwoordelijke. Verwerker verwerkt de Persoonsgegevens uitsluitend voor zover de Verwerking noodzakelijk is ter uitvoering van de Overeenkomst, nimmer ten eigen nutte, ten nutte van Derden en/of voor reclamedoeleinden c.q. andere doeleinden, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

2.5 Verwerker en Verwerkingsverantwoordelijke leven de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens na. Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar mening van Verwerker een instructie van Verwerkingsverantwoordelijke inbreuk oplevert op de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

2.6 Indien Verwerker in strijd met de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker voor die Verwerkingen als Verwerkingsverantwoordelijke beschouwd.

ARTIKEL 3. VERWERKING VAN PERSOONSGEGEVENS

3.1 Voorafgaand aan het sluiten van de Verwerkersovereenkomst informeert Verwerker Verwerkingsverantwoordelijke in Bijlage A volledig en naar waarheid over de Verwerkingen die Verwerker ter uitvoering van de Overeenkomst uitvoert, tenzij in Bijlage A is opgenomen dat Verwerkingsverantwoordelijke de betreffende informatie in deze Bijlage opneemt. Verwerker is uitsluitend tot de in Bijlage A gespecificeerde Verwerkingen gerechtigd.

ARTIKEL 4. VERLENEN VAN BIJSTAND EN MEDEWERKING

4.1 Verwerker verleent Verwerkingsverantwoordelijke alle benodigde bijstand en medewerking bij het doen nakomen van de op Partijen rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens. Verwerker verleent Verwerkingsverantwoordelijke in ieder geval bijstand met betrekking tot:

(i) De beveiliging van Persoonsgegevens;

(ii) Het uitvoeren van controles en audits;

(iii) Het uitvoeren van DPIA's;

(iv) Voorafgaande raadpleging van de Toezichthoudende autoriteit;

(v) Het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie;

(vi) Het voldoen aan verzoeken van Betrokkenen;

(vii) Het melden van Inbreuken in verband met Persoonsgegevens.

4.2 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van Betrokkenen, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.2.1 Verwerker neemt alle redelijke maatregelen om ervoor te zorgen dat Betrokkene zijn rechten kan uitoefenen.

4.2.2 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten direct contact opneemt met Verwerker, dan gaat Verwerker hier – behoudens uitdrukkelijke andersluidende instructie van Verwerkingsverantwoordelijke – niet (inhoudelijk) op in, maar bericht Verwerker dit onverwijld aan Verwerkingsverantwoordelijke met een verzoek om nadere instructies.

4.2.3 Indien Verwerker de Dienst rechtstreeks aanbiedt aan Betrokkene, is Verwerker verplicht om Betrokkene namens de Verwerkingsverantwoordelijke te informeren over de Verwerking van de Persoonsgegevens van Betrokkene op een wijze die in overeenstemming is met de rechten van Betrokkene.

4.3 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.3.1 Indien Verwerker een verzoek of een bevel van een Nederlandse en/of buitenlandse overheidsinstantie ontvangt met betrekking tot Persoonsgegevens, waaronder maar niet beperkt tot een verzoek van de Toezichthoudende autoriteit, informeert Verwerker Verwerkingsverantwoordelijke onverwijld, voor zover dat wettelijk is toegestaan. Bij de behandeling van het verzoek of bevel neemt Verwerker alle instructies van Verwerkingsverantwoordelijke in acht en verleent Verwerker alle redelijkerwijs benodigde medewerking aan Verwerkingsverantwoordelijke.

4.3.2 Indien het Verwerker wettelijk is verboden om te voldoen aan zijn verplichtingen op grond van artikel 4.3.1, behartigt Verwerker de redelijke belangen van Verwerkingsverantwoordelijke. Hieronder wordt in ieder geval verstaan:

4.3.2.1 Verwerker laat juridisch toetsen in hoeverre: (i) Verwerker wettelijk verplicht is om aan het verzoek of bevel te voldoen; en (ii) het Verwerker daadwerkelijk is verboden om aan zijn verplichtingen jegens Verwerkingsverantwoordelijke op grond van artikel 4.3.1 te voldoen.

4.3.2.2 Verwerker werkt alleen mee aan het verzoek of bevel indien Verwerker hiertoe wettelijk verplicht is en waar mogelijk maakt Verwerker (in rechte) bezwaar tegen het verzoek of bevel of het verbod om Verwerkingsverantwoordelijke hierover te informeren of de instructies van Verwerkingsverantwoordelijke op te volgen.

4.3.2.3 Verwerker verstrekt niet meer Persoonsgegevens dan strikt noodzakelijk om aan het verzoek of bevel te voldoen.

4.3.2.4 Verwerker onderzoekt indien sprake is van doorgifte in de zin van artikel 9 de mogelijkheden om te voldoen aan de artikelen 44 tot en met 46 AVG.

ARTIKEL 5. TOEGANG TOT PERSOONSGEGEVENS

5.1 Verwerker beperkt de toegang tot Persoonsgegevens aan Medewerkers, Sub-verwerkers, Derden en andere Ontvangers van Persoonsgegevens tot een noodzakelijk minimum.

5.2 Verwerker verschaft uitsluitend toegang aan die Medewerkers voor wie ter uitvoering van de Overeenkomst deze toegang tot Persoonsgegevens noodzakelijk is. De categorieën Medewerkers zijn in Bijlage A gespecificeerd.

5.3 Verwerker verschaft Sub-verwerkers geen toegang tot Persoonsgegevens zonder voorafgaande algemene of specifieke Schriftelijke toestemming van Verwerkingsverantwoordelijke. Algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers is slechts verleend indien dit expliciet in Bijlage A is opgenomen. Specifieke toestemming voor het inschakelen van Sub-verwerkers is slechts verleend aan Sub-verwerkers die in Bijlage A zijn gespecificeerd.

5.4 Verwerker licht Verwerkingsverantwoordelijke in geval van algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers uiterlijk drie (3) maanden voorafgaand aan beoogde veranderingen inzake de toevoeging, vervanging of wijziging van Sub-verwerker(s), Schriftelijk in, waarbij de Verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken. Partijen treden hierop in onderhandeling.

5.5. De algemene of specifieke toestemming van Verwerkingsverantwoordelijke voor het inschakelen Sub-verwerkers laat de verplichtingen voor Verwerker voortvloeiende uit de Verwerkersovereenkomst, waaronder maar niet beperkt tot artikel 9, onverlet. Verwerkingsverantwoordelijke kan zijn algemene of specifieke Schriftelijke toestemming voor het inschakelen van Sub-verwerkers intrekken, indien Verwerker niet of niet langer voldoet aan de verplichtingen uit de Verwerkersovereenkomst, de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

5.6 Verwerker verstrekt op eerste verzoek van Verwerkingsverantwoordelijke een overzicht van de door Verwerker ingeschakelde Sub-verwerkers aan Verwerkingsverantwoordelijke.

5.7 Verwerker legt de in de Verwerkersovereenkomst opgenomen verplichtingen op aan de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers. Verwerker draagt er zorg voor dat de door Verwerker ingeschakelde (rechts)personen,

waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, de in de Verwerkersovereenkomst opgenomen verplichtingen naleven door middel van een Schriftelijke overeenkomst.

5.8 Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, in strijd handelen met de Verwerkersovereenkomst en/of de met Verwerker gesloten Schriftelijke overeenkomst zoals bedoeld in artikel 5.7.

5.9 Verwerker verstrekt op verzoek van Verwerkingsverantwoordelijke een afschrift van de Schriftelijke overeenkomst tussen Verwerker en de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers.

5.10 Verwerker blijft ten aanzien van de Verwerkingsverantwoordelijke volledig verantwoordelijk en volledig aansprakelijk voor het nakomen van de verplichtingen door de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, voortvloeiende uit de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens en de verplichtingen voortvloeiende uit de Overeenkomst en de Verwerkersovereenkomst.

ARTIKEL 6. BEVEILIGING

6.1 Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, opdat de Verwerking aan de vereisten van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet en de bescherming van de rechten van Betrokkenen is gewaarborgd. Verwerker treft hiertoe tenminste de technische en organisatorische maatregelen die zijn opgenomen in Bijlage B.

6.2 Verwerker treedt in een zo vroeg mogelijk stadium via de Algemene contactpersoon van de Verwerkingsverantwoordelijke in contact met de IT Security Officer (ITSO) of diens vervanger. Ten bewijze van het voldoen aan de in bijlage B genoemde OWASP-beveiligingsstandaard overlegt Verwerker een recent (jonger dan 12 maanden) IT Security rapport, uitgevoerd door een gerenommeerd IT-security bedrijf, eventueel onder een Non Disclosure Agreement. Indien Verwerker geen rapport wil of kan opleveren, dient Verwerker de Algemene contactpersoon en de ITSO daarover gemotiveerd te informeren. Verwerkingsverantwoordelijke beslist vervolgens of het rapport achterwege kan blijven.

6.3 Bij de beoordeling van het passende beveiligingsniveau houdt Verwerker rekening met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

6.4 Verwerker legt zijn beveiligingsbeleid Schriftelijk vast. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker inzage in het beveiligingsbeleid van Verwerker.

6.5 Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 AVG of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 AVG kan worden gebruikt als element om aan te tonen dat de in dit artikel bedoelde vereisten worden nageleefd.

ARTIKEL 7. AUDIT

7.1 Verwerker is verplicht periodiek een onafhankelijke, externe deskundige een audit te laten uitvoeren ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in

de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.2 Verwerker verricht tenminste een keer per twee jaar een periodieke audit, zoals bedoeld in artikel 7.1. Indien Bijzondere categorieën Persoonsgegevens worden verwerkt, verricht Verwerker tenminste eenmaal per jaar een periodieke audit zoals bedoeld in artikel 7.1.

7.3 Verwerker is enkel niet gehouden tot het verrichten van een periodieke audit zoals bedoeld in artikel 7.1, indien Verwerker uitsluitend Persoonsgegevens verwerkt met een laag risico en uitdrukkelijk in Bijlage A is opgenomen dat Verwerker niet gehouden is tot het verrichten van een periodieke audit. Verwerkingsverantwoordelijke stelt vast of er sprake is van een laag risico en neemt daarbij de Handreiking Auditverplichting (bijlage van het SURF Juridisch Normenkader (Cloud)services) in aanmerking.

7.4 Verwerker is verplicht de bevindingen van de onafhankelijke, externe deskundige, op verzoek aan Verwerkingsverantwoordelijke ter beschikking te stellen in de vorm van een verklaring, waarin de deskundige een oordeel geeft over de kwaliteit van de door Verwerker getroffen technische en organisatorische beveiligingsmaatregelen met betrekking tot de Verwerkingen die Verwerker ten behoeve van Verwerkingsverantwoordelijke verricht.

7.5 Verwerkingsverantwoordelijke heeft het recht om op zijn verzoek een audit te laten uitvoeren door een door Verwerkingsverantwoordelijke gemachtigde (rechts)persoon, ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.6 De kosten van de periodieke audit komen voor rekening van Verwerker. De kosten van de audit op verzoek van Verwerkingsverantwoordelijke komen voor rekening van Verwerkingsverantwoordelijke, tenzij uit de bevindingen van de audit blijkt dat Verwerker de bepalingen uit de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens niet is nagekomen. Deze bepaling laat de overige rechten van Verwerkingsverantwoordelijke, waaronder het recht op schadevergoeding, onverlet.

7.7 Indien tijdens een audit wordt vastgesteld dat Verwerker niet aan het bepaalde in de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet, neemt Verwerker onverwijld alle redelijkerwijs noodzakelijke maatregelen om te zorgen dat Verwerker hieraan alsnog voldoet. De bijbehorende kosten komen voor rekening van Verwerker.

ARTIKEL 8. INBREUK IN VERBAND MET PERSOONSGEGEVENS

8.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging en uiterlijk binnen 24 uur na kennisneming, over een Inbreuk in verband met Persoonsgegevens of een redelijk vermoeden van een Inbreuk in verband met Persoonsgegevens. Verwerker informeert Verwerkingsverantwoordelijke via de contactpersonen en de contactgegevens van Verwerkingsverantwoordelijke zoals opgenomen in Bijlage A en ten minste ten aanzien van hetgeen is opgenomen in Bijlage C. Verwerker garandeert dat de verstrekte informatie volledig, correct en accuraat is.

8.2 Indien en voor zover het voor Verwerker niet mogelijk is om alle informatie uit Bijlage C gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging en uiterlijk binnen 24 uur na het ontdekken, in stappen worden verstrekt aan Verwerkingsverantwoordelijke.

8.3 Verwerker heeft adequaat beleid en adequate procedures ingericht om Inbreuken in verband met Persoonsgegevens in een zo vroeg mogelijk stadium te detecteren, Verwerkingsverantwoordelijke

hierover uiterlijk binnen 24 uur te informeren, hierop adequaat en onmiddellijk te reageren, (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige Verwerking te voorkomen of te beperken en herhaling hiervan te voorkomen. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker informatie over en inzage in dit door Verwerker ingerichte beleid en deze door Verwerker ingerichte procedures.

8.4 Verwerker houdt Schriftelijk een register bij van alle Inbreuken in verband met Persoonsgegevens die betrekking hebben op of verband houden met de (uitvoering van de) Overeenkomst, met inbegrip van de feiten omtrent de Inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de getroffen corrigerende maatregelen. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker Verwerkingsverantwoordelijke een afschrift van dit register.

ARTIKEL 9. DOORGIFTE VAN PERSOONSGEGEVENS

9.1 Persoonsgegevens mogen enkel worden doorgegeven aan derde landen of internationale organisaties indien sprake is van een passend beschermingsniveau en Verwerkingsverantwoordelijke hiervoor specifieke Schriftelijke toestemming heeft verleend. Deze specifieke Schriftelijke toestemming is slechts verleend indien dit is opgenomen in Bijlage A. Verwerker is uitsluitend gerechtigd tot deze in Bijlage A gespecificeerde doorgiften aan derde landen of internationale organisaties, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

9.2 Verwerkingsverantwoordelijke kan aan de Schriftelijke toestemming, zoals bedoeld in artikel 9.1, nadere voorwaarden verbinden, waaronder maar niet beperkt tot het aantonen dat aan de vereisten zoals opgenomen in artikel 9.3 is voldaan.

9.3 Verwerkingsverantwoordelijke kan Verwerker slechts toestemming verlenen voor een doorgifte van Persoonsgegevens aan derde landen of internationale organisaties indien, ofwel:

(i) Een adequaatheidsbesluit overeenkomstig artikel 45 lid 3 AVG is genomen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(ii) Passende waarborgen overeenkomstig artikel 46 AVG met inbegrip van bindende voorschriften zoals bedoeld in artikel 47 AVG, zijn getroffen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(iii) Aan één van de specifieke voorwaarden uit artikel 49 lid 1 AVG is voldaan ten aanzien van het betreffende derde land of de betreffende internationale organisatie.

ARTIKEL 10. VERTROUWELIJKHEID VAN PERSOONSGEGEVENS

10.1 Alle Persoonsgegevens worden als vertrouwelijke gegevens gekwalificeerd en dienen als zodanig te worden behandeld.

10.2 Partijen houden alle Persoonsgegevens geheim en maken deze op geen enkele wijze verder intern of extern bekend, behalve voor zover:

(i) Bekendmaking en/of verstrekking van de Persoonsgegevens in het kader van de uitvoering van de Overeenkomst of Verwerkersovereenkomst noodzakelijk is;

(ii) Enig dwingendrechtelijk wettelijk voorschrift of rechterlijke uitspraak Partijen tot bekendmaking en/of verstrekking van die Persoonsgegevens verplicht, waarbij Partijen eerst de andere Partij hiervan op de hoogte stellen;

(iii) Bekendmaking en/of verstrekking van die Persoonsgegevens geschiedt met voorafgaande Schriftelijke toestemming van de andere Partij.

10.3 Overtreding van artikel 10.1 en/of artikel 10.2 wordt beschouwd als een Inbreuk in verband met Persoonsgegevens.

ARTIKEL 11. AANSPRAKELIJKHEID EN VRIJWARING

11.1 Verwerker is aansprakelijk voor alle schade die voortvloeit uit of verband houdt met het niet nakomen van de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

11.2 Verwerker vrijwaart Verwerkingsverantwoordelijke voor alle aanspraken, boeten en/of maatregelen van derden, daaronder begrepen Betrokkenen en de Toezichthoudende autoriteit, die jegens Verwerkingsverantwoordelijke worden ingesteld of opgelegd wegens een schending van de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens door Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers.

ARTIKEL 12. WIJZIGING

12.1 Verwerker is verplicht Verwerkingsverantwoordelijke onmiddellijk te informeren over voorgenomen wijzigingen in de Dienst, de uitvoering van de Overeenkomst en de uitvoering van de Verwerkersovereenkomst die betrekking hebben op de Verwerking van Persoonsgegevens. Hieronder wordt in ieder geval verstaan:

(i) Wijzigingen die invloed (kunnen) hebben op de te verwerken (categorieën) Persoonsgegevens;

(ii) Wijziging van de middelen waarmee de Persoonsgegevens worden verwerkt;

(iii) Het inschakelen van andere Sub-verwerkers;

(iv) Wijziging in de doorgifte van Persoonsgegevens aan derde landen en/of internationale organisaties.

12.2 Indien een wijziging met betrekking tot de Verwerking van Persoonsgegevens of een audit daartoe aanleiding geeft, treden Partijen op eerste verzoek van Verwerkingsverantwoordelijke in overleg over het wijzigen van de Verwerkersovereenkomst.

12.3 Verwerker is pas gerechtigd tot het uitvoeren van een wijziging als bedoeld in artikel 12.1, indien Verwerkingsverantwoordelijke daaraan voorafgaand Schriftelijk toestemming voor deze wijziging(en) heeft gegeven.

12.4 Wijzigingen die betrekking hebben op de Verwerking van Persoonsgegevens mogen nooit tot gevolg hebben dat Verwerkingsverantwoordelijke niet kan voldoen aan de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

12.5 In geval van nietigheid of vernietigbaarheid van één of meer bepalingen van de Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

ARTIKEL 13. DUUR EN BEËINDIGING

13.1 De duur van de Verwerkersovereenkomst is gelijk aan de duur van de Overeenkomst. De Verwerkersovereenkomst is niet los van de Overeenkomst te beëindigen. Bij beëindiging van de Overeenkomst eindigt de Verwerkersovereenkomst van rechtswege en vice versa.

13.2 Verwerkingsverantwoordelijke is gerechtigd de Verwerkersovereenkomst op te zeggen, indien Verwerker niet voldoet of niet langer kan voldoen aan de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zonder dat Verwerker aanspraak maakt op enige schadevergoeding. Bij de opzegging neemt Verwerkingsverantwoordelijke een redelijke opzegtermijn in acht, tenzij de omstandigheden onmiddellijke opzegging rechtvaardigen.

13.3 Binnen een maand nadat de Overeenkomst eindigt, vernietigt en/of retourneert Verwerker alle Persoonsgegevens en/of draagt Verwerker deze over aan Verwerkingsverantwoordelijke en/of een andere door Verwerkingsverantwoordelijke aan te wijzen partij, naar gelang de keuze van Verwerkingsverantwoordelijke. Alle bestaande (overige) kopieën van Persoonsgegevens, zich al dan niet bevindende bij door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, worden hierbij aantoonbaar permanent verwijderd, tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.

13.4 Verwerker bevestigt op verzoek van Verwerkingsverantwoordelijke Schriftelijk dat Verwerker aan alle verplichtingen uit artikel 13.3 heeft voldaan.

13.5 Verwerker draagt de kosten voor vernietiging, retournering en/of overdracht van de Persoonsgegevens. Verwerkingsverantwoordelijke kan nadere eisen stellen aan de wijze van vernietiging, retournering en/of overdracht van de Persoonsgegevens, waaronder eisen aan het bestandsformaat.

13.6 Verplichtingen uit de Verwerkersovereenkomst die naar hun aard bestemd zijn om na beëindiging van de Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst voortduren.

ARTIKEL 14. TOEPASSELIJK RECHT EN GESCHILLENBESLECHTING

14.1 De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.

14.2 Alle geschillen, die tussen Partijen ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in de plaats waar Verwerkingsverantwoordelijke gevestigd is.

ALDUS OVEREENGEKOMEN DOOR PARTIJEN:

Tilburg University	**[NAAM VERWERKER]**
Op <datum invullen>	<datum invullen>
_____	_____
Naam	*Naam*
_____	_____
Handtekening	*Handtekening*

Bijlage E – Interview Functionaris Gegevensbescherming TiU

Interview Functionaris Gegevensbescherming

1. *Wie bent u en wat is uw functie?*
   Moswa Herregodts, functionaris voor de gegevensbescherming, in het Engels ook wel Data Protection Officer. Het is een oude functie die vroeger alleen bij de overheid bestond. Maar bij de komende AVG veel meer zal worden ingezet. De AP heeft deze functie afgelopen ander half jaar prominenter in beeld gebracht, na aanpassing van de Wbp. Dat is een functie die er op toe ziet dat de organisatie zich conformeert aan de Wbp/AVG.

2. *Waarom bent u aangesteld?*
   Ik ben vrijwillig ingesteld.

3. *Wat zijn uw taken en bevoegdheden als FG?*
   De belangrijkste twee taken zijn: het adviseren van de organisatie over de privacy verplichtingen. Het advies wordt primair aan het College van Bestuur (hierna: CvB) van TiU en de directeuren gegeven. Maar dit gaat ook tot aan de werkvloer. Op alle lagen geef ik dus advies. De tweede taak is het zorgen voor een compleet beeld van alle verwerkingen van de persoonsgegevens binnen de organisatie, ook wel het register. Mijn taak is er voor te zorgen dat er een register is. De inhoud van het register moet natuurlijk wel van de mensen komen die er mee werken. Dus dat is een gedeelde verantwoordelijkheid. De bevoegdheden die ik heb zijn dat ik toegang kan verlangen tot data, zowel fysieke data als in databases. Maar dat doe ik niet zomaar, dat spreken we binnen de organisatie af. Ik geef dan advies aan de intern verantwoordelijke (systeemeigenaar, representative, leidinggevende, directeur). Zij zijn dan verantwoordelijk voor de verandering van de verwerking/het proces. Enkel in geval van hoog risico (impact/kans) en bij geen opvolging van advies zal ik casuïstiek direct aan CvB voorleggen.

4. *Wat verandert er voor TiU met de toepassing van de AVG? Welke gevolgen heeft dit voor de TiU?*
   Het heeft grote gevolgen. Principieel verandert er niet veel. De AVG bepalingen zijn redelijk conform de Wbp wetgeving. De twee grootste veranderingen zijn dat we een veel grotere documentatieplicht hebben, we moeten veel beter in kaart hebben waar er persoonsgegevens worden verwerkt en hoe dat aan elkaar is gelinkt, dit wordt de accountability genoemd. Daarnaast de stok achter de deur door de AP, zij hebben meer handhavingsbevoegdheden gekregen. Dat speelt natuurlijk ook mee. Maar het grootste gevolg is de documentatieplicht, wij moeten veel beter in kaart hebben waar er persoonsgegevens worden verwerkt en de excessen waar dit niet goed verloopt, moeten we aanpakken. Dus de accountability en compliance.

5. *Welke stappen zijn er al ondernomen om aan de toekomstige AVG te voldoen?*
   Wij zijn al in 2015 begonnen. Eerst met het aanstellen van de FG. De organisatie heeft meteen gehoor gegeven aan de oproep van de AP. De organisatie wist dat het nog niet verplicht was maar dat het wel belangrijk wordt. In 2016 is de Wbp aangepast vooruitlopend op en in lijn met de AVG. O.a. werd de FG al prominenter in beeld gebracht, er is een meldplicht datalekken gekomen en een paar andere veranderingen zoals de verhoging van de boetes. De meldplicht datalekken was wel echt iets nieuws. Daarvoor is een werkgroep in het leven geroepen. Het heette toen werkgroep Datalekken maar kort daarna werd bepaald om het bredere te trekken en werd het de werkgroep Privacy en Security. De werkgroep bestaat uit verschillende personen, uit juridische zaken, de IT security officer, de FG, de Chief Information Security Officer en een informatiespecialist. Een vrij brede groep en we bespreken niet alleen datalekken maar eigenlijk alles wat met privacy en security te maken

heeft. Daarnaast is destijds al een protocol en procedure opgesteld. De protocol is meer voor de medewerkers en studenten; wat moet je doen als er zich een datalek voordoet of als je dit constateert; die is vrij beknopt en waar het op neer komt is: meld het! De procedure is voor de werkgroep intern, van hoe wij er mee omgaan.

Dus het melden aan de AP?
Ja, eerst vindt er een intake plaats. Dan ga je verder op onderzoek. Bij grotere casussen wordt het gezamenlijk besproken. De melding aan de AP is helemaal op het einde. Het incident moet eerst gerepareerd worden, maar je moet ook een stukje awareness creëren zodat het de volgende keer niet zal gebeuren.

Kan ik de protocol en procedure inzien?
De protocol staat gewoon op de website van TiU. De procedure kun je ook inzien maar daarin staat meer wie doet wat. Dat is echt persoonsgericht binnen de werkgroep opgesteld. Normaal neem ik daarin de lead maar als ik er niet ben neemt iemand anders het van mij over. Meldingsplichtige datalekken moeten bij de AP binnen 72 gemeld worden dus het moet wel vrij strak geregeld zijn. Dit was allemaal al in begin 2016. De werkgroep komt twee/drie wekelijks bij elkaar, op dit moment is dat drie wekelijks. Er is al zoveel gedaan. Inmiddels is er ook een projectgroep Implementatie AVG ingesteld. Dat is eigenlijk de werkgroep plus twee andere personen. Compliance officer en een van de bestuur ondersteuners. Daarvoor hebben wij ook een externe partij benaderd. Die heeft een compliance check gedaan, soort van een nulmeting, dat was Considerati. Onderdeel daarvan was onder andere de verschillende onderdelen/afdelingen binnen de organisatie te interviewen. Die hebben ook afgelopen week hun definitieve rapport opgeleverd. Naar aanleiding van dat definitieve rapport hebben we die projectgroep echt formeel belegd en zijn we nu bezig met een plan van aanpak voor de komende maanden. De geïnterviewde worden spoedig in kennis gesteld over dit definitieve rapport. Er zal voor later ook veel beleid en procedures worden opgesteld en herzien, daar gaat de werkgroep eerst zelf naar kijken en rond half januari komt daarin ook weer een groot communicatiemoment met de verschillende afdelingen.

6. *Is er al een eenduidig en duidelijk privacy beleid?*
   Ja er is al beleid, maar niet duidelijk. Het zit nog versnipperd. Dat is nu onderdeel van het project. Er wordt nu een strategisch privacy beleid opgesteld en een algemeen privacy beleid. Dat is een heel algemeen overkoepelend document waarin wordt verwezen naar bestaande documenten. Want nu zit het eigenlijk overal verspreid. We hebben een Informatie beveiligingsbeleid, een datalek procedure, een document met bewaartermijnen, een document met gedragscodes zowel voor intern als extern. Het zit dus overal versnipperd. Het algemene privacy beleid wordt een soort kapstok document dat gaat verwijzen naar die verschillende onderdelen in de andere documenten.

7. *Op welke rechtmatigheidsgrondslag(en) berust de gegevensverwerkingen binnen TiU?*
   Dat is heel verschillend. De drie voornaamste zijn; op basis van een overeenkomst; arbeidsovereenkomst/studieovereenkomst van de studenten en medewerkers worden veel gegevens verwerkt, doorverwerkingen en verwerking voor wetenschappelijke onderzoeken gebeurt vaak op basis van toestemming of gerechtvaardigd belang.
   Verschillende per afdeling. 3 voornaamste. Obv overeenkomst, gerechtvaardigd belang en toestemming. En incidenteel heb je weleens andere gronden, zoals als de politie vraagt om beelden van de camera’s hier op de campus.

8. *Binnen de TiU worden er gegevens verwerkt. Wie is de verwerkingsverantwoordelijke voor deze verwerkingen? Is dat de Universiteit of de afdelingsmanagers per afdeling?*
   Het is een gedeelde verantwoordelijkheid. De hoofdverantwoordelijke is het CvB. Maar die heeft dat natuurlijk gedelegeerd naar de leidinggevende van de afdelingen. De eindverantwoordelijkheid ligt bij het CvB.

9. *Wat is de verhouding tussen de afdelingen van de University (in het bijzonder verhouding DARO – Studentdesk)? Mogen zij persoonsgegevens vrijelijk aan elkaar verstrekken en van elkaar verwerken? (wettelijke grondslag of overeenkomst ten grondslag)*
   Nee, de data verkrijgen we voor een bepaald doel en op een bepaalde grondslag. Hergebruik van deze data mag onder voorwaarden. Daarin vindt ook een toetsmoment plaats. We hebben bijvoorbeeld mailadressen van studenten, voor welke doeleinden mogen we die ook gebruiken. Het mag dus maar wel onder voorwaarden. Heel belangrijk punt is awareness. Mensen moeten zich er van bewust zijn dat ze zorgvuldig met die data omgaan. Dit wordt ook bij de verschillende afdelingen bijgebracht. Wettelijk is het dus toegestaan maar wel onder voorwaarden. De wettelijke grondslag betreft art. 6 lid 4 AVG. Hierin staan ook de voorwaarden genoemd die worden gesteld bij verdere verwerking van persoonsgegevens.

10. *Hoe zorgen jullie ervoor dat de medewerkers bewust blijven mbt de privacy van betrokkene?*
    Daar zijn verschillende actiepunten voor. Deze week organiseren we, vanuit de landelijke awareness week, informatiebijeenkomsten over de AVG. Dit zijn inloopsessies. Onderdeel van de projectgroep is de communicatie richting de organisatie; de medewerkers en studenten. Vanuit de projectgroep AVG zal er ook een moment zijn, maar dit zal begin 2018 plaatsvinden. Wij organiseren voor afdelingen vaak sessies; kan zijn algemene sessie; wat zijn de verplichtingen van AVG, kan ook heel specifiek zijn voor afdeling; wat doen jullie, wat hebben jullie op papier staan, hoe ziet het er technisch uit, afhankelijk van wat de vraag is wordt dit bepaald.

11. *Is de bewerkersovereenkomst recent?*
    Ja en nee; ja hij is aangepast. Hij is door SURF aangepast, dat is de verzameling van alle Universiteiten en HBO scholen. Die hebben een modelovereenkomst die in de eindfase zit. Onze Juridische Zaken is daarbij betrokken. De verwachting is dat de modelovereenkomst in dezer dagen af zal zijn. De modelovereenkomst die wij gebruiken is ook in SURF verband gemaakt en hebben wij een paar dingen aan toegevoegd.

12. *Is er weleens sprake geweest van een datalek? Werd u toen hierover geïnformeerd? Zo ja, hebt u toen contact gehad met de AP?*
    Wekelijks krijgen we meldingen. Maar daar zit een gradatie in want niet alle meldingen zijn daadwerkelijk datalekken. We zeggen tegen de afdelingen dat ze gewoon moeten melden zodat ze ons ook weten te vinden. Al staat er een karretje met post ergens onbeheerd dan willen we dat dat wordt gemeld. Zodra een melding binnenkomt doe ik de eerste schifting, waarin ik constateer of het een beveiligingsincident of een datalek is. Ook daarin zit een gradatie in van de ernst. Bij datalekken gaat de melding naar de hele groep, maar een iemand pakt de melding dan op. Dan zal er een eerste indruk zijn van de ernst van de lek en als het een ernstige lek is kijken we met meerdere personen hoe we dit gaan aanpakken en of het meldingsplichtig is. Afgelopen jaar hebben we veertig meldingen gehad, waarvan vijftien daadwerkelijke als datalek werden gekwalificeerd. Daarvan hebben we ook een aantal gemeld bij de AP. Bij een drietal meldingen hebben we ook de betrokkene waarvan de data verloren is geraakt erover geïnformeerd.

13. *Gaat er een gegevensbeschermingseffect-beoordeling (PIA) plaatsvinden of heeft er al een plaatsgevonden? Wie gaat dit uitvoeren en hoe gaat dit in zijn werk? Wat zijn de resultaten van deze PIA? Welke rol heeft u hierin?*
    Ja, die hanteren wij al langer. We moeten alleen nog kijken naar de omvang en breedte van de beoordeling. Nu doen we dat vooral bij applicaties waarin grootschalig of juist gevoelige gegevens worden verwerkt. Bij onderzoeken wordt er ook vaak om gevraagd. Soms doen we dit omdat we vinden dat het noodzakelijk is en soms omdat een derde het noodzakelijk vindt. Bijv. bij de Europese subsidieverstrekkers zoals ERC.
    Voor de beoordeling wordt op dit moment gebruik gemaakt van een SURF model, die weer gebaseerd is op twee andere partijen. De PIA wordt uitgevoerd door de degene die de verwerking gaat uitvoeren of in ieder geval daarbij betrokken is en een informatiespecialist. De PIA ziet op privacy en security maar ook breder, voorbeelden zijn reputatieschade en mitigerende maatregelen. We zijn nu bezig met het ontwikkelen van een tooling voor de verwerkingsregister, om alle verwerkingen goed bij te houden. Hierin komt dan ook de PIA. Een soort van pre PIA wordt dan ingesteld, in de vorm van een vragenlijst waaruit dan blijkt of een PIA noodzakelijk is. Via deze vragenlijst kan de FG de personen die de PIA uitvoeren ook sturen, en wijzen op dingen die ook meegenomen moeten worden. Als FG denk ik mee met het model dat gebruikt wordt en achteraf toets ik. De beoordeling zelf dient echt door de ‘aanvrager’ zelf worden gedaan en een derde.

14. *Bestaat er al een dergelijke risicoanalyse/audit?*
    Zo nee, waarom niet? Zo ja, mag ik die inzien?
    Ja, soms wordt er gekeken naar een derde partij die zich niet conformeert met onze bewerkersovereenkomst. In de onderhandelingen komen we dan net niet goed uit over bepalingen. Dit kan juridische risico’s meebrengen. Een voorbeeld is dat wij een audit willen en kunnen uitvoeren zodat we kunnen zien hoe de derde partij de gegevensverwerking plaats laat vinden. Er zijn partijen die dat niet willen, zoals grote partijen. Die zitten er niet op te wachten dat kleine partijen een kijkje in de keuken komen nemen. In dat geval maken we een risico overweging. Zij willen namelijk niet conformeren met bepalingen uit onze bewerkersovereenkomst. Dan kijken we welke risico’s dit mee brengt en of er mitigerende maatregelen toegepast kunnen worden.

15. *Wordt er al een verwerkingsregister bijgehouden, waarin staat welke persoonsgegevens verwerkt worden en de beveiligingsmaatregelen ter bescherming van deze persoonsgegevens?*
    Ja, maar nog niet structureel. We werken nog met excel bestandjes maar daar wil ik van af. We zijn op dit moment heel hard opzoek naar een tooling. We hebben er al een gevonden maar kijken nog naar twee andere. Bij de excel bestanden werkt de actualisatie niet goed en moet je per mail vragen of diegene het kan toelichten etc. Dit gaan we goed en structureel inbedden in de tooling.

Bijlage F – Interview Managing Director DARO

Interview Frederique Knoet (Managing Director DARO)

1. Wie bent u en wat zijn uw taken/werkzaamheden/bevoegdheden?
   Mijn naam is Frederique Knoet, ik werk als Managing Director bij de afdeling Development and Alumni Relations. Mijn taak is 2 ledig: enerzijds het betrekken van alumni in onderwijs en onderzoek en anderzijds het organiseren van fondsenwerving, onder alumni.

2. Wie is de interne verantwoordelijke voor de gegevensverwerkingen binnen DARO?
   De interne verantwoordelijke is Joost. Ik ben uiteindelijk eindverantwoordelijke, maar ik heb het gedelegeerd naar hem.

3. Waarom worden er persoonsgegevens verwerkt binnen DARO?
   Dit heeft verschillende redenen. We halen gegevens aan om te kijken waar onze alumni terechtkomen, dus om te kijken wat voor levensloop ze hebben. In de zin van levensloop bedoel ik professionele levensloop. Bijvoorbeeld wat voor type werkgever, waar gaan ze werken, type organisatie, wat voor baan, wat is hun verloop in hun carrière etc. Hiermee kunnen we laten zien wat voor profiel studenten kunnen krijgen als ze een bepaalde studie afronden. Hiermee kunnen we dus rolmodellen opstellen. De tweede reden is om de alumni te benaderen om terug te komen, ofwel voor netwerken, professional education, als mentor of misschien om een stageplek ter beschikking te stellen voor studenten. Als laatste ook voor fondsenwerving. De alumni worden gesegmenteerd in groepen in kaart gebracht, om bepaalde projecten te ondersteunen.

   Wat bedoel je precies met gesegmenteerd?
   We maken profielen aan, maar niet persoonsgericht. In de belcampagne stoppen we bijvoorbeeld iedereen tussen de 27 jaar tot 70 jaar. Dan segmenteren we wie we als eerst gaan bellen van deze groep omdat we weten dat dit de beste groep is om te bellen. Dus ze worden niet op basis van persoon gebeld maar op basis van een aantal karakteristieke van de groep.

4. Van welke personen worden er persoonsgegevens verwerkt?
   Van alumni worden gegevens verwerkt en van een aantal mensen die niet bij ons hebben gestudeerd, maar die wel een relatie met de universiteit hebben, corporate relaties noemen we die. Dit is een aparte groep want hun gegevens worden bijgehouden en bewerkt, maar daar zijn we niet nadrukkelijk mee bezig als de groep alumni. Van alumni houden we bijvoorbeeld de levensloop bij, terwijl corporate relaties veel meer gebonden is op de organisatie waar ze voor werken, niet zozeer op de persoon.

5. Op welke manier verzamelt DARO de persoonsgegevens?
   Wij komen aan de gegevens door ofwel een datadump van de studentenadministratie, we laten alumni hun gegevens updaten via een formulier, dus door mensen zelf worden de gegevens geüpdatet en we hebben een overeenkomst met PostNL. Als alumni dan verhuizen kunnen ze op een formulier aangeven dat PostNL de universiteit moet informeren over de verhuizing. Sinds kort hebben we een project met een bedrijf om LinkedIn op te scrapen om daar gegevens uit te halen. Maar dit kan alleen als alumni op hun LinkedIn profiel hebben aangegeven dat de gegevens openbaar zijn.

   Wordt dat verzoek om gegevens up te daten periodiek gedaan?
   Nee, we pakken regelmatig een groep die we een mailing en brief sturen waarin we ze verzoeken om hun gegevens te actualiseren. Dit gebeurt niet regelmatig, in

de zin van elke halfjaar of jaar. Maar meestal gebeurt dit doordat we bij een ICARS, een check waarbij we aan een organisatie moeten doorgeven van hoeveel mensen we gegevens hebben en hoeveel van deze actueel zijn. Hierdoor zien we soms groepen uitvallen en ondernemen we actie. Dit gebeurt minstens een of twee keer per jaar.

Er is dus nog geen protocol waarin staat dat dit elk half jaar moet?
Nee, dat hebben we nu nog niet maar daar wil ik wel naar toe.

6. Wat doen jullie met de verwerkte persoonsgegevens? Voor wat gebruiken jullie de persoonsgegevens?
   We gebruiken ze voor verschillende doeleinden, om onze vakgroepen te helpen. Als zij bijvoorbeeld alumni willen betrekken bij het onderwijsproces. Dan maken wij een selectie van alle mensen die tussen nu en tien jaar geleden afgestudeerd zijn in een bepaalde richting. Die sturen we dan een email of ze bijvoorbeeld willen helpen met een mentorship. Of we gebruiken de gegevens om ons professional education programma onder de aandacht te brengen, dit doen we meestal ook gesegmenteerd en gaat niet naar alle alumni. Dan kijken we bijvoorbeeld welke alumni dit interessant zouden vinden, die selecteren we en mailen we. We nodigen de hele groep alumni uit voor activiteiten. Als er dan een alumnivereniging van een faculteit iets organiseert dan segmenteren we weer. De gegevens worden dus gebruikt om alumni te wijzen op evenementen en programma's die voor hun ontworpen zijn. De andere kant benaderen we ze gericht om te vragen of ze willen doneren, via de belcampagne bijvoorbeeld. Dat gebeurt op basis van een selectie uit de database.

7. Wie verwerkt er binnen DARO de persoonsgegevens?
   De grote verwerkingsklussen worden door Joost gedaan. De dumps etc. en de contracten met derden om bijvoorbeeld een gegevensupdate te doen. Maar iedere medewerker van DARO heeft toegang tot de database. Iedereen kan ook een record openen en daarin bijvoorbeeld een wijziging aan brengen.

8. Op welke manier worden de betrokkene geïnformeerd over de gegevensverwerking?
   Op dit moment worden ze niet geïnformeerd. Dit weet ik niet honderd procent zeker, maar ik denk dat we nergens actief een tekst hebben staan met daarin de manier waarop we met de persoonsgegevens om gaan.

   Ook niet bij de diploma-uitreiking?
   Nee, bij de diploma-uitreiking herinneren we ze dat ze niet moeten vergeten om hun gegevens bij te werken. ''Keep in touch'' noemen we dat. Eigenlijk vragen we ze op een aardige manier om door te geven wat ze precies doen. Dit gebeurt middels een filmpje tijdens de uitreiking. Maar, dit staat nergens op de website. In de email staat wel wat informatie. Als we bijvoorbeeld een uitnodiging verzenden en de alumni geeft aan dat hij/zij komt dan geven wij aan dat de gegevens die ze invullen, in de database terechtkomen. Daarbij geven we ze de mogelijkheid om hierover hun bezwaar kenbaar te maken. Dus hier zit het wel actief in. Voor de rest zit het passief in de zin van dat je je kunt afmelden voor mailings etc. en dat we ze dan niet meer zullen benaderen in de toekomst.

9. Hoe worden de persoonsgegevens (organisatorisch) beveiligd?
   Iedereen bij DARO heeft toegang tot de database, daarbuiten hebben een select groep mensen toegang. Als je dus voor de afdeling werkt heb je toegang en anders niet. Verder is Joost degene die alle rechten beheert en kan dus zien wie er toegang heeft en wat die personen aan het doen zijn. Alleen Joost mag op

grote schaal gegevens verwerken. De andere medewerkers mogen alleen updates over bijvoorbeeld adres/mail/telefoonnummer wijzigen, indien betrokkene hen hierover informeert. De volgende check is de standaard firewalls die de Universiteit heeft.

10. Met welke partijen zijn er bewerkersovereenkomsten aangegaan en waarom met deze partijen?
    Met verschillende partijen.
    Met Rux Button hebben we een bewerkersovereenkomst. Met hun organiseren we de belcampagne. Zij verzorgen de belsoftware voor de belcampagne.
    Met Building Blocks hebben we ook een bewerkersovereenkomst. Met hun doen we LinkedIn scrapen. BB haalt werkgeversinformatie van LinkedIn af. Wij leveren een groep alumni aan, waarmee zij aan de slag gaan op LinkedIn.
    We hebben ook nog met Morphis een bewerkersovereenkomst gesloten. We hebben nu Rux Burton met wie we de belcampagnes doen, maar we willen in de toekomst misschien van hun af, wat betekent dat we eigen belsoftware willen ontwikkelen. Voor het ontwikkelen van deze software moeten we af en toe try-outs doen. Deze try-outs betekenen dat we dan een aantal alumni inladen om te checken of het lukt. Aangezien zij dan ook toegang hebben tot de persoonsgegevens van alumni, hebben we met hun ook een bewerkersovereenkomst gesloten.

11. Door wie worden de derde partijen met wie een bewerkersovereenkomst is aangegaan gecontroleerd?
    Binnen de Universiteit is het zo geregeld dat ik de bewerkersovereenkomst sluit en in die overeenkomst staat dat onze audit/cert team langskomt om te controleren. Ik ga er ook vanuit dat dit gebeurd. Ik sluit de bewerkersovereenkomst, dus IT weet er van af en licht dat team in.

12. Worden de persoonsgegevens doorgestuurd naar derde partijen waarmee geen bewerkersovereenkomst is aangegaan? Zo ja, hoe is dit geregeld en waarom is dit nodig?
    Nee. Iedereen binnen DARO is zich bewust van bewerkersovereenkomsten en privacy. Het is in principe zo dat Joost altijd vraagt als mensen query's uit willen draaien en bestanden willen opvragen van: waar is het voor? Het is echt wel zo dat als iemand de gegevens aan iemand buiten de organisatie wilt geven, dat Joost dan zegt dat dit niet zomaar gaat. We hebben zelf ook onderling afgesproken dat we alles via SecureFile sturen, dus het zit niet meer in emails etc. Daarmee is bij iedereen wel het besef doorgedrongen dat ze de gegevens niet zomaar naar mensen buiten de organisatie mogen sturen. Tenzij de alumni misschien toestemming heeft gegeven.

    Hoe is dit stukje awareness gecreëerd?
    Er is een keer een sessie door afdeling Legal georganiseerd, dat is alweer twee jaar geleden. Toen hebben ze dit allemaal met ons doorgenomen.

13. Is er weleens een datalek voorgekomen? Hoe is er toen gehandeld? Welke maatregelen zijn er toen naar aanleiding van het lek genomen (protocol/instructies)?
    Ja, mijn laptop was een keer gestolen. Het was wel een ding. Een aantal van ons hebben laptops, waarop misschien nog bestanden staan waarin persoonsgegevens staan. Deze bestanden zijn niet beveiligd.

Hoe is er toen gehandeld?
Zoals het hoort heb ik meteen de FG (Moswa) ingelicht. Die heeft me toen opgedragen om mijn wachtwoord te wijzigen. Ook hebben we toen doorgenomen welke bestander er mogelijk op mijn laptop stonden. Ik heb toen geconcludeerd dat er een aantal persoonsgegevens van medewerkers, gevoelige gegevens en ook paspoortgegevens op stonden. Dit hebben we bij de AP aangegeven en ik heb alle mensen, over de diefstal, geïnformeerd waarvan ik dacht dat zijn of haar gevoelige gegevens op mijn laptop stonden.

Bestaat er een protocol waarin staat hoe medewerkers moeten handelen bij een datalek? We weten allemaal dat we meteen de FG moeten informeren. Dat is wat het protocol in werking zet en wat er zich vanaf dat moment afspeelt dat weten wij niet. Mijn medewerkers zouden mij wel gelijk Whatsappen dat zijn/haar laptop gestolen is. Zodat we samen de volgende ochtend bij Moswa op de stoep staan om het te regelen.

14. Wordt er weleens een risicoanalyse uitgevoerd met betrekking tot de verwerking van persoonsgegevens binnen DARO?
Nee. Joost doet wel checks. Op maandelijkse basis kijkt hij wat er gewijzigd is in de database en wie van ons misschien enorme fouten maakt. Dan wordt deze medewerker daar ook op aangesproken. Fouten zoals bijvoorbeeld telkens het verkeerde nummer opvoeren in de database etc. Hier blijft het ook bij want grote risicoanalyses doen we eigenlijk niet. Het is wel zo dat er een risicoanalyse wordt gedaan op het moment dat wij iets willen. Bijvoorbeeld op het moment dat we bedacht hebben dat we data op een bepaalde manier willen bewerken, dan moet ik van Legal weer terug naar het inventarisatieschema waarin staat of een verwerking rechtvaardig is en wat de basis is van de verwerking. Op dat moment wordt er in principe een risicoanalyse gepleegd, want we gaan terug naar alle verwerkingen. Dit is wel heel erg eventdriven. Het is niet zo dat we bijvoorbeeld iedere drie maanden een risicoanalyse doen.

15. De betrokkene van wie persoonsgegevens worden verwerkt krijgt enkele nieuwe rechten erbij. Hoe gaan jullie invulling geven aan deze rechten van betrokkene?
We zullen gewoon gehoor moeten geven aan het beroep van betrokkene op een van zijn rechten. Als iemand verzocht om verwijdering uit de database dan lieten wij deze persoon in de database, maar zette we achter zijn gegevens de tagg: do not contact. Tot nu toe hebben we nog geen gegevens permanent verwijdert uit de database, maar dit zal in de toekomst dus wel moeten gebeuren.

Ik moet aan Legal vragen wat zwaarder weegt, mijn taak of het belang van betrokkene. Ik kan me er bij voorstellen dat het belang van betrokkene op een gegeven moment toch zwaarder zal wegen. Stel alle afstudeerders van Global Law willen verwijdert worden uit de database, dan hebben wij een probleem. Maar of dit probleem groter weegt dan het belang van betrokkene, dat is onzeker. Ik kan me voorstellen dat als onze plicht om alle alumnis van de Universiteit bij te houden, vanuit een wettelijke taak gebeurt dat dit sterker zal zijn dan wanneer deze taak door de Universiteit zelf is opgedragen aan ons. Maar aan de andere kant denk ik: hoeveel mensen zouden zo'n verzoek indienen? Ik denk namelijk dat er niet veel mensen zijn die dergelijk verzoek indienen. Daardoor zal de situatie niet echt veranderen. De personen die wel om verwijdering verzoeken, kunnen dan uit de database worden gehaald. Deze personen gaan namelijk nooit meer hun gegevens updaten, dus alle informatie die we hebben over deze personen is niet meer relevant. Dus deze personen zullen we er dan gewoon uit moeten halen.

16. Worden er binnen DARO nog andere bijzondere gegevens verwerkt over betrokkene? (medische of fav. professor of dergelijke).
    Ja, de gegevens over de favoriete professor moeten er nog uit. Joost is wel strikt op welke gegevens wij over een persoon willen vastleggen. Hij wilt dan van ons weten waar we deze gegevens voor willen gebruiken. Hij verlangt van ons dat we goed nadenken over waarom die gegevens echt nodig zijn en voor welk doel, anders wilt hij het ook niet registreren.

Vragen naar aanleiding van inventarisatieschema

1. Waarom is het relevant voor het doel om het oude adres van de alumni te verwerken?
   Volgens mij werd dit ooit gedaan vanuit het idee dat de oude adressen soms ook adressen van de ouders zijn, en we merkten dat als we die mensen een brief schreven, dat ze dan zeiden van: mijn zoon woont hier al jaren niet meer, hij woont nu op… Dit was voor ons dus een uitstekende manier om iemand toch te achterhalen. Daarom is het idee ontstaan van we houden de oude adressen want daar zitten de ouders bij of familie en daardoor kunnen we die mensen toch vinden. Dit is 5 of 6 jaar geleden bedacht. Mocht dit niet meer kunnen ogv de nieuwe regelgeving dan deleten we alle oude adressen. De vraag is ook wat je aan het oude adres hebt als je al een nieuwe hebt gekregen.

   Aan de andere kant is het bij studenten wel handig. Veel studenten komen hier in het systeem, terwijl ze nog een master doen. Dit komt omdat ook afgestudeerden bachelor-studenten in de database terechtkomen. Tijdens hun master wonen ze dan nog op het studentenadres. Daar wonen altijd studenten. Soms weten de nieuwe bewoners dan te vertellen waar de afgestudeerde tegenwoordig woont. Dan is het een kwestie van opzoeken in het telefoonboek. Dit was denk ik de achterliggende gedachte. Maar dit wordt alleen in zeldzame individuele gevallen gedaan. Alleen als we iemand echt niet kunnen vinden.

2. Waarom wordt de verwerking van bankgegevens gebaseerd op toestemming?
   We komen op twee manieren aan de bankgegevens van alumni. Dit kan via het machtigingskaart. Dit wordt door de alumni zelf ingevuld en getekend. Als ze achteraf aangeven dat ze het toch niet meer willen, dan doen we het niet meer. Andere kant gaat het via de telefoon. We bellen die alumni op en geven ze over de telefoon hun bankgegevens. Die voeren we in en dan sturen we ze vervolgens een bevestiging, waarin we ze aangeven welk bankrekeningnummer zij hebben doorgegeven en dat we van dit nummer incasso plegen. Zij kunnen dan ook aangeven dat het nummer verkeerd is of dat ze het achteraf gezien toch niet willen.

   Staat er dan een toestemmingvakje?
   Op de machtigingsformulier staat dit wel. Maar niet in de mail. Maar als er via email wordt aangegeven dat ze het toch niet eens waren, dan storten we alles terug.

3. Waarom wordt de verwerking van het land van alumni gebaseerd op vitaal belang?
   Ja, wij hebben natuurlijk ook een internationaliseringsbeleid en zijn daarom heel erg op zoek zijn van: hoe kunnen wij bijv. met een aantal buitenlandse partners zij het Universiteiten of bedrijfsleven onze studenten in het buitenland meer kans geven of ook op een andere manier onderzoek en onderwijs stimuleren. Daarom hebben we besloten dat we dit bijhouden. We maken namelijk buitenlandse chapters en als we dan niet weten waar de personen verblijven dan wordt het lastig. Dan kun je geen potentiele leden van je chapter uitnodigen en zou je hypothetisch gezien al je alumni moeten lastig vallen voor een bijeenkomst in Brazilie. Volgens mij hebben we ook de nationaliteiten erin staan, deze gegevens komen mee vanuit de studentenadministratie.

Bijlage G Interview functioneel database beheerder

Interview functioneel database beheerder

1. Wie bent u en wat zijn uw taken/werkzaamheden/bevoegdheden?
   Mijn naam is Joost Groen en ik ben verantwoordelijk voor de database, The Raiser's Edge, van afdeling DARO. Ik ben functioneel beheerder van de database. Ik draag zorg voor de database, bewaak de kwaliteit, doe aanbevelingen en ontwikkel nieuwe procedures voor de gebruikers van de database. Daarnaast geef ik leiding aan een studenten-assistenten team van 4 personen.

   Worden er uitsluitend persoonsgegevens van (natuurlijke) personen verwerkt?
   De database bestaat uit ongeveer 88.000 'records'. Grof genomen zijn 67.000 van de 88.000 records profielen van afgestudeerden (alumni) van TiU. 17.000 records zijn organisaties en de resterende 4000 records zijn personen die niet hier gestudeerd hebben, maar wel een relatie met ons hebben of hadden. Dit kan bijvoorbeeld een persoon zijn die een donatie heeft gedaan of een persoon die een alumni event heeft bezocht. Daarnaast valt ook de 'corporate relatie' groep onder die 5000; dat zijn de relaties van de Universiteit zelf. Denk hierbij aan directeuren van andere universiteiten, burgemeesters van Tilburg en omringende gemeentes etc.

2. Hoe verzamelt DARO de persoonsgegevens/ hoe komen de persoonsgegevens in de database terecht?
   De gegevens komen op een aantal verschillende manieren in de database:
   1. Nieuwe afgestudeerden komen wekelijks in de database. Vanuit de studentenadministratie krijgen wij iedere week een nieuwe Excel lijst met afgestudeerden die de week daarvoor zijn afgestudeerd. Dit zijn personen die een Bachelor of Master hebben afgerond en officieel de week daarvoor bij de Studenten Administratie een alumni status hebben gekregen. Wij hebben, in samenwerking met LIS, bepaald welke data in dat Excelbestand moet komen. Alle data die wij dan dus krijgen van de Studenten Administratie is relevant en importeren wij in de database. Het bestand is, in principe, al ''import-klaar''; we hoeven alleen dit bestand via een import optie van de database in de database te zetten. Alhoewel het regelmatig voorkomt dat we de data moeten aanpassen om deze zonder fouten te importeren. Maar dit zijn vaak fouten die te maken hebben met het (moeilijke) import proces van de software.
   2. Zoals gezegd zitten er ook zo'n 4000 personen in de database die hier geen studie hebben afgerond, maar wel een relatie met ons hebben. Deze groep personen worden handmatig opgevoerd. De gegevens van deze personen krijgen wij vaak van hen zelf: via bijvoorbeeld een bussinesscard of via een email of aanmeldformulier (van een event) waarin ze hun contactgegevens hebben gezet.

   Het is dus niet zo dat ze een bepaalde formulier in moeten vullen?
   Relaties vaak niet, alhoewel niet-alumni die een event bezoeken dat wel doen via een aanmeldformulier. Afgestudeerden kunnen, nadat ze in onze database zijn gekomen, via een ''wijzig je gegevens'' formulier op onze website hun contact- en werkgeversgegevens updaten.

   Krijgen ze de optie om hun gegevens te wijzigen meteen op het moment dat ze zijn afgestudeerd?
   Ze krijgen wel te horen dat ze dat kunnen doen. Ze krijgen namelijk een kaartje in hun diploma map, waarin wordt aangegeven dat ze nu alumnus/alumna zijn en dat ze hun contact- en werkgeversgegevens kunnen wijzigen. Het is erg fijn als zoveel mogelijk nieuwe alumni dit doen omdat we dan meteen hun privé

emailadres hebben. Iedere afgestudeerde die in onze database komt, komt namelijk met een UiT mailadres in de database te staan. Het zou natuurlijk fijn zijn als we van iedereen meteen hun privé-emailadres krijgen in plaats van hun UiT mailadres.

3. Welke persoonsgegevens worden verwerkt in de database?
Ik zal je een inventarisatieschema sturen waarin staat welke persoonsgegevens wij verwerken, voor welk doel en op welke grondslag wij dat baseren.

4. Hoe worden de persoonsgegevens verwerkt?
Als een adreswijziging wordt doorgevoerd met behulp van een formulier op onze website zorgen onze student-assistenten er voor dat deze (handmatig) in de database worden gezet.

5. Wie verwerkt deze persoonsgegevens in de database?
De student-assistenten verwerken de persoonsgegevens in de database: 2 student-assistenten ondersteunen mij bij het technische gedeelte van deze verwerking (bijvoorbeeld wekelijkse importwerk) en 2 andere student-assistenten verzorgen weer de contactgegevens wijzigingen en voeren deze handmatig op in de database.

6. Hoe wordt er gezorgd voor het actualiseren van deze persoonsgegevens?
Dat is heel moeilijk omdat je afhankelijk bent van de alumni zelf. Wij kunnen namelijk niet gaan opzoeken waar iemand woont. Wij zijn dus afhankelijk of iemand zelf zijn persoon- en adresgegevens doorgeeft via een formulier, mail of telefoontje. Dit gaat puur over de contactgegevens. Werkgeverinformatie bijvoorbeeld, zoeken wij vaak wel zelf op. We hebben bijvoorbeeld afgelopen weken een werkgeversproject gedaan via een extern bedrijf. Dit bedrijf zoekt naar de werkgeversinformatie van bepaalde personen. Deze werkgevergegevens werden dus niet zelf door de betreffende personen aangeleverd maar zocht het bedrijf op via het internet.

Het is dus niet zo dat jullie een mail uitzetten naar alumnus van: ‘’check of je gegevens nog actueel zijn’’?
Dat doen we soms ook wel. Daarnaast hebben we ook onder onze handtekening van een emailbericht een link staan waarin staat: ‘’update je gegevens’’. Maar alsnog blijven we afhankelijk van de persoon zelf of hij/zij via die link daadwerkelijk zijn gegevens up-to-date houdt.

7. Welke personen hebben toegang tot de database? Waarom zij en waarom is dat nodig?
Iedereen binnen afdeling DARO. Dat geldt zowel voor de vaste medewerkers als voor de studentassistenten. Ook de stagiaires hebben toegang, mits ze dat nodig hebben. Sommige stagiaires hebben namelijk geen toegang nodig. Daarnaast hebben we nog twee andere afdelingen die ook gebruik maken van de database. Dat zijn de Carreeroffice en International Recruiting Marketing. Ook Petra de Koster heeft nog toegang. Zij heeft voorheen op deze afdeling gewerkt, maar nu bij afdeling Communicatie werkt. Zij doet nog steeds veel ‘werkzaamheden’ voor onze afdeling. Iedereen die toegang heeft tot de database, kan thuis ook de database benaderen. Dit kan echter wel alleen met een werklaptop van TiU en met een VPN verbinding.

Waarom kunnen de andere twee afdelingen ook bij de database?
Dat is toentertijd, begin van 2017, besloten zodat zij makkelijker bij gegevens kunnen van bepaalde personen. International Recruiting Marketing gaat bijvoorbeeld ook over de recruitment van nieuwe studenten uit het buitenland. Dan is het essentieel om te weten of er bijv. mensen in China of Duitsland werken die dan bij ons alumnus waren. Die kunnen ze dan contacteren om dan eventueel te vragen om mee te helpen met recruiten van nieuwe studenten. Career Office heeft onder andere te maken met het zoeken van stages en werk voor studenten. Die zoeken dan een bepaalde persoon op die in een bepaald vakgebied is afgestudeerd. Die proberen ze dan te benaderen om hen te helpen met hun zoektocht.

Krijgen zij werkinstructies mee mbt het gebruik van de database en de privacy van de betrokkene?
Ja, iedereen krijgt een instructie over de database. Het is wel een redelijk korte instructie, hij kan wel uitgebreider en groter. Door tijdgebrek is het lastig om een uitgebreide instructie te geven. Ik vind wel dat we vaker de gebruikers moeten trainen om ze te laten excelleren met het gebruik van de database. Je ziet namelijk ook dat sommige mensen geen zin meer hebben om met de database te werken omdat ze gewoon niet meer weten hoe of wat.

Mijn 2 database student-assistenten en ik controleren wekelijks of data op een correcte manier wordt opgevoerd. We kunnen niet elke wijziging tot in detail controleren (daar is het database systeem te beperkt voor), maar we kunnen wel zien of bijvoorbeeld adressen of telefoonnummers op de goede wijze in de database worden gezet. Als wij dan zien dat een persoon vaak dezelfde fout maakt, dan sturen we die persoon een mail met daarin het verzoek hierop te letten.

Worden er ook privacyaspecten meegenomen in de werkinstructie?
Hiervan is geen officieel document, maar er wordt uiteraard wel verteld dat ze niet zomaar lijsten mogen weg geven aan derden en dat ze zorgvuldig met de data moeten omgaan. Ook hebben sommige personen beperkte toegang tot de database en kunnen ze alleen groepen inzien welke voor hen relevant zijn.

8. Welke technische en (organisatorische) beveiligingsmaatregelen zijn er getroffen om de gegevens te beschermen in de database?

Dit is meer een technische vraag. Ik ben de functioneel beheerder en LIS, ons IT departement gaat over de technische gedeelte en ook over de veiligheid van de server.
Naast het feit dat je natuurlijk een login voor de database nodig hebt, moet de software natuurlijk ook op de laptop zijn geïnstalleerd. Daarnaast hebben alleen maar UiT laptops en computers netwerktoegang tot de database en mogen alleen computers op het UiT netwerk verbinding maken met de server.
Dat heeft LIS ook geregeld. Daarnaast zijn er ook veel veiligheidsprotocollen binnen het netwerk van de UiT die LIS heeft geïnstalleerd maar waar ik niet veel van af weet.

9. Heeft er weleens een risico-analyse plaatsgevonden met betrekking tot de beveiliging van de database?

Aan LIS vragen

10. Met welke partijen is een bewerkersovereenkomst? Waarom juist met deze partij(en)?

Met Rux-Button: De belcampagne fabrikant. Zij leveren de software voor de belcampagne van ons. Dit is een leverancier uit England die belsoftware hebben gemaakt en support leveren voor de belcampagnes. Zij zorgen voor het samenstellen van de alumnilijst van personen die moeten worden gebeld. De gegevens van deze personen komen dan in hun software te staan. Daarnaast begeleiden zij ook de studenten die de alumni bellen tijdens de belcampagne.
Building Blocks: Zij zoeken werkgeversinformatie van alumni voor ons op. Wij sturen hun bijvoorbeeld een lijst met 10.000 alumni. Op hun beurt zoeken zij dan de werkgeversinformatie van deze personen op. Dit doen zij via LinkedIN. Dus dan weten we van de betreffende personen welke functie ze bekleden, waar ze op dat moment werken en voorheen hebben gewerkt.
Morphis: Dit is ook een maker van belsoftware. Wij willen nu namelijk onze eigen belsoftware ontwikkelen. Dit is voor ons goedkoper en makkelijker om vaker belcampagnes te draaien.

Worden deze partijen ook gecontroleerd met betrekking tot de verwerking van persoonsgegevens?
Daar is die bewerkersovereenkomst voor die we met hun overeen zijn gekomen. Die bewerkersovereenkomst wordt ook voorgelegd aan Juridische Zaken.

11. Is, bij het opzetten van het IT-systeem waarmee en waarin gegevens worden verwerkt, rekening gehouden met privacy? Hoe is er rekening gehouden met privacy?

Een of anderhalf jaar voordat ik hier kwam werken begonnen ze met Raisers Edge te werken. Toen hebben ze een kleine gedeelte van alle alumni in RE gezet. Hiermee hebben ze toen een begin gemaakt met het opzetten van deze database. De functioneel beheerder die er toen was, is toen gestopt. Een jaar of anderhalf later kwam ik hier werken en werd de functioneel beheerder (dit deed ik trouwens samen met nog een andere persoon). Wij hebben toen de database echt opgebouwd door iedere alumni toe te voegen aan de database. Een jaar na mijn intreden hier hebben we de complete alumni groep in de database geïmplementeerd. RE is vanaf dat moment ook leidend geweest voor de gehele afdeling. Ik neem aan dat in de tijd voordat ik hier kwam werken, er ook door LIS rekening werd gehouden met de privacy van de betrokkene.

12. Is er weleens een datalek voorgekomen mbt de database?

Ja. Vorig jaar was de laptop van onze leidinggevende gestolen uit haar auto. Omdat er op de laptop ook bestanden stonden met informatie van onze alumni was dit een datalek.

En met betrekking tot de database zelf? Bijv een datalek door een virus
Nee, niet dat ik weet. Misschien dat LIS daar wat van weet en het nooit heeft verteld, maar in principe weet ik er zelf niks van.

13. Welke preventieve maatregelen worden genomen om een datalek te voorkomen en hoe wordt er gehandeld indien er een datalek plaatsvindt (protocol of instructies)? Misschien naar aanleiding van een datalek?

Ten eerste natuurlijk toen vorig jaar die laptop was gestolen, is iedereen strenger bezig met het beveiligen van hun eigen laptop. Zo laten we onze laptops niet zomaar ergens achter, zoals in de auto. We versturen databestanden ook niet meer via een emailbericht (als bijlage), maar via een download link. Dit is een beveiligde link waarin data kan worden gedownload. Dan blijft het namelijk niet in je eigen inbox staan, zodat bij een mogelijke hack die kwaadaardige personen niet meer bij die data kan. Voorheen stuurden we alles via een email naar elkaar

toe, waardoor iedereen veel data in hun mailbox hadden staan. Als die mailbox dan worden gehackt, zijn ook al die gegevens beschikbaar voor de hacker. Sinds een half jaar zijn we nu bezig met het uitsluitend versturen van bestanden via deze beveiligde verbinding. Deze verbinding heet SecureFilesender: http://send.avt.nl/. Deze website heeft LIS in beheer. Je kan via deze website een bestand uploaden in een veilige omgeving en dan stuurt deze website de downloadlink naar het emailadres die jij dan opgeeft. Deze persoon heeft dan een korte tijd (zelf in te stellen) om dit bestand te downloaden. Deze download link is dus een vorm van versleutelde gegevensverwerking. Je kunt er ook nog een extra versleuteling erop te zetten door er een wachtwoord aan te koppelen. Dan kan iemand de link downloaden maar nog niet openen. Voor het openen heeft die persoon het wachtwoord nodig. Dit wachtwoord kan je dan op een andere manier versturen (bijv. via een smsje of via een belletje).

Ik persoonlijk kies er voor, als ik data naar externe dataverwerkers stuur (bijv. Rux Button), om alles via SecureFilesender te sturen. Daarbij stuur ik dan ook een wachtwoord mee (via en naar een ander emailadres). Dan hebben ze dus een dubbele beveiliging op de data. Dat doe ik omdat ik niet weet hoe goed hun servers en mailboxen beveiligd zijn. Binnen de UiT weet ik wel dat de servers etc. goed zijn beveiligd en dat de lekken goed opgepakt worden door LIS.

14. Hoelang worden de gegevens bewaard in de database (bewaartermijn)? Worden ze daadwerkelijk vernietigd als het doel van de verwerking niet meer geldt? Indien nee, waarom worden ze niet vernietigd/verwijdert?

Voor alumni geldt: in principe oneindig. Als mensen vragen om te willen worden verwijderd uit de database, dan kan dat niet. Wel kunnen we alle contactgegevens, werkgeversinformatie etc. verwijderen. Maar de naam en de studiegegevens van de persoon zelf blijven er wel in staan. Wij hebben deze gegevens nodig om te kunnen controleren of hij/zij hier afgestudeerd is.

15. Wat gebeurt er als een betrokkene een beroep doet op een van zijn rechten; in het bijzonder recht op inzien van gegevens en verwijdering uit database?

Ten eerste kan dit nu op een officiële manier. Er is nu een juridische procedure die moet worden gevolgd. Wij zijn bijvoorbeeld niet de enige afdeling die persoonsgegevens heeft van een bepaalde persoon, want in ons geval heeft de studentenadministratie ook gegevens over alumnus of alumna. Als bijvoorbeeld een verzoek om verwijdering binnenkomt, krijgen wij een mail van de werkgroep AVG, met de opdracht, alle gegevens van desbetreffende persoon uit de database te verwijderen.

Is er tot nu toe dergelijk verzoek binnengekomen?
In het verleden zijn er wel een aantal mensen geweest die hebben gevraagd om te willen worden verwijderd uit de database. Maar dan antwoorden wij dat we alleen alle contactgegevens kunnen verwijderen, maar de persoon zelf (naam en studie) blijft wel bestaan in de database vanwege het feit dat hij/zij is afgestudeerd.

16. Wordt er gebruik gemaakt van profilering?

Binnen de database hebben wij een keer een Excel lijst gekregen van de top 100 met rijkste postcodes. Dat betekende dus dat de top 100 rijkste postcodes werden genoteerd. Bijv. een straat in Wassenaar. Wat wij toen hebben gedaan, is onze database matchen met de Excel lijst met de 100 rijkste postcodes. Zo konden we zien welke alumni in die postcode woont. Zo wisten we dus dat deze persoon

(hoogstwaarschijnlijk) een vermogend persoon is. Op dit moment hebben we er echter nog niet veel mee gedaan, we hebben deze personen alleen een tag gegeven in RE. Deze tag staat nog steeds in onze database, maar hebben we dus (nog) niet gebruikt voor bijvoorbeeld gerichte communicatie.

Hebben jullie ook andere soorten tag/aanwijzingen?
Functies kun je ook vaak zien. Daaruit kunnen wij ook concluderen dat die persoon vermogend is. Zoals bijv. een CEO van een groot bedrijf.

Wordt er ook nog bijgehouden wie de favoriete professor is?
Dat wordt niet meer bijgehouden, maar dit staat er nog wel in. Ik weet nog niet precies wat we hier mee gaan doen, maar ik ga deze gegevens hoogstwaarschijnlijk binnenkort uit de database verwijderen.

Staan er nog andere bijzondere gegevens in? Zoals medische of dergelijke?
In de database staan geen medische gegevens. Echter, kan het soms voorkomen dat ze er wel in staan. Tijdens belcampagnes bijvoorbeeld vertellen mensen hun verhaal aan de belstudent. De belstudent moet dan een korte samenvatting maken van het gesprek. Soms kan het dan zijn dat hierin staat dat die persoon afgelopen periode ernstig ziek was, dus die persoon wil dan bijv. op dat moment geen donatie doen. In dit verslag van het telefoongesprek komt dit dan ook te staan. Dit verslag komt dan wel weer in onze database, voor bijv. bij een volgende belcampagne of bij een volgende keer dat we die persoon benaderen. Dan weten we dat die persoon eventueel nog ziek is of niet benaderd wilt worden. Maar deze gegevens staan er dan alleen in als de persoon zelf aangeeft dat hij/zij ziek is. Dit gebeurt uitsluitend bij de gesprekken met die persoon tijdens de belcampagnes.

Bijlage H – Interview medewerkers van Library and IT-Servics

Interview over technische beveiliging RE

Dit interview heeft met twee personen plaatsgevonden. Een is werkzaam bij afdeling LIS en onderdeel van CERT team en de andere persoon is afdelingshoofd van IT Office Automation.

1. Hoe is de server (van de Universiteit) waarop RE draait beveiligd?
   Standaard met een firewall.

2. Welke technische beveiligingsmaatregelen zijn er getroffen om de persoonsgegevens te beschermen in de database RE?
   De database draait op een database cluster, waar meerdere databases op draaien. De beveiligingsmaatregelen die we genomen hebben aan de hand van toegangscontroles. Functioneel beheerder, technisch applicatie beheerder en back office personeel heeft daar digitale toegang tot. Verder is het afgeschermd met firewalls. Firewalls staan standaard dicht behalve. Dus niet standaard open en bepaalde delen dicht. Ze staan dus standaard op dicht, behalve op sommige werkplekken. De database zelf is ook beveiligd met gebruikersnaam en wachtwoord. De database is niet ge-encrypt omdat dit niet genoodzaakt is. De fysieke toegang is geregeld middels datacenter, alarmcode, sleutels en pasjes.

   Waarom is het niet genoodzaakt dat de database ge-encrypt is?
   Wij hoeven niet standaard gebruikersgegevens te encrypten, op een ge-ecnrypte schijf. We hoeven er alleen voor te zorgen dat het niet buiten de organisatie kan belanden. Er zijn natuurlijk gebruikers op RE, die kunnen er data uithalen maar ook daar zijn maatregelen getroffen maar die zijn eerder niet technisch van aard. Zoals het ondertekenen van iets. Het is niet encrypt omdat het nog niet is voorgeschreven. Bij wetenschappelijk onderzoek worden de gegevens soms wel ge-encrypt omdat je dan te maken hebt met bedrijfsgegevens of bankgegevens. De leverancier van deze data eist dan dat het ge-encrypt is. In dit geval is het door de juristen bepaald dat het nog niet hoeft voor RE.

3. Is, bij het opzetten van RE waarmee en waarin gegevens worden verwerkt, rekening gehouden met privacy (privacy by design)? Indien ja, hoe is er dan rekening gehouden met de privacy?
   Deze vraag kan ik niet beantwoorden.

4. Hoe wordt bij het gebruik van RE rekening gehouden met de privacy? (Privacy by default)/ Zijn de standaardinstellingen van RE op de meest privacy vriendelijke manier ingericht?
   Deze vraag kan ik niet beantwoorden.

5. Heeft er weleens een risico-analyse plaatsgevonden met betrekking tot de beveiliging van de database RE?
   Wij doen een keer per jaar risico-analyses op de gehele database omgeving, waar RE onderdeel van uit maakt. Het pakket zelf wordt door onze CERT team gepentest. Eens in de zoveel tijd pakken zij een applicatie eruit en proberen ze deze te hacken. Een keer per jaar doen we aan een landelijke security evenement, waar we een lokaal security risico-analyse; dat er bijvoorbeeld een nepstudent die in allerlei systemen probeert te komen.
   De risico-analyse ziet niet per se toe op alleen RE. Het pakket van alle databases wordt geanalyseerd. Het CERT team kiest jaarlijks een paar applicaties die ze pentesten. Kan ook op verzoek van een afdeling. Het kan ook zo zijn dat het bedrijf RE zelf pentesten overlegd met bevindingen. Dit kost wel altijd geld.

6. Worden er back-ups gemaakt van de database?

Elke uur, elke dag en elke week. De back-ups worden bewaard in Amsterdam, bij SURFsara. Deze back-ups worden ge-encrypt opgeslagen. Elk uur wordt een deel van de database en elke dag een volledige. Elk uur wordt er geplust. Dus van alle nieuwe wijzigingen wordt een back-up gemaakt. Aan het einde van de dag wordt een gehele back-up gemaakt. De back-ups van een uur worden dan weggegooid. Dit gebeurt heel het jaar door. Met een retentie van twee weken. Dus we kunnen back-ups van databases tot twee weken terug erbij pakken. Na twee weken worden de volledige back-ups weggegooid. Met SURFsara hebben we een bewerkersovereenkomst. Vroeger was SURFsara onderdeeld van SURFnet, maar dit is nu geprivatiseerd. Met elke leverancier waarmee we data uitwisselen wordt een bewerkersovereenkomst gesloten. Waarin staat locatie, hoe wat waar certificaten etc. Zij hebben ook toegangscontroles tot hun datacenter en dit moeten ze overleggen. Zoals hoe krijg je toegang tot onze back-ups daar op locatie.

7. Welke preventieve maatregelen zijn er getroffen ter voorkoming van een datalek uit de database? Is er weleens een datalek voorgekomen mbt de database? Hoe werd dit opgelost? Welke stappen werden er toen genomen?
   We hebben een datalek protocol en een team. Er zijn naar mijn weten nog nooit gegevens gelekt uit RE. Maar het kan ook zijn dat het nooit gemeld is, aangezien de meldplicht datalekken pas sinds 2016 in is gegaan.

8. Worden de medewerkers door jullie geïnstrueerd welke beveiligingsmaatregelen ze kunnen treffen? (vb. laptop locken als ze van plek af gaan etc)
   Ja, we instrueren. Met CERT hebben we security awareness trainingen. Deze doen we meestal per afdeling. Dit noemen we de roadshow. Waarbij we eigenlijk in een uurtje de basisbeginselen van IT uitleggen. Hoe ze bijvoorbeeld om moeten gaan met phising, hoe ze phising kunnen herkennen. Dus eigenlijk welke risico's komen op hun af. Daaraan vast plakken we een half uurtje over persoonsgegevens en dat doet Juridische Zaken. CERT (Computer Emergency Response Team). Ook hebben we regelmatig overleg. Heel vaak hebben bepaalde incidenten een juridische kant. De beheerders weten ook dat als er een bepaalde dataset naar een leverancier gaat, dat ze dat niet zomaar mogen doen. Ze dienen zichzelf de vraag te stellen of er een verwerkersovereenkomst is en of dit wel mag. Er is dus veel aandacht voor persoonsgegevens.

9. Indien DARO een bewerkersovereenkomst aangaat met een derde partij. Zijn jullie hiervan op de hoogte? Wie controleert de technische beveiliging van deze partijen dan? Hoe worden deze partijen gecontroleerd? (audit wss)
   Ik weet niet of we van alle bewerkersovereenkomsten op de hoogte zijn. Als er een bewerkersovereenkomst gesloten wordt, die bij Juridische Zaken bekend is dan ben ik hiervan ook op de hoogte. Er wordt een standaard model bewerkersovereenkomst gebruikt, die toegespitst is op TiU. Dit model hebben we wat zwaarder gemaakt. Wat betreft de veiligheid heb ik er een stuk ingezet. Dit stuk houdt in dat de software moet voldoen aan de ACS standaard en deze bestaat uit drie niveaus. De gevoeligheid van de persoonsgegevens; middel hoog of laag; bepaald de beveiligingsstandaard. Een bedrijf moet zelf een rapport opleveren waarin de beveiliging staat beschreven, die wij vervolgens controleren. Aan de hand van deze controle kunnen wij bepalen of zij voldoen aan de standaard. Hier tekenen zij ook voor.

   Wat staat er in dit rapport?

Wij vragen een recent security rapport van minder dan een jaar oud. Die moeten zij overleggen, desnoods onder NDA. Dit houdt in dat wij het rapport inzien, maar niet doorzenden naar andere. Dit rapport is eigenlijk een waarborg voor ons dat een bedrijf serieus met de beveiliging omgaat.

Is dit de enige manier waarop de partij gecontroleerd wordt?
Als zij niet een rapport overleggen, dan gaan wij met hun in overleg. Eventueel testen wij hun beveiliging zelf. Wij hebben een CERT team waarin mensen zitten die kunnen pentesten. Deze mensen kunnen dus de beveiliging van applicaties onderzoeken. Op het moment dat wij vinden dat het niet veilig is, dan gaan wij in discussie met de leverancier. In enkele gevallen kan het zo zijn dat wij het MT adviseren om niet met een bepaalde softwarepakket in zee te gaan, omdat wij vinden dat het niet veilig is en dus niet aan onze standaarden voldoet. Dit waarborgen we ook doordat zij hiervoor tekenen in de bewerkersovereenkomst.

Je hebt een information security audit en je hebt een technische audit penetratietest; waarbij je eigenlijk probeert in te breken in een applicatie. Waarbij je eigenlijk echt de beveiliging probeert te testen. Een it audit richt zich vaak meer op procedures; is er een back-up geregeld, wat gebeurt er in het geval er calamiteit voordoet. Die eigenlijk de procedures bekijkt of dat je die geregeld hebt. Wat wij meer doen is kijken of een pakket echt veilig is.

We proberen dit periodiek te doen, maar in de praktijk hebben we niet een tijdstip vastgelegd waarop we het doen. We houden mensen wel de rechten voor dat op het moment dat er een kwetsbaarheid is, dan kijken we wel of applicaties daarvoor vatbaar zijn. Dit doen we alleen niet op een structurele manier. Dit doen we meestal als we zien dat er ergens op de wereld een lek is. Dan kijken we of dat wij er last van hebben of de servers waar wij data hebben ondergebracht. Dan spreken we ook de leverancier daarop aan. Dus dat is eigenlijk meer incidenteel.