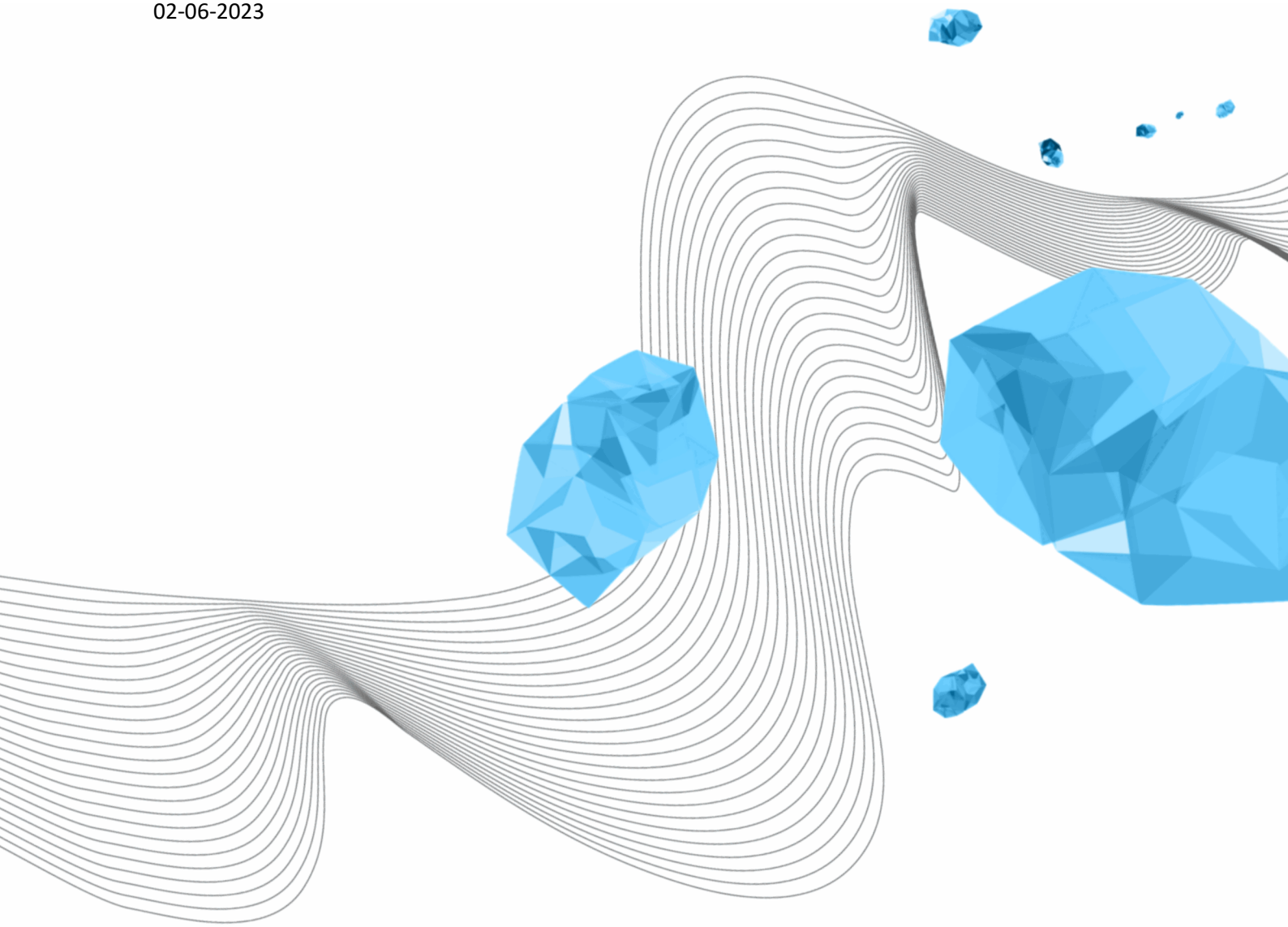
Status: Definitief
Datum vastgesteld in CvB: 12-06-2023
Auteur: Rianne te Brake/Jan Evers/Meike van de Ven-Davids/G.B. Meijer

PRIVACYBELEID UNIVERSITEIT TWENTE

LISA

Versie v2.4

02-06-2023



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Privacybeleid Universiteit Twente

KENMERK
UIM/181218/brk

VERSIE (STATUS)
v2.4

DATUM
02-06-2023

AUTEUR(S)
R. te Brake/J.L. Evers/M. van de Ven-Davids/G.B. Meijer

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR(S)	OPMERKINGEN
1.0	10-10-2016	W. Koolhoven / J.L. Evers	Definitieve eerste versie Vastgesteld in CvB van 17-10-2016
1.1	19-12-2018	R. te Brake	Actualisatie: - Nieuw Model beleid SURF (maart 2018) - Aanvullingen door nieuwe privacywetgeving (AVG) - Kleine correcties
1.2	16-01-2019	R. te Brake	Opmerkingen uit Security + Privacy overleg verwerkt
1.3	12-02-2019	J.L. Evers	Opmerkingen MT LISA verwerkt Bijlage Privacyregels uit het Beleid gehaald; zal als apart document beheerd worden; deze regels geven een praktische vertaling van het Privacybeleid voor verschillende deelgebieden.
1.4	18-06-2019	J.L. Evers	Advies UR dd 5-6-2019 in par. 4.9 verwerkt: begeleider verantwoordelijk voor onderzoek door en voorlichting aan student
1.5	02-10-2019	J.L. Evers	25-09-2019 UR: instemming, onder toezegging van 1. UT-begeleider, 2. cultuurverenigingen toevoegen aan lijst met derden
2.0	14-10-2022	M. van de Ven-Davids	Actualisatie: - Nieuw Model Privacy Beleid SURF (november 2021) - Actualisaties naar feitelijke situatie - Correcties - Meer aansluiting op beleidsprincipes
2.1	14-11-2022	G.B. Meijer	Review en enkele aanpassingen.
2.1	06-01-2023	M. van de Ven-Davids	Aantal tekstuele aanpassingen en aanpassingen in layout
2.2	17-02-2023	M. van de Ven-Davids	Aanpassingen n.a.v. opmerkingen MT LISA

[1] https://www.surf.nl/files/2022-02/surf-model-beleid-verwerking-persoonsgegevens-update-2021_0.pdf
[2] https://creativecommons.org/licenses/by/4.0/deed.nl

2.3	03-05-2023	M. van de Ven-Davids	Aanpassingen n.a.v. advies Universiteitsraad
2.4	02-06-2023	M. van de Ven-Davids	Aanpassingen n.a.v. besluit Universiteitsraad
2.4	12-06-2023	M. van de Ven-Davids	Vaststelling door CvB

DISTRIBUTIELIJST

VERSIE	DATUM	AUTEUR(S)	GEDISTRIBUEERD AAN
1.1	19-12-2018	R. te Brake	Leden Security + Privacy overleg
1.2	25-01-2019	J.L. Evers	MT LISA
1.3	12-02-2019	J.L. Evers	02-04-2019 UCB (positief advies) 15-04-2019 CvB (vastgesteld) 24-04-2019 UR (ter informatie)
1.4	18-06-2019	J.L. Evers	01-07-2019 CvB (ter vaststelling) 25-09-2019 UR (ter instemming)
1.5	02-10-2019	J.L. Evers	14-10-2019 CvB (vastgesteld)
2.1	06-01-2023	M. van de Ven-Davids	MT LISA
2.2	20-02-2023	M. van de Ven-Davids	MT LISA
2.2	06-03-2023	M. van de Ven-Davids	CvB
2.2	30-03-2023	M. van de Ven-Davids	UR
2.3	03-05-2023	M. van de Ven-Davids	CvB UR
2.4	02-06-2023	M. van de Ven-Davids	CvB UR

INHOUDSOPGAVE

1 Inleiding 6
1.1 Definities en afkortingen 6
1.2 Reikwijdte en doelstelling van het privacybeleid 7
1.2.1 Reikwijdte van het Beleid 7
1.2.2 Doelstelling van het Beleid 8
2 Beleidsprincipes Verwerking Persoonsgegevens 9
3 Wet- en regelgeving 11
3.1 Wet op het Hoger onderwijs en Wetenschappelijk onderzoek 11
3.2 Algemene Verordening Gegevensbescherming en Uitvoeringswet AVG 11
3.3 Arbeidsregelgeving en CAO 11
3.4 Archiefwet 11
3.5 Telecommunicatiewet 11
4 Rollen en verantwoordelijkheden met betrekking tot Verwerking Persoonsgegevens 12
4.1 Overlap met informatiebeveiliging 12
4.2 College van Bestuur 12
4.3 Portefeuillehouder privacy 12
4.4 Functionaris Gegevensbescherming 12
4.5 De Systeemeigenaar 13
4.6 Directeur 13
4.7 Leidinggevende 13
4.8 Privacy Contact Persoon 13
4.9 Onderzoeker 14
4.10 Gerelateerde organisaties en gelieerde instellingen 14
4.11 Verdeling van verantwoordelijkheden 14
5 Implementatie privacybeleid 15
5.1 Inpassing in de instellingsgovernance 15
5.2 Bewustwording en training 15
5.3 Controle en naleving 15
6 Rechtmatige en zorgvuldige Verwerking van Persoonsgegevens 16
6.1 Verantwoordelijkheid 16
6.2 Legitiem doel en grondslag 16
6.3 Ethisch verantwoord 17

6.4 Dataminimalisatie 17
6.5 Doelbinding 18
6.6 Bewaren en vernietigen 18
6.7 Juistheid 18
6.8 Transparantie en informatie 18
6.8.1 Recht op informatie 19
6.9 Delen van Persoonsgegevens 19
6.9.1 Uitbesteden van Verwerking aan een Verwerker 19
6.9.2 Verwerking door of gezamenlijk met een andere Verwerkingsverantwoordelijke 19
6.9.3 Doorgifte Persoonsgegevens binnen de Europese Economische Ruimte 20
6.9.4 Doorgifte Persoonsgegevens buiten de EER 20
6.10 Informatiebeveiliging 20
6.11 Rechten van Betrokkenen 20
6.11.1 Recht op inzage 21
6.11.2 Recht op gegevensoverdraagbaarheid 22
6.11.3 Recht op rectificatie, aanvulling, verwijdering of beperking van de Verwerking 22
6.11.4 Recht van bezwaar 22
6.11.5 Geautomatiseerde besluitvorming 23
6.11.6 Rechtsbescherming 23
6.12 Verantwoordingsplicht 24
7 Datalekken 25
7.1 Datalek 25
7.2 Melding en registratie 25
7.3 Afhandeling 25
7.4 Evaluatie 25
8 Tot slot 26

1 INLEIDING

In onze toenemend gedigitaliseerde maatschappij krijgt privacy steeds meer aandacht. High Tech, Human Touch is het motto van de Universiteit Twente (UT), en Human Touch impliceert aandacht voor privacy bij onderzoek, onderwijs en bedrijfsvoering. Het gebruik van Persoonsgegevens is noodzakelijk om de bedrijfsprocessen van de UT te kunnen uitvoeren. Dit dient met de grootste zorgvuldigheid te gebeuren, omdat de UT het welzijn van studenten, medewerkers en andere Betrokkenen belangrijk vindt en misbruik van Persoonsgegevens grote schade kan berokkenen.

Met de maatregelen beschreven in dit beleidsdocument neemt de UT haar verantwoordelijkheid om de kwaliteit van de Verwerking en de beveiliging van Persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving.

Dit Beleid is een herziene versie van het Privacybeleid Universiteit Twente van 2 oktober 2019.

1.1 DEFINITIES EN AFKORTINGEN[3]

Anonimiseren: is een methode waarbij Persoonsgegevens zodanig worden bewerkt dat deze niet meer gebruikt kunnen worden om een persoon te identificeren. Ook niet als deze gegevens gecombineerd worden met andere gegevens. Deze bewerking is onomkeerbaar.

AP: Autoriteit Persoonsgegevens. De Nederlandse privacy toezichthouder.

AVG: Algemene Verordening Gegevensbescherming[4].

Beleid: Dit beleid met betrekking tot het Verwerken van Persoonsgegevens door de UT.

Betrokkene: Een geïdentificeerd of identificeerbaar natuurlijk persoon op wie een Persoonsgegeven betrekking heeft.

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

CERT-UT: Computer Emergency Response Team Universiteit Twente.

CvB: College van Bestuur

Datalek: Een inbreuk op de beveiliging van Persoonsgegevens, die per ongeluk of opzettelijk leidt tot de vernietiging, het verlies, de wijziging of ongeoorloofde toegang tot die gegevens.

Derde: Een partij, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch enig persoon die onder rechtstreeks gezag valt van de Verwerkingsverantwoordelijke of de Verwerker, die gemachtigd is om Persoonsgegevens te Verwerken.

DPIA (Data Protection Impact Assessment of gegevensbeschermingseffectbeoordeling): Een beoordeling van een Verwerking die helpt bij het beoordelen van de rechtmatigheid van de Verwerking, het identificeren van privacy risico's en die maatregelen voorstelt om deze risico's te verkleinen om bescherming van persoonsgegevens te garanderen.

DTIA (Data Transfer Impact Assessment): Aan de hand van een DTIA doet de UT voorafgaand onderzoek naar de privacy risico's die spelen bij een doorgifte van Persoonsgegevens naar een land buiten de EER. Het is de bedoeling om de risico's in kaart te brengen en extra maatregelen te nemen om deze weg te nemen of zo veel mogelijk te verminderen.

[3] In verband met leesbaarheid zijn sommige definities verkort weergegeven. Voor volledige definities zie AVG.
[4] De AVG is op 25 mei 2016 in werking getreden en per 25 mei 2018 van kracht.

EER: Europese Economische Ruimte.

Functionaris Gegevensbescherming (FG): de persoon die door de UT is aangewezen om intern toe te zien op naleving van privacy wetgeving en te adviseren op nader in de AVG genoemde specifieke onderwerpen. De FG is aangemeld bij de AP en heeft een FG-nummer toegekend gekregen. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie bij de UT.

Minderjarige: Iedereen die de leeftijd van 16 jaar nog niet heeft bereikt is in het kader van de privacy wetgeving minderjarig.

PBV: Portefeuillehouder Bedrijfsvoering van een faculteit.

PCP: Privacy Contact Persoon van een dienst of faculteit.

Persoonsgegeven: Alle informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon.

Privacy by Default: De verplichting die op de Verwerkingsverantwoordelijke rust om de standaardinstellingen van Verwerkingen zo in te stellen dat de privacy van Betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk Persoonsgegevens worden gevraagd en Verwerkt.

Privacy by Design: De verplichting die op de Verwerkingsverantwoordelijke rust om gedurende de gehele levenscyclus van Persoonsgegevens passende waarborgen in te bouwen en maatregelen te treffen om de beginselen die de AVG noemt op een doeltreffende manier uit te voeren. Hierbij wordt stelselmatig aandacht besteed aan allesomvattende waarborgen m.b.t. vertrouwelijkheid, integriteit, beschikbaarheid, fysieke veiligheid en verwijdering van de Persoonsgegevens (bv. Autorisatiematrixen bewaartermijnen,..).

Profilering: Elke vorm van geautomatiseerde Verwerking van Persoonsgegevens waarbij aan de hand van Persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming.

UCB: Universitaire Commissie Bedrijfsvoering.

UT: Universiteit Twente.

Verwerker: Een partij die ten behoeve van en op instructie van de UT Persoonsgegevens Verwerkt.

Verwerking: Elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: Een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, doel en middelen van een Verwerking van Persoonsgegevens vaststelt. In dit Beleid doorgaans het College van Bestuur (CvB) van de UT.

1.2 REIKWIJDTE EN DOELSTELLING VAN HET PRIVACYBELEID

1.2.1 REIKWIJDTE VAN HET BELEID

Het Beleid is van belang voor alle medewerkers, studenten en andere relaties van de UT. Het heeft consequenties voor het werk van alle medewerkers en studenten die met Persoonsgegevens werken. Het Beleid heeft betrekking op het Verwerken van Persoonsgegevens van alle Betrokkenen binnen de

UT, waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur/outsourcing), alsmede op andere Betrokkenen waarvan de UT Persoonsgegevens Verwerkt, bijvoorbeeld proefpersonen die deelnemen aan wetenschappelijk onderzoek[5].

Het Beleid betreft niet het Verwerken van Persoonsgegevens voor persoonlijk of huishoudelijk gebruik, zoals persoonlijke werkaantekeningen of een verzameling visitekaartjes. In het Beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde en/of systematische Verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de UT, alsmede op de daaraan ten grondslag liggende (al dan niet elektronische) documenten. Eveneens is het Beleid van toepassing op de Verwerking van Persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder Persoonsgegevens. Er wordt aandacht geschonken aan deze raakvlakken en er wordt zowel planmatig als inhoudelijk afstemming gezocht.

Het Beleid heeft als doel om de kwaliteit van de Verwerking en de beveiliging van Persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de Betrokkene zoveel mogelijk te respecteren. De gegevens die betrekking hebben op een Betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik en tegen verlies dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar Persoonsgegevens. Dit brengt met zich mee dat het Verwerken van Persoonsgegevens dient te voldoen aan relevante wet- en regelgeving zodat Persoonsgegevens veilig zijn bij de UT.

1.2.2 DOELSTELLING VAN HET BELEID

Het Beleid geeft studenten, medewerkers en andere Betrokkenen inzicht in hoe de UT invulling geeft aan gegevensbescherming. Daarnaast helpt het bij het creëren van bewustwording over het belang en de noodzaak van het beschermen van Persoonsgegevens.

Doelstelling van het Beleid is concreet het volgende:

- Het bieden van een *kader*: om (toekomstige) Verwerkingen van Persoonsgegevens te toetsen aan een vastgestelde ‘best practice’ of norm; en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie eenduidig te beleggen.
- Het stellen van *normen*: vaststellen hoe de organisatie om wil gaan met Persoonsgegevens.
- Het SURF Juridisch Normenkader Cloudservices[6] wordt gehanteerd als best practice voor cloud services en andere outsource contracten.
- Het nemen van *verantwoordelijkheid* door het CvB: door de uitgangspunten en de organisatie van het Verwerken van Persoonsgegevens vast te leggen voor de hele UT.
- *Daadkrachtige* implementatie van het Beleid door duidelijke keuzes te maken in maatregelen en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen.
- *Compliant* zijn met de Nederlandse en Europese wetgeving.

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het creëren van bewustwording van het belang en de noodzaak van het beschermen van Persoonsgegevens, mede ter vermijding van risico’s als gevolg van het niet compliant zijn met de relevante wet- en regelgeving.

[5] Het document ‘Zorgvuldig gebruik van persoonsgegevens in onderzoek volgens de AVG’ (zie https://www.utwente.nl/nl/cyber-safety/privacy/leidraad-voor-onderzoek/) gaat specifiek in op het Verwerken van Persoonsgegevens in wetenschappelijk onderzoek.

[6] SURF juridisch Normenkader (Cloud)services, vastgesteld door bestuur Platform ICT & Bedrijfsvoering 3 april 2014 en geüpdatet in 2016, te vinden via surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch-normenkader-cloudservices.pdf

2 BELEIDSPRINCIPES VERWERKING PERSOONSGEGEVENS

Algemeen beleidsuitgangspunt is dat Persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden Verwerkt. Hierbij dient een goede balans te worden gevonden tussen het belang van de UT om Persoonsgegevens te Verwerken en het belang van Betrokkene ter eerbiediging van zijn persoonlijke levenssfeer en om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

1. Verantwoordelijkheid:
    - Voor iedere gegevensverwerking is (intern) een verantwoordelijke benoemd.
    - De verantwoordelijke maakt afspraken met Verwerkers en eventuele Derden over de veilige en zorgvuldige Verwerking van Persoonsgegevens.
2. Legitiem doel en grondslag:
    - Het doel van de Verwerking moet voorafgaande aan de Verwerking voldoende specifiek en helder omschreven zijn.
    - Een Verwerking van Persoonsgegevens is gebaseerd op één van de wettelijke grondslagen zoals genoemd in artikel 6 van de AVG en in paragraaf 6.2 van dit Beleid.
3. Ethisch verantwoord
    - Bij het beoordelen van Verwerkingen van Persoonsgegevens wordt ook rekening gehouden met ethische aspecten (het mag misschien, maar willen we dit ook).
4. Dataminimalisatie
    - Er worden niet meer Persoonsgegevens verzameld dan noodzakelijk is voor het doel dat men wil bereiken. Persoonsgegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn.
    - Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (subsidiariteits- en proportionaliteitsbeginsel).
5. Doelbinding
    - Persoonsgegevens worden niet verder Verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
6. Bewaren en vernietigen
    - Persoonsgegevens zijn voorzien van een bewaartermijn.
    - Persoonsgegevens worden vernietigd of geanonimiseerd wanneer deze niet langer nodig zijn voor de vastgestelde verwerkingsdoelen.
7. Juistheid
    - Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te Verwerken Persoonsgegevens juist en actueel zijn.
8. Transparantie en informatie
    - Voor Betrokkenen is het inzichtelijk in hoeverre en op welke manier er Persoonsgegevens worden Verwerkt. Informatie en communicatie hierover moet eenvoudig toegankelijk en begrijpelijk zijn, bijvoorbeeld door middel van een privacy statement.
9. Delen van Persoonsgegevens
    - Persoonsgegevens worden alleen gedeeld met anderen als daar een rechtmatige grondslag voor is.
    - Waar Persoonsgegevens gedeeld worden met andere partijen dienen daar goede afspraken over gemaakt te worden.

10. Informatiebeveiliging
    - Persoonsgegevens worden beveiligd door het nemen van passende technische en organisatorische maatregelen (risk-based).
    - Toegang tot Persoonsgegevens wordt gegeven op basis van need-to-know.
    - Systemen worden ontworpen en ingericht volgens de principes Privacy by Design en Privacy by Default.
11. Rechten van Betrokkenen
    - Iedere Betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van zijn/haar Persoonsgegevens, en heeft het recht van bezwaar.
    - Bij alle registraties die gebaseerd zijn op de grondslag “toestemming” wordt voorafgaande aan de Verwerking om toestemming gevraagd.
    - Toestemming is voor Betrokkenen net zo eenvoudig in te trekken als deze gegeven is.
12. Verantwoordingsplicht
    - De UT kan aantonen dat zij voldoet aan de AVG.

3 WET- EN REGELGEVING

Bij de UT wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

3.1 WET OP HET HOGER ONDERWIJS EN WETENSCHAPPELIJK ONDERZOEK

De UT heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden gedrags- en integriteitscodes voor (niet-)wetenschappelijk personeel nageleefd en toegepast.

3.2 ALGEMENE VERORDENING GEGEVENSBESCHERMING EN UITVOERINGSWET AVG

De UT heeft de wettelijke vereisten van de AVG en UAVG geïmplementeerd op basis van het Beleid. Dit betreft onder andere het rechtmatig en zorgvuldig Verwerken van Persoonsgegevens en het nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige Verwerking van Persoonsgegevens.

3.3 ARBEIDSREGELGEVING EN CAO

De UT draagt zorg voor goed werkgeverschap, waarin (onder meer) het zorgvuldig omgaan met Persoonsgegevens in de personeelsadministratie is gewaarborgd. Daarnaast worden er Persoonsgegevens gedeeld met bijvoorbeeld UWV, Belastingdienst en de bedrijfsarts.

3.4 ARCHIEFWET

De UT houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop moet worden omgegaan met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites en dergelijke.

3.5 TELECOMMUNICATIEWET

De UT voldoet aan de regelgeving ten aanzien van onder meer het gebruik van cookies zoals beschreven in de Telecommunicatiewet.

4 ROLLEN EN VERANTWOORDELIJKHEDEN MET BETREKKING TOT VERWERKING PERSOONSGEGEVENS

Om de Verwerkingen van Persoonsgegevens gestructureerd en gecoördineerd op te pakken is een aantal rollen en verantwoordelijkheden toegewezen aan functionarissen in de bestaande organisatie.

4.1 OVERLAP MET INFORMATIEBEVEILIGING

De Information Security Officer[7] en de IT Security Manager[8] zijn nauw betrokken bij de implementatie van het Beleid. Het zorgvuldig omgaan met Persoonsgegevens valt namelijk deels onder de algemene regels rondom informatiebeveiliging[9].

4.2 COLLEGE VAN BESTUUR

Het CvB is de Verwerkingsverantwoordelijke en daarmee eindverantwoordelijk voor de rechtmatige en zorgvuldige Verwerking van Persoonsgegevens binnen de UT. Het CvB stelt het beleid, de maatregelen en de procedures rondom Verwerkingen vast met dit Beleid.

4.3 PORTEFEUILLEHOUDER PRIVACY

De portefeuillehouder privacy is het bestuurslid dat privacy in portefeuille heeft. Hij/zij is namens het CvB eindverantwoordelijk voor de bescherming van Persoonsgegevens binnen de UT.

4.4 FUNCTIONARIS GEGEVENSBESCHERMING

De AVG verplicht de UT een interne toezichthouder op de Verwerking van Persoonsgegevens aan te stellen. Deze toezichthouder wordt de FG genoemd. De FG dient door de UT tijdig te worden betrokken bij alle aangelegenheden waar Persoonsgegevens bij komen kijken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De UT meldt de FG aan bij de AP.

De taken van de FG zijn:

- Het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG;
- Het toezien op de naleving van de AVG en andere relevante privacywetgeving;
- Het toezien op de naleving van dit Beleid;
- Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het betrokken personeel en de betreffende audits;
- Adviseren over en toezien op de uitvoering van DPIA’s;
- Het behandelen van klachten en/of vragen die rechtstreeks aan de FG zijn gericht;
- Het samenwerken met de AP;
- Fungeren als eerste aanspreekpunt voor de AP.

[7] De rol van Information Security Officer is vastgelegd in het Informatiebeveiligingsbeleid.
[8] De rol van Information Security Manager is vastgelegd in het Informatiebeveiligingsbeleid.
[9] Zie Informatiebeveiligingsbeleid Universiteit Twente, www.utwente.nl/nl/cyber-safety/cybersafety/wetgeving/informatiebeveiligingsbeleid.pdf.

4.5 DE SYSTEEMEIGENAAR

De systeemeigenaar is ervoor verantwoordelijk dat de applicatie (en bijbehorende ICT-faciliteiten) voldoet aan het Beleid. Dit betekent dat de systeemeigenaar er voor zorgt dat zowel nu als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving.

De systeemeigenaar heeft de volgende taken:

- Het (laten) opnemen van Verwerkingen van Persoonsgegevens in het verwerkingsregister;
- Het (laten) maken van schriftelijke afspraken over het delen van Persoonsgegevens zoals een verwerkersovereenkomst[10];
- Het in beeld (laten) brengen van risico's in geval van een Verwerking (DPIA en/of een DTIA)[11];
- Het (laten) uitvoeren van de maatregelen die nodig zijn om de risico's te beperken.

De systeemeigenaar kan hierin worden ondersteund door de PCP van de betreffende eenheid en de FG.

4.6 DIRECTEUR

De dienstdirecteur of PBV is verantwoordelijk voor de implementatie van het Beleid binnen zijn of haar eenheid. De directeur of PBV is ook verantwoordelijk voor Persoonsgegevens die vanuit zijn/haar eenheid in een instellingssysteem worden ingevoerd.

De directeur of PBV kan hierin ondersteund worden door de PCP en de FG.

4.7 LEIDINGGEVENDE

Het creëren van bewustwording en de naleving van het Beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn/haar medewerkers op de hoogte zijn van (de voor hun relevante aspecten van) het Beleid;
- het privacy bewustzijn van zijn/haar medewerkers toereikend te laten zijn;
- toe te zien op de naleving van het Beleid door zijn/haar medewerkers;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

De leidinggevende kan hierin ondersteund worden door de PCP en de FG.

4.8 PRIVACY CONTACT PERSOON

Ter ondersteuning van de taken van de FG is in elke eenheid (dienst / faculteit) een PCP aanwezig. Voor een universiteits-brede consistente uitvoering van het Beleid dragen de PCP's en FG er zorg voor bekend te zijn met elkaars werkzaamheden. Zij voeren periodiek overleg en informeren en ondersteunen elkaar. De PCP stemt de privacy-aangelegenheden binnen de eenheid af met de dienstdirecteur of PBV. Onder diens verantwoordelijkheid voert de PCP de volgende taken uit namens of binnen de eenheid:

- ambassadeurschap op het gebied van privacy;
- vergroten privacy-bewustzijn;
- borgen van de aandacht voor privacy in processen;
- adviseren, trainen en optreden als privacy-vraagbaak;
- coördineren van informatiebehoefte;
- ondersteunen van de uitvoering van een DPIA en/of DTIA;
- ondersteunen bij het vastleggen van gegevensverwerkingen;

[10]De UT hanteert modellen van o.a. verwerkersovereenkomsten. Ondertekende overeenkomsten dienen eveneens te worden opgenomen in het verwerkingsregister.
[11]De UT hanteert modellen van DPIA's en DTIA's. Uitgevoerde DPIA's en DTIA's dienen eveneens te worden opgenomen in het verwerkingsregister.

- ondersteunen bij het vaststellen verwerkersovereenkomsten;
- adviseren en ondersteunen bij Datalekken.

4.9 ONDERZOEKER

Iedere onderzoeker is verantwoordelijk voor de wijze waarop hij of zij met onderzoek data omgaat, in voorkomende gevallen samen met een onderzoeksleider. De hoogleraar of voorzitter van de onderzoeksgroep is eindverantwoordelijke.

De privacy-gevoeligheid en de ethische implicaties kunnen gevolgen hebben voor de wijze waarop met de onderzoek data moet worden omgegaan en voor de opzet van het onderzoek. Het proportionaliteitsprincipe geeft aan dat de Verwerking van Persoonsgegevens proportioneel moet zijn aan het beoogde (onderzoeks-)doel. Het is aan de onderzoeker om deze afweging te maken. In geval onderzoek wordt uitgevoerd door een student, is de UT-begeleider van de student verantwoordelijk voor de wijze waarop met Persoonsgegevens wordt omgegaan. De UT-begeleider draagt zorg voor een goede voorlichting aan de student.

4.10 GERELATEERDE ORGANISATIES EN GELIEERDE INSTELLINGEN

Aan de UT gelieerde instellingen, stichtingen en verenigingen zijn zelf verantwoordelijk voor het voldoen aan de privacywetgeving. Het is aan de gelieerde instelling zelf om compliancy met de (privacy-)wetgeving te realiseren. De UT zal het belang hiervan benadrukken en inzicht vragen in hoe compliancy gerealiseerd is.

Gegevensverwerkingen van gelieerde instellingen kunnen niet worden gemeld bij de FG van de UT. De gelieerde instellingen zijn zelf verantwoordelijk voor het bijhouden van een register met hun Verwerkingen.

Voor advies kunnen gelieerde instellingen een beroep doen op de FG van de UT.

4.11 VERDELING VAN VERANTWOORDELIJKHEDEN

Het zorgvuldig Verwerken van Persoonsgegevens is *een lijnverantwoordelijkheid***.** Dit betekent dat leidinggevenden de primaire verantwoordelijkheid dragen voor een zorgvuldige Verwerking van Persoonsgegevens binnen hun afdeling/eenheid. Dit omvat ook de keuze van en afstemming met de FG omtrent de maatregelen en de uitvoering en handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het Beleid met betrekking tot de Verwerking van Persoonsgegevens te communiceren met alle relevante partijen.

Het zorgvuldig omgaan met Persoonsgegevens is *ieders verantwoordelijkheid*. Van medewerkers, studenten, docenten en Derden wordt verwacht dat ze zich integer gedragen. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd[12].

Iedere Betrokkene van de instelling, waaronder medewerkers en studenten, wordt geacht een Datalek of vermoeden daarvan te melden bij CERT-UT (cert@utwente.nl). Er is een Datalekprocedure waarbij de FG een adviserende rol vervult.

[12] Zie https://www.utwente.nl/nl/cyber-safety/cybersafety/wetgeving/.

5 IMPLEMENTATIE PRIVACYBELEID

5.1 INPASSING IN DE INSTELLINGSGOVERNANCE

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van Verwerking van Persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.

Op **strategisch niveau** wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacy (IT-Board, CvB).

Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering (UCB, I-Beraad).

Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan (werkvloer, Security Managers, PCP, CERT-UT, werkoverleggen).

De FG adviseert en houdt toezicht binnen alle niveaus.

5.2 BEWUSTWORDING EN TRAINING

Beleid en technische en organisatorische maatregelen zijn niet voldoende om risico's op het terrein van het Verwerken van Persoonsgegevens uit te sluiten. Het is noodzakelijk om bij medewerkers en studenten het bewustzijn met betrekking tot privacy (en security) voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Good practices kunnen worden gedeeld met anderen in de organisatie, bijvoorbeeld via de Cybersafety-website van de UT.

Onderdeel van de uitvoering van het Beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en Derden. Deze campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met andere beveiligingscampagnes.

Verhoging van het security- en privacybewustzijn van medewerkers is de verantwoordelijkheid van de leidinggevenden, daarin ondersteund door de FG, de PCP's, de Information Security Officer (ISO) en de Security Managers.

5.3 CONTROLE EN NALEVING

De FG houdt toezicht op de naleving van de privacywetgeving en het Beleid. Aanvullend hierop maken audits het mogelijk het Beleid en de genomen maatregelen te controleren op effectiviteit.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus. Peer-reviews van SURFaudit maken onderdeel uit van de externe controles van de UT.

Mocht de naleving van maatregelen ter bescherming van Persoonsgegevens ernstig tekortschieten, dan kan de UT de betrokken medewerker of student een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Het Verwerken van Persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten de UT maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het Beleid.

6 RECHTMATIGE EN ZORGVULDIGE VERWERKING VAN PERSOONSGEGEVENS

De UT Verwerkt Persoonsgegevens in overeenstemming met de principes zoals uitgewerkt in paragraaf 2.1 van dit Beleid. Ter uitwerking van deze principes treft de UT de in dit hoofdstuk genoemde maatregelen.

6.1 VERANTWOORDELIJKHEID

Voor iedere gegevensverwerking is een verantwoordelijke aangewezen, veelal de systeemeigenaar (zie 4.5). De verantwoordelijke ziet erop toe dat de Verwerking voldoet aan de principes uit dit Beleid en laat zo nodig een DPIA en/of een DTIA uitvoeren. Middels een DPIA worden risico's in verband met de Verwerking van Persoonsgegevens in beeld gebracht en worden maatregelen ter verkleining van deze risico's door de systeem- of proceseigenaar toegepast. Aan de hand van een DTIA doet een organisatie voorafgaand onderzoek naar de privacy risico's die spelen bij een doorgifte van Persoonsgegevens naar een land buiten de EER. Het is de bedoeling om de risico's in kaart te brengen en extra maatregelen te nemen om deze weg te nemen of zo veel mogelijk te verminderen.

In samenwerkingsverbanden en bij uitbesteding is niet altijd direct duidelijk wie als Verwerkingsverantwoordelijke aangemerkt dient te worden. Helderheid hierover bij het maken van contractafspraken is noodzakelijk. Verwerkingsverantwoordelijke is degene die doel en middelen van de Verwerking bepaalt. De FG kan ondersteunen bij en adviseren over de vraag wie als Verwerkingsverantwoordelijke aangemerkt dient te worden.

De verantwoordelijke maakt afspraken met Verwerkers en eventuele Derden over de veilige en zorgvuldige Verwerking van Persoonsgegevens. Voor het maken van afspraken met andere partijen over het Verwerken en uitwisselen van Persoonsgegevens wordt gebruik gemaakt van de modelovereenkomsten van de UT. De PCP's en de FG kunnen hierover adviseren.

6.2 LEGITIEM DOEL EN GRONDSLAG

De UT Verwerkt alleen Persoonsgegevens als daar een gerechtvaardigd doel voor is. Het doel van een Verwerking wordt voorafgaande aan de Verwerking voldoende specifiek en helder omschreven. Dit ligt o.a. vast in het verwerkingsregister. De PCP's en FG kunnen ondersteunen bij de registratie in het verwerkingsregister.

De UT Verwerkt slechts Persoonsgegevens als er sprake is van één van de wettelijke grondslagen zoals beschreven in artikel 6 van de AVG:

a. toestemming van de Betrokkene;
b. noodzakelijk voor de uitvoering van een overeenkomst met de Betrokkene;
c. noodzakelijk om te voldoen aan een wettelijke verplichting die op de Verwerkingsverantwoordelijke rust;
d. noodzakelijk om de vitale belangen van de Betrokkene of een ander natuurlijk persoon te beschermen;
e. noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van uitoefening van openbaar gezag;
f. noodzakelijk voor de behartiging van het gerechtvaardigd belang van de Verwerkingsverantwoordelijke of een Derde.

Bij gebruik van de grondslag “toestemming” wordt de Betrokkene voordat deze toestemming geeft geïnformeerd over doel van de gegevensverwerking conform hetgeen in 6.9.1 staat bij het recht op informatie. De UT kan aantonen:

I) op welke wijze deze toestemming is gevraagd;
II) dat deze toestemming specifiek voor het beschreven doel is verleend; en
III) dat deze toestemming ondubbelzinnig is verleend.

De UT draagt er zorg voor dat het intrekken van toestemming net zo eenvoudig is als het geven ervan. Zij informeert de Betrokkene vooraf dat intrekken van toestemming de rechtmatigheid van de Verwerking tot het moment van intrekken niet aantast. Het intrekken van de toestemming werkt niet met terugwerkende kracht.
De UT houdt er rekening mee dat de toestemming vrijelijk moet worden gegeven zonder directe of indirecte druk. Aangezien er tussen de UT enerzijds en studenten of medewerkers anderzijds een machtsverhouding bestaat, zal goed gemotiveerd moeten worden waarom in het specifieke geval de toestemming wel vrij kan worden gegeven.

Bijzondere persoonsgegevens

Het Verwerken van Bijzondere persoonsgegevens is in beginsel verboden, tenzij er sprake is van een wettelijke uitzondering (o.a. wanneer de Betrokkene uitdrukkelijk toestemming heeft gegeven; ook gelden er uitzonderingen voor wetenschappelijk onderzoek). Bovendien gelden zwaardere eisen voor de beveiliging van Bijzondere persoonsgegevens. Daar waar de basisbescherming niet voldoende is, moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

6.3 ETHISCH VERANTWOORD

Bij het beoordelen van Verwerkingen van Persoonsgegevens wordt ook rekening gehouden met ethische aspecten (het mag misschien, maar willen we dit ook?). Deze aspecten worden meer in het bijzondere meegenomen bij Verwerkingen die bedoeld zijn om te Profileren of daar naar hun aard om vragen, bijvoorbeeld omdat nieuwe technologieën worden gebruikt.

Ethische aspecten spelen ook een rol bij mensgebonden onderzoek. Als het onderzoek daarnaast ook nog WMO[13] plichtig is dient er een toetsing plaats te vinden door een erkende medisch ethische commissies (METC).

6.4 DATAMINIMALISATIE

Er worden niet meer gegevens verzameld dan noodzakelijk voor het doel dat de UT wil bereiken met het Verwerken van die gegevens. Persoonsgegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn.

Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (subsidiariteits- en proportionaliteitsbeginsel). Als het doel ook bereikt kan worden op een manier die minder inbreuk maakt op de privacy van de Betrokkene, dan wordt voor deze manier gekozen. (Denk bijvoorbeeld aan het vragen naar een geboortedatum vs het vragen naar een leeftijdscategorie of het anoniem verzamelen van gegevens).

De UT geeft invulling aan deze beginselen door het toepassen van Privacy by Default en Privacy by Design bij ingebruikname van nieuwe systemen of processen.
Privacy by Design betreft het realiseren van gegevensbescherming door ontwerp, waarbij mechanismen worden ontworpen om gedurende de levenscyclus van Persoonsgegevens de privacy van Betrokkenen zoveel mogelijk te beschermen. Hierbij wordt stelselmatig aandacht besteed aan onder meer nauwkeurigheid, vertrouwelijkheid en integriteit van Persoonsgegevens.

[13] Uw onderzoek: WMO-plichtig of niet? | Onderzoekers | Centrale Commissie Mensgebonden Onderzoek (ccmo.nl)

Privacy by Default gaat om het beschermen van Persoonsgegevens door middel van standaardinstellingen van producten en diensten, die er zoveel mogelijk op gericht zijn de privacy van Betrokkenen te beschermen.

6.5 DOELBINDING

Persoonsgegevens die voor een bepaald doel verzameld zijn, mogen alleen verder worden Verwerkt voor andere doeleinden als deze doeleinden verenigbaar zijn met het oorspronkelijke doel.

Indien de UT verdere Verwerking wenselijk acht, dan dient aan een aantal elementen te worden getoetst of de verdere Verwerking verenigbaar is:

- Het verband tussen het nieuwe doel en het oorspronkelijke doel. Hoe dichter de twee doelen bij elkaar liggen, hoe eerder de verdere Verwerking van Persoonsgegevens verenigbaar is met het oorspronkelijke doel.
- De context waarin de Persoonsgegevens zijn verzameld. Hierbij wordt in belangrijke mate rekening gehouden met de redelijke verwachting die de Betrokkene mag hebben betreffende de verdere Verwerking van zijn Persoonsgegevens voor dit nieuwe doel.
- De aard van de Persoonsgegevens. Wanneer het bijvoorbeeld gevoelige Persoonsgegevens betreft, geldt dat deze een hoger beschermingsniveau verdienen en dat deze minder snel voor andere doelen mogen worden gebruikt.
- De mogelijke gevolgen van de verdere Verwerking voor Betrokkenen.
- Het bestaan van passende waarborgen, zoals versleuteling of het gebruik van gepseudonimiseerde Persoonsgegevens.

De verdere Verwerking van Persoonsgegevens voor wetenschappelijk en historisch onderzoek, voor statistische doeleinden en voor archiveringsdoeleinden in het algemeen belang, worden door de AVG als verenigbaar aangemerkt, mits voldoende passende technische en organisatorische maatregelen zijn toegepast, zoals bijvoorbeeld het pseudonimiseren van Persoonsgegevens.

Indien de UT Persoonsgegevens wenst te Verwerken voor een doel dat onverenigbaar is met het oorspronkelijk doel dan kan dat alleen als de Betrokkene hiervoor toestemming heeft gegeven of in geval van een specifieke wettelijke verplichting om bepaalde Persoonsgegevens te verstrekken aan een overheidsorgaan. In zo'n geval is er sprake van een nieuwe Verwerking van Persoonsgegevens en moet opnieuw de rechtmatigheid, zorgvuldigheid en noodzakelijkheid hiervan worden beoordeeld.

6.6 BEWAREN EN VERNIETIGEN

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. De UT zal de Persoonsgegevens na het verlopen van de bewaartermijn vernietigen, Anonimiseren of, indien de Persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren en passende technische en organisatorische maatregelen nemen, zoals pseudonimisering

6.7 JUISTHEID

Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te Verwerken Persoonsgegevens juist en actueel zijn. Deze maatregelen kunnen verschillen per proces/systeem. Gegevens die onjuist of achterhaald zijn worden gecorrigeerd of gewist. De UT toont een actieve houding in het juist en actueel houden van Persoonsgegevens. Processen en systemen zijn zoveel mogelijk zo ontworpen en ingericht dat juistheid van gegevens zoveel mogelijk afgedwongen en controleerbaar wordt.

6.8 TRANSPARANTIE EN INFORMATIE

De UT Verwerkt Persoonsgegevens op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat de UT aan de Betrokkene onder andere inzichtelijk maakt in hoeverre en op welke manier diens Persoonsgegevens Verwerkt worden, bijvoorbeeld door middel van een

privacy statement of informatiebrief. Het informeren van Betrokkenen vindt plaats voorafgaand aan de Verwerking, tenzij dit redelijkerwijs niet mogelijk is.

6.8.1 RECHT OP INFORMATIE

De Betrokkene heeft het recht om door de UT te worden geïnformeerd over bepaalde aspecten van de Verwerking van zijn Persoonsgegevens, bijvoorbeeld door middel van een privacy statement. De UT informeert de Betrokkene over de Verwerking van diens Persoonsgegevens, zowel in de situatie waarin de Persoonsgegevens direct bij de Betrokkene zijn verzameld, als wanneer ze langs een andere route zijn verkregen. De UT kan aantonen dat de informatie verstrekt is.

6.8.1.1 VERKRIJGING DIRECT VAN BETROKKENE

De UT verstrekt de Betrokkene voorafgaand aan de verzameling van de gegevens, tenminste de volgende informatie indien de gegevens direct bij de Betrokkene worden verzameld:

- De identiteit en contactgegevens van de Verwerkingsverantwoordelijke en de FG;
- De doeleinden en de grondslag van de Verwerking;
    - Wanneer de Verwerking is gebaseerd op de grondslag ‘gerechtvaardigd belang’: de gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of Derde;
- De (categorieën van) ontvangers van de Persoonsgegevens;
- In voorkomend geval, het voornemen van de Verwerkingsverantwoordelijke om de Persoonsgegevens door te geven aan een land buiten de EER, welk land dit is en op welke juridische grond;
- De bewaartermijn van de Persoonsgegevens of de criteria om deze termijn te bepalen;
- De rechten van Betrokkenen;
- Indien de Verwerking is gebaseerd op de grondslag ‘toestemming’, het recht van de Betrokkene om die toestemming te allen tijde in te trekken;
- Het recht om een klacht in te dienen bij de AP;
- Of en waarom de Betrokkene verplicht is de Persoonsgegevens te verstrekken en wat de gevolgen zijn als de Persoonsgegevens niet worden verstrekt;
- Of gebruik wordt gemaakt van geautomatiseerde besluitvorming (inclusief Profilering).

6.8.1.2 VERKRIJGING NIET DIRECT VAN BETROKKENE

Als de Persoonsgegevens niet direct bij de Betrokkene zelf zijn verzameld maar langs een andere route, zal aan de Betrokkene, in aanvulling op de hiervoor genoemde punten, de volgende informatie worden verstrekt:

- De categorieën van Persoonsgegevens.
- De bron waar de Persoonsgegevens vandaan komen.

Deze informatie zal zo snel mogelijk, maar niet later dan één maand, na verkrijging van de gegevens, dan wel bij het eerste contact met de Betrokkene, worden verstrekt.

6.9 DELEN VAN PERSOONSGEGEVENS

6.9.1 UITBESTEDEN VAN VERWERKING AAN EEN VERWERKER

Indien de UT Persoonsgegevens laat Verwerken door een Verwerker, wordt de uitvoering van Verwerkingen geregeld in een verwerkersovereenkomst tussen de UT, de Verwerkingsverantwoordelijke, en de Verwerker. Een verwerkersovereenkomst wordt overeengekomen vóór de aanvang van de betreffende Verwerking.

6.9.2 VERWERKING DOOR OF GEZAMENLIJK MET EEN ANDERE VERWERKINGSVERANTWOORDELIJKE

Indien de UT samen met één of meerdere partijen de doelen en middelen voor de Verwerking van Persoonsgegevens bepaalt, dan is er sprake van een gezamenlijke Verwerkingsverantwoordelijkheid en worden afspraken omtrent de zorgvuldige en veilige Verwerking van Persoonsgegevens vastgelegd in een passende overeenkomst, zoals een gezamenlijke Verwerkingsverantwoordelijken overeenkomst. Indien de UT Persoonsgegevens moet aanleveren om gebruik te kunnen maken van diensten van een andere partij, waarbij die partij een zelfstandige verantwoordelijkheid heeft met betrekking tot de Verwerking van die Persoonsgegevens, dan worden de afspraken vastgelegd in een gegevens uitwisselingsovereenkomst.

6.9.3 DOORGIFTE PERSOONSGEGEVENS BINNEN DE EUROPESE ECONOMISCHE RUIMTE

De UT verstrekt Persoonsgegevens alleen aan een ontvanger (Verwerker, Verwerkingsverantwoordelijke of Derde) gevestigd binnen de EER, als de Verwerking is gebaseerd op één van de grondslagen voor gegevensverwerking uit artikel 6 (zie paragraaf 6.2) van de AVG en als de ontvanger voldoet aan de wettelijke vereisten uit de AVG. Wanneer de Verwerking Bijzondere persoonsgegevens bevat gelden moet bovendien worden voldaan aan artikel 9 van de AVG.

6.9.4 DOORGIFTE PERSOONSGEGEVENS BUITEN DE EER

Naast de voorwaarden die gelden voor verstrekking van Persoonsgegevens binnen de EER, hanteert de UT voor verstrekking aan ontvangers buiten de EER de volgende aanvullende voorwaarden:

1. het derde land, gebied, welbepaalde sector in een derde land, of de internationale organisatie in kwestie biedt volgens de Europese Commissie een passend beschermingsniveau.
   Als passend beschermingsniveau hanteert de Universiteit de algemene lijst van landen met passend beschermingsniveau gepubliceerd door de Europese Commissie[14];
2. doorgifte vindt plaats op basis van passende waarborgen uit de AVG, artikel 46 en 47. Daarbij maakt de UT gebruik van de Standard Contractual Clauses zoals vastgesteld door de Europese Commissie en aanvullende beveiligingsmaatregelen, die per voorgenomen doorgifte worden beoordeeld;
3. doorgifte vindt plaats op basis van één van de wettelijke uitzonderingen uit artikel 49 van de AVG.

6.10 INFORMATIEBEVEILIGING

De UT draagt zorg voor een adequaat beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking. Deze maatregelen zijn er mede op gericht onnodige en onrechtmatige verzameling en Verwerking van Persoonsgegevens te voorkomen. De UT heeft een Informatiebeveiligingsbeleid geïmplementeerd waarin maatregelen zijn uitgewerkt die binnen de UT worden gehanteerd[15].

Wanneer Persoonsgegevens worden Verwerkt, wordt een risicoanalyse op privacybescherming en informatiebeveiliging uitgevoerd. Toegang tot Persoonsgegevens wordt gegeven op basis van need-to-know en systemen worden zoveel mogelijk ontworpen en ingericht volgens de principes Privacy by Design en Privacy by Default.

Bij de UT worden alle Persoonsgegevens als vertrouwelijk geclassificeerd. Iedereen behoort de vertrouwelijkheid van Persoonsgegevens te kennen en daarnaar te handelen.

Iedereen die kennisneemt van Persoonsgegevens is verplicht tot geheimhouding hiervan. De geheimhoudingsplicht geldt niet wanneer mededeling van de gegevens wettelijk verplicht is of mededeling noodzakelijk is voor de uitvoering van hun taak.

6.11 RECHTEN VAN BETROKKENEN

De AVG geeft Betrokkenen bepaalde rechten waarmee zij controle kunnen uitoefenen op de Verwerking van hun Persoonsgegevens. Een verzoek kan worden ingediend via een formulier op de privacy website[16].

Voor alle in dit hoofdstuk uitgewerkte rechten van Betrokkenen gelden de volgende punten:

Mededeling aan Betrokkene
De UT draagt er zorg voor dat de informatie en communicatie op een beknopte, toegankelijke en begrijpelijke manier en in duidelijke en eenvoudige taal wordt verstrekt aan Betrokkene. De taal zal worden afgestemd op de doelgroep.

[14] Zie voor deze lijst: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[15] Zie: https://www.utwente.nl/nl/cyber-safety/cybersafety/wetgeving/informatiebeveiligingsbeleid.pdf
[16] Zie: https://www.utwente.nl/nl/cyber-safety/privacy/jouw-privacyrechten/

Termijn
Op een verzoek van een Betrokkene wordt zo spoedig mogelijk, doch uiterlijk binnen één maand na indiening schriftelijk gereageerd. Hierbij zal de Betrokkene in ieder geval in kennis worden gesteld van het gevolg dat aan het verzoek is gegeven. Indien de termijn van één maand redelijkerwijs niet haalbaar is, zal Betrokkene daarvan binnen deze termijn op de hoogte worden gesteld. De UT zal in dat geval binnen twee maanden na het verstrijken van de eerste termijn gevolg geven aan het verzoek van de Betrokkene.

Identiteit Betrokkene
De UT draagt bij het verstrekken van de betreffende informatie zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker. Hiertoe kan de UT om extra informatie verzoeken.

Minderjarigen
Een verzoek tot uitoefening van een van de rechten zoals uitgewerkt in dit hoofdstuk door een Betrokkene die Minderjarig is, onder curatele is gesteld of ten behoeve van wie een bewind of mentorschap is ingesteld, wordt ingediend door diens wettelijk vertegenwoordiger. Een reactie door de UT zal ook naar deze wettelijke vertegenwoordiger worden verstuurd.

6.11.1 RECHT OP INZAGE

Verzoek
Iedere Betrokkene heeft het recht om te informeren of zijn Persoonsgegevens worden Verwerkt en, als dat het geval blijkt, het recht op inzage in hem betreffende Verwerkte Persoonsgegevens. Als de UT veel gegevens van Betrokkene Verwerkt, dan mag de UT de Betrokkene voorafgaand aan de informatieverstrekking verzoeken om te preciseren op welke informatie of welke verwerkingsactiviteiten het verzoek betrekking heeft[17].

Mededeling
Indien Persoonsgegevens worden Verwerkt, bevat de mededeling van de UT een overzicht van de gevraagde gegevens, dit kan mogelijk zijn:
- De Persoonsgegevens zelf;
- De doeleinden van de Verwerking;
- De categorieën van Persoonsgegevens waarop de Verwerking betrekking heeft;
- De ontvangers of categorieën van ontvangers, met name ontvangers in derde landen of internationale organisaties, indien van toepassing;
- De bewaartermijn van de Persoonsgegevens of de criteria om die termijn te bepalen;
- Of de Persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet de onderliggende logica, alsmede het belang en de verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.
- De rechten van de Betrokkene;
- Het recht van de Betrokkene om een klacht in te dienen bij de AP;
- Indien de Persoonsgegevens niet rechtstreeks van de Betrokkene zijn verkregen: de bron van de Persoonsgegevens.

Kopie
De Betrokkene kan om een kopie van zijn Persoonsgegevens verzoeken. Niet altijd hoeft de UT een kopie te verstrekken[18].
Een kopie dient in een gangbare elektronische vorm te worden verstrekt, tenzij het verzoek op papier is gedaan of de Betrokkene expliciet om een papieren kopie verzoekt.

Kosten
Ieder eerste kopie kan kosteloos worden aangevraagd. Per additionele kopie kan de UT een vergoeding van administratieve kosten in rekening brengen bij de Betrokkene.

[17] Zie o.a. nummer 63 van de considerans van de AVG, rechtbank Amsterdam 20 juni 2019 ECLI:NL:RBAMS:2019:4418, Hof Den Bosch 1 februari 2018 ECLI:GHSHE:2018:363 en rechtbank Noord-Holland 23 mei 2019, ECLI:NL:RBNHO:2019:4283
[18] ECLI:NL:RBMNE:2020:5275

Rechten en vrijheden van anderen
De UT zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen. Dit kan er bijvoorbeeld toe leiden dat bij het verstrekken van inzage in de Persoonsgegevens van Betrokkene, de gegevens die herleidbaar zijn tot anderen worden afgeschermd of weggelakt.

6.11.2 RECHT OP GEGEVENSOVERDRAAGBAARHEID

Gronden voor verzoek
Iedere Betrokkene kan een verzoek indienen bij de UT om zijn gegevens te verkrijgen in een gestructureerde, gangbare en machine leesbare vorm dan wel deze rechtstreeks aan een andere Verwerkingsverantwoordelijke over te laten dragen, zonder daarbij te worden gehinderd door de UT, indien is voldaan aan beide volgende voorwaarden:

1. De Verwerking door de UT berust op de grondslag ‘toestemming’ dan wel ‘uitvoering van een overeenkomst met de Betrokkene’.
2. De Verwerking in kwestie is geheel geautomatiseerd.

Rechten en vrijheden van anderen
De UT zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen.

Verwijderen van gegevens
Indien een Betrokkene zijn recht van gegevensoverdraagbaarheid heeft uitgeoefend in het kader van een Verwerking ter uitvoering van een overeenkomst, mag de UT niet besluiten de gegevens te wissen. Na het verstrijken van de bewaartermijn, dient de UT de gegevens echter alsnog te wissen.

Indien het recht is uitgeoefend in het kader van een Verwerking op grond van toestemming van de Betrokkene, mag de UT wel besluiten om de gegevens te wissen na uitoefenen van het recht.

6.11.3 RECHT OP RECTIFICATIE, AANVULLING, VERWIJDERING OF BEPERKING VAN DE VERWERKING

Verzoek tot rectificatie, aanvulling, verwijdering of beperking
Iedere Betrokkene kan met betrekking tot over hem opgenomen Persoonsgegevens bij de UT van deze gegevens verzoeken die te corrigeren, aan te vullen, te verwijderen of de Verwerking te beperken.

Kennisgeving
Indien blijkt dat de Verwerkte Persoonsgegevens van de Betrokkene feitelijk onjuist zijn, voor het doel of doeleinden van de Verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn Verwerkt, zal de gegevensbeheerder (dat kan zowel de Verwerkingsverantwoordelijke als de Verwerker zijn) deze gegevens verbeteren, permanent verwijderen, aanvullen dan wel beperken.

Bovendien worden Derden aan wie de gegevens, voorafgaand aan de rectificatie, aanvulling, verwijdering dan wel beperking, zijn verstrekt hiervan in kennis gesteld, tenzij dit redelijkerwijs niet mogelijk of gezien de omstandigheden niet relevant is. De verzoeker mag opgave verzoeken van degene aan wie de UT deze mededeling heeft gedaan.

Termijn voor uitvoering
De Verwerkingsverantwoordelijke zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

6.11.4 RECHT VAN BEZWAAR

Gronden voor bezwaar
Voor Betrokkenen bestaan er twee gronden om bezwaar te maken tegen een Verwerking:

1. In verband met zijn of haar persoonlijke omstandigheden, mag iedere Betrokkene bezwaar maken tegen Verwerking bij de UT, als deze Verwerking plaatsvindt op grond van

a. de vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag van de Verwerkingsverantwoordelijke, of
b. de behartiging van het gerechtvaardigd belang van de UT of van een Derde aan wie de gegevens worden verstrekt.

De UT zal bij bezwaar de Verwerking in beginsel staken. Indien de UT kan aantonen dat haar dwingende gerechtvaardigde belangen zwaarder wegen dan de belangen of grondrechten en de fundamentele vrijheden van de Betrokkene, zal de Verwerking worden voortgezet. Indien het bezwaar gerechtvaardigd is, treft de UT (kosteloos) maatregelen die nodig zijn om de Persoonsgegevens voor de betreffende doeleinden niet meer te Verwerken.

2. Bij een Verwerking met het doel 'direct marketing', heeft een Betrokkene te allen tijde het recht om bezwaar te maken. De UT zal bij bezwaar de Verwerking voor direct marketing doeleinden direct staken en gestaakt houden.

6.11.5 GEAUTOMATISEERDE BESLUITVORMING

Gronden
Betrokkenen hebben het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde Verwerking gebaseerd besluit, waaraan voor hem rechtsgevolgen zijn verbonden. Onder een 'besluit gebaseerd op een geautomatiseerde Verwerking' wordt verstaan een besluit dat is gemaakt zonder menselijke tussenkomst. Hieronder valt onder andere Profilering.

Slechts in de volgende drie situaties mag de UT besluiten nemen op grond van geautomatiseerde Verwerking:

1. Indien het besluit noodzakelijk is bij de sluiting of uitvoering van een overeenkomst met de Betrokkene;
2. Indien het besluit is toegestaan bij een Europese of nationale wet, mits deze wet voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de Betrokkene;
3. Indien het besluit berust op uitdrukkelijke toestemming van de Betrokkene. Deze toestemming kan te allen tijde worden ingetrokken.

In alle hierboven beschreven situaties, zal de UT passende maatregelen nemen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de Betrokkene. Hieronder zullen tenminste vallen het recht op menselijke tussenkomst door de UT, het recht van de Betrokkene om zijn standpunt kenbaar te maken, alsmede het recht om het besluit aan te vechten. Minderjarigen zullen nooit worden onderworpen aan geautomatiseerde besluitvorming.

6.11.6 RECHTSBESCHERMING

Algemene klachten
Indien de Betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit Beleid jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij de UT. Vragen of klachten in verband met (de Verwerking van) Persoonsgegevens kunnen gemeld worden bij de FG (fg@utwente.nl).

Overige bezwaarmogelijkheden
Naast de algemene interne klachtenprocedure, heeft de Betrokkene de volgende mogelijkheden als hij het idee heeft dat de UT een hem rakende overtreding van de AVG heeft begaan:

A. <u>Verzoekschriftprocedure bij de rechtbank</u>

Indien de UT afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 6.12 van dit Beleid, of de UT heeft het verzoek van de Betrokkene afgewezen, dan wel naar de opvatting van de Betrokkene onvoldoende beantwoord, dan heeft de Betrokkene op grond van artikel 35 lid 2 UAVG de mogelijkheid een verzoekschriftprocedure te starten bij de rechtbank.

Het verzoekschrift dient binnen zes weken na ontvangst van het antwoord van de UT ingediend te worden bij de rechtbank. Indien de UT niet binnen de gestelde termijn heeft geantwoord op het

verzoek van Betrokkene, moet het verzoekschrift binnen zes weken na afloop van die termijn worden ingediend. Indiening van het verzoekschrift hoeft niet door een advocaat te geschieden.

B. <u>Verzoek tot handhaving bij de AP</u>

Indien de UT afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 6.12 van dit Beleid, of de UT heeft het verzoek van de Betrokkene afgewezen, heeft de Betrokkene de mogelijkheid om een klacht in te dienen bij de AP, dan wel om een belangenorganisatie namens hem op te laten treden.

6.12 VERANTWOORDINGSPLICHT

De UT heeft meerdere maatregelen getroffen om aan te tonen te voldoen aan de wettelijke eisen uit de AVG, waaronder implementatie van het onderhavige Beleid.

6.12.1.1 VERWERKINGSREGISTER

De intern verantwoordelijke van de UT zorgt ervoor dat iedere (geheel of gedeeltelijk geautomatiseerde) Verwerking van Persoonsgegevens wordt opgenomen in het verwerkingsregister. De verantwoordelijke dient hiervoor contact op te nemen met de betrokken PCP of de FG. De registratie valt onder het toezicht van de FG. De FG beoordeelt de rechtsgeldigheid van de Verwerking. De FG toetst of de inrichting van het verwerkingsregister voldoet aan de vereisten van artikel 30 AVG en draagt zorg voor de controle en monitoring van de documentatie/ bewijsvoering van de geregistreerde Verwerkingen.

6.12.1.2 DATA PROTECTION IMPACT ASSESSMENTS / DATA TRANSFER IMPACT ASSESSMENTS

Tevens voert de UT een DPIA uit, bij (onderzoeks-)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. De pre-DPIA kan helpen te bepalen of een volledige DPIA nodig is[19]. Indien nodig kan de UT besluiten een DTIA te laten uitvoeren. Bij het opstellen van een DPIA en/of DTIA wordt de FG om advies gevraagd.

[19] Zie: https://www.utwente.nl/nl/cyber-safety/privacy/pre_dpia_formulier/

7 DATALEKKEN

Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van Datalekken of het vermoeden van een Datalek.

7.1 DATALEK

Van een Datalek is sprake als er een inbreuk op de beveiliging van Persoonsgegevens plaatsvindt, die per ongeluk of op onrechtmatige wijze leidt tot enige ongeoorloofde Verwerking daarvan. Het kan hierbij bijvoorbeeld gaan om diefstal van een laptop, een verloren USB-stick, verkeerd uitgegeven autorisatie of een e-mail die naar de verkeerde persoon is verstuurd. Alle Datalekken of vermoedens van Datalekken moeten intern worden gemeld bij CERT-UT: cert@utwente.nl. Sommige Datalekken moeten worden gemeld bij de AP en in sommige gevallen ook bij de Betrokkene(n). De beoordeling of een melding bij de AP gedaan wordt ligt bij het CvB op advies van de FG. Melding bij de AP dient binnen 72 uur na ontdekking plaats te vinden en wordt gedaan door de FG.

7.2 MELDING EN REGISTRATIE

Een Datalek bij de UT kan binnen de eigen organisatie ontstaan, maar ook bij een door de UT ingeschakelde Verwerker. Ook een ander dan een medewerker, student of Verwerker kan een Datalek signaleren. Iedereen die een (mogelijk) Datalek waarneemt of vermoedt zelf onderdeel te zijn van een Datalek, neemt direct contact op met het meldpunt Datalekken van de UT via cert@utwente.nl.

Een melding van een (mogelijk) Datalek dient direct na ontdekking te worden gedaan, ook als nog niet zeker is of er sprake is van een Datalek of wanneer er nog informatie ontbreekt.

Indien mogelijk, dienen de volgende gegevens te worden doorgegeven bij melding van een (mogelijk) Datalek:

- Wie heeft er gemeld?
- Wat is er gemeld?
- Waar kwam de melding vandaan?
- Om welke data (gegevens) gaat het?
- Hoe heeft het incident plaatsgevonden?
- Welke systemen zijn betrokken bij/geraakt door het incident?
- Wanneer heeft het incident plaatsgevonden?
- Indien de melding is gedaan door een medewerker / student van de UT: wat is er gedaan om het incident op te lossen/in de toekomst te voorkomen?

Elk Datalek en de afhandeling daarvan wordt door de FG bijgehouden in een register.

7.3 AFHANDELING

Indien sprake is van een Datalek, wordt dit afgehandeld zoals beschreven in de procedure voor het afhandelen van Datalekken[20].

De onderliggende inbreuk op de beveiliging wordt conform de geldende procedures door CERT-UT afgehandeld om de kans op herhaling en op de impact te minimaliseren.

7.4 EVALUATIE

Het is van belang om te leren van incidenten. Registratie van incidenten en een periodieke rapportage daarover horen thuis bij een professionele manier van Verwerken van Persoonsgegevens. De rapportage over incidenten met betrekking tot Persoonsgegevens maken daarom een vast onderdeel uit van de privacy rapportage.

[20] Zie: www.utwente.nl/nl/cyber-safety/meld-incidenten/procedure-voor-het-afhandelen-van-datalekken.pdf.

8 TOT SLOT

Het Beleid wordt jaarlijks gereviewd en indien nodig geactualiseerd.

Het Beleid is geschreven in Nederlands en er is een Engelse vertaling. Wanneer de interpretatie van deze teksten verschilt, heeft de Nederlandse versie voorrang.

Voor vragen of opmerkingen met betrekking tot dit Beleid kunt u terecht bij de FG.