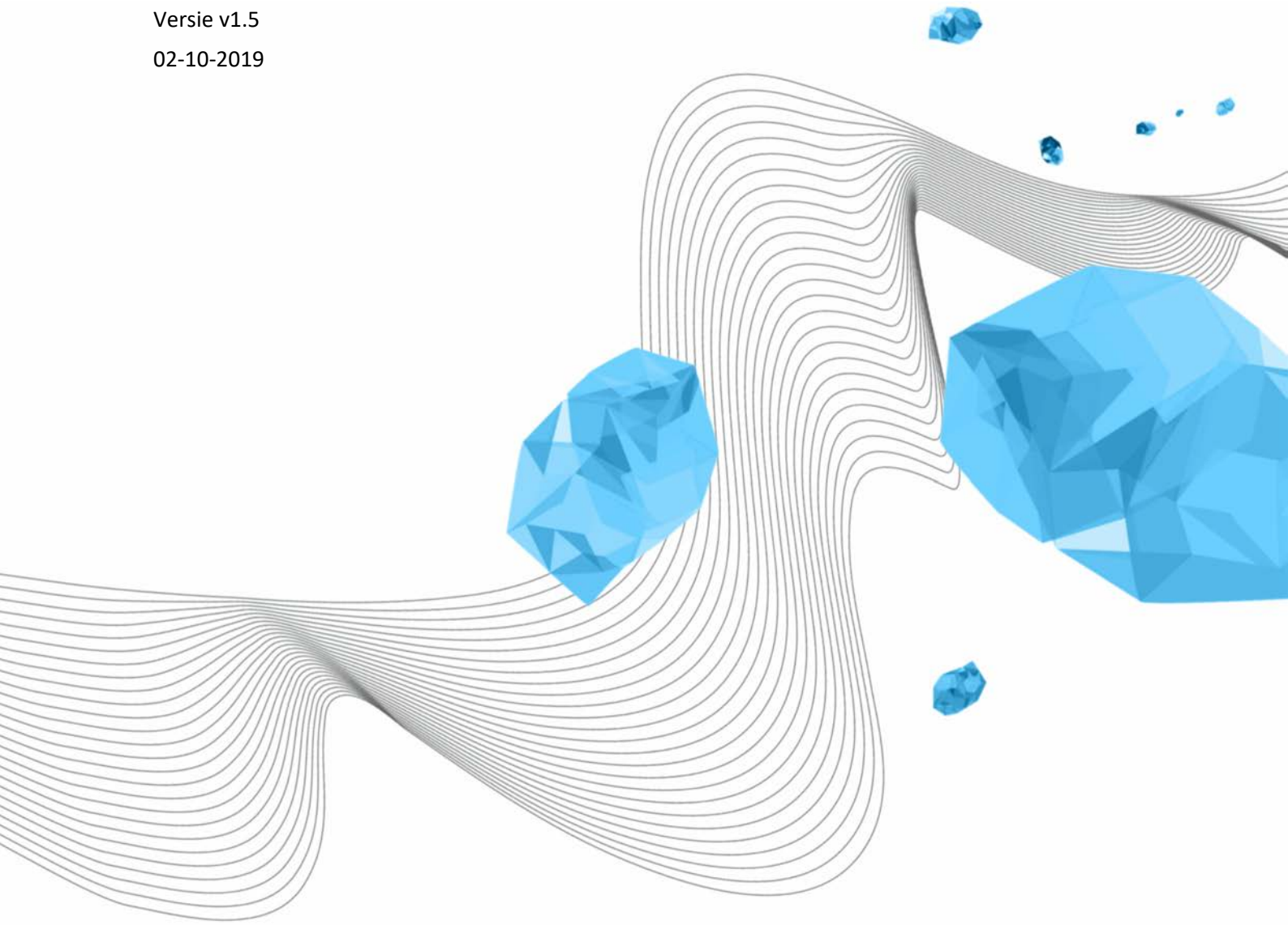
Status: Definitief
Datum vastgesteld in CvB: 14-10-2019
Auteur: Rianne te Brake/Jan Evers

PRIVACYBELEID UNIVERSITEIT TWENTE

LISA

Versie v1.5

02-10-2019



UNIVERSITY OF TWENTE.

COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Privacybeleid Universiteit Twente

KENMERK
UIM/181218/brk

VERSIE (STATUS)
v1.5

DATUM
02-10-2019

AUTEUR(S)
R. te Brake/J.L. Evers

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

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)

INHOUDSOPGAVE

1 INLEIDING

In onze toenemend gedigitaliseerde maatschappij krijgt privacy steeds meer aandacht. Medewerkers en studenten vinden privacy steeds belangrijker. High Tech, Human Touch impliceert aandacht voor privacy bij onderzoek, onderwijs en bedrijfsvoering. Het gebruik van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van instellingen van onderwijs en onderzoek. Opslag en verwerking van deze persoonsgegevens dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en andere betrokkenen. Het College van Bestuur van de Universiteit Twente is wettelijk verantwoordelijk voor het op een juiste manier verwerken van persoonsgegevens.

Met de maatregelen beschreven in dit beleidsdocument neemt de Universiteit Twente 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 gebaseerd op het Model beleid verwerking persoonsgegevens van SURF[1], de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek. Deze publicatie is beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal[2].

Dit privacybeleid is een herziene versie van het Privacybeleid Universiteit Twente van 10 oktober 2016. Naast enkele kleine wijzigingen betreft de herziening voornamelijk het actualiseren van het beleid voor de nieuwe privacywetgeving. De aanpassingen hiervoor volgen het hiervoor genoemde SURF Model en zijn vooral te vinden in hoofdstuk 6 (aanvulling) en hoofdstuk 8 (nieuw).

Definities en afkortingen zijn opgenomen in Bijlage 1.

1.1 REIKWIJDTE EN DOELSTELLING VAN HET PRIVACYBELEID

Het privacybeleid is van belang voor alle medewerkers, studenten en andere relaties van de Universiteit Twente. Het heeft consequenties voor het werk van alle medewerkers en studenten die met persoonsgegevens werken. Het privacybeleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen de Universiteit Twente, waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur/outsourcing), alsmede op andere betrokkenen waarvan de Universiteit Twente persoonsgegevens verwerkt, bijvoorbeeld proefpersonen die deelnemen aan wetenschappelijk onderzoek.

Het privacybeleid betreft niet het verwerken van persoonsgegevens voor persoonlijk of huishoudelijk gebruik, zoals persoonlijke werkaantekeningen of een verzameling visitekaartjes. Het privacybeleid betreft de geheel of gedeeltelijk geautomatiseerde en/of systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de Universiteit Twente alsmede de daaraan ten grondslag liggende (al dan niet elektronische) documenten. Eveneens is het privacybeleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij de Universiteit Twente wordt het beschermen van persoonsgegevens breed geïnterpreteerd. 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 privacybeleid 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 Universiteit Twente.

[1] https://www.surf.nl/files/2019-03/201803-model-beleid-verwerking-persoonsgegevens.pdf
[2] https://creativecommons.org/licenses/by/4.0/deed.nl

Het privacybeleid geeft studenten, medewerkers en andere betrokkenen inzicht in hoe privacy geregeld is op de Universiteit Twente. Daarnaast helpt het bij het creëren van bewustwording over het belang en de noodzaak van het beschermen van persoonsgegevens.

Het privacybeleid beoogt:

- 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*: de basis voor de beveiliging van persoonsgegevens is ISO 27001[3]. Maatregelen worden genomen op basis van best practices in het hoger onderwijs en op basis van ISO 27002[4]. Het SURF Juridisch Normenkader Cloudservices[5] wordt gehanteerd als best practice voor cloud services en andere outsource contracten.
- Het nemen van *verantwoordelijkheid* door het College van Bestuur: door de uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor de hele Universiteit Twente.
- *Daadkrachtige* implementatie van het privacybeleid 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.

[3] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging
[4] Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging
[5] SURF juridisch Normenkader (Cloud)services, vastgesteld door bestuur Platform ICT & Bedrijfsvoering 3 april 2014 en geüpdate 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 Universiteit Twente om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

- Een verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen zoals genoemd in artikel 6 van de Algemene Verordening Gegevensbescherming (AVG) (‘rechtmatigheid’). Zie paragraaf 6.1 voor een opsomming van de wettelijke grondslagen.
- Persoonsgegevens worden alleen verwerkt op een manier die ten aanzien van de betrokkene behoorlijk en transparant is. Dit houdt in dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Informatie en communicatie hierover moet eenvoudig toegankelijk en begrijpelijk zijn (‘behoorlijkheid en transparantie’).
- Persoonsgegevens worden alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het gaat hier om specifieke en gerechtvaardigde doeleinden, die zijn vastgelegd en omschreven voordat men begint met de verwerking. Persoonsgegevens worden niet verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (‘doelbinding’).
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze. Hierbij wordt de hoeveelheid en het soort gegevens beperkt tot de gegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn (‘minimale gegevensverwerking’).
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn (‘juistheid’).
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen (‘integriteit en vertrouwelijkheid’).
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking. Hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen (‘opslagbeperking’).

3 WET- EN REGELGEVING

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

3.1 WET OP HET HOGER ONDERWIJS EN WETENSCHAPPELIJK ONDERZOEK

De Universiteit Twente 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

De Universiteit Twente heeft de wettelijke vereisten van de AVG geïmplementeerd door middel van het privacybeleid. 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 ARCHIEFWET

De Universiteit Twente 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.

3.4 TELECOMMUNICATIEWET

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

3.5 AUTEURSWET

De Auteurswet beschrijft onder meer dat het publiceren van afbeeldingen, foto’s en video’s niet is toegestaan wanneer een redelijk belang van de betrokkene zich daartegen verzet (portretrecht). De Universiteit Twente past deze regelgeving toe.

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[6] en de IT Security Manager[7] zijn nauw betrokken bij de implementatie van het Privacybeleid. Het zorgvuldig omgaan met persoonsgegevens valt namelijk deels onder de algemene regels rondom informatiebeveiliging[8].

4.2 COLLEGE VAN BESTUUR

Het College van Bestuur (CvB) is de verwerkingsverantwoordelijke en daarmee eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen de Universiteit Twente. Het CvB stelt het beleid, de maatregelen en de procedures rondom verwerkingen vast met dit privacybeleid.

4.3 PORTEFEUILLEHOUDER PRIVACY

De portefeuillehouder privacy is het bestuurslid dat privacy in portefeuille heeft. Hij/zij is namens het CvB eindverantwoordelijk voor beveiliging van persoonsgegevens binnen de Universiteit Twente.

4.4 FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING

De AVG verplicht de Universiteit Twente een interne toezichthouder op de verwerking van persoonsgegevens aan te stellen. Deze toezichthouder wordt de Functionaris voor de Gegevensbescherming (FG) genoemd. De FG houdt binnen de Universiteit Twente toezicht op de toepassing en naleving van de privacywetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

De FG adviseert en informeert de gehele organisatie en de individuele eenheden over hun verplichtingen onder de AVG en ziet toe op de naleving hiervan. De FG draagt zorg voor de voorlichting over verwerking van persoonsgegevens aan medewerkers, studenten en leidinggevenden. De FG bevordert het privacy bewustzijn van medewerkers en studenten, bijvoorbeeld door informatieverstrekking over privacy. Jaarlijks wordt er een privacy jaarverslag opgesteld.

De FG is aanspreekpunt en vraagbaak voor degenen die vragen hebben over de bescherming van persoonsgegevens. Daarnaast beheert de FG het register van meldingen van verwerkingen van persoonsgegevens van de Universiteit en ziet toe op de uitvoering van de Data Protection Impact Assessment (DPIA, gegevensbeschermingseffect beoordeling). De FG is het eerste aanspreekpunt voor de toezichthoudende autoriteit (Autoriteit Persoonsgegevens) en werkt hiermee samen.

De FG vervult de rol van procesmanager van het privacy incident proces. Dat houdt in dat hij/zij de universiteits-brede inrichting van het proces bewaakt en verantwoordelijk is voor de kwaliteitszorg.

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

4.5 SYSTEEMHOUDER

De systeemhouder[9] is ervoor verantwoordelijk dat de applicatie (en bijbehorende ICT-faciliteiten) een goede ondersteuning biedt aan het bedrijfsproces waarvoor deze verantwoordelijk is en voldoet aan het privacybeleid. Dit betekent dat de systeemhouder 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 systeemhouder kan hierin worden ondersteund door de Privacy Contact Persoon (PCP) en de FG.

4.6 DIRECTEUR

De dienstdirecteur of portefeuillehouder bedrijfsvoering (PBV) is verantwoordelijk voor de implementatie van het privacybeleid 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 privacybeleid 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 privacybeleid;
- het privacybewustzijn van zijn/haar medewerkers toereikend te laten zijn;
- toe te zien op de naleving van het privacybeleid door zijn 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 Privacy Contact Persoon (PCP) aanwezig. Voor een universiteits-brede consistente uitvoering van het privacybeleid 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 Data Protection Impact Assessment (DPIA);
- ondersteunen bij het vastleggen van gegevensverwerkingen;
- 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 onderzoeksdata omgaat, in voorkomende gevallen samen met een onderzoeksleider. De hoogleraar of voorzitter van de onderzoeksgroep is eindverantwoordelijke.

[9] Zie verder de notitie 'Houderschap van een instellingssysteem', www.utwente.nl/nl/sb/beleidsterreinen/universitair-informatiemanagement/it-governance/houderschap-van-een-instellingssysteem.pdf.

De privacy-gevoeligheid en de ethische implicaties kunnen gevolgen hebben voor de wijze waarop met de onderzoeksdata 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 Universiteit Twente 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 Universiteit Twente 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 Universiteit Twente. 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 Universiteit.

5 IMPLEMENTATIE PRIVACYBELEID

Het College van Bestuur is verantwoordelijk voor verwerkingen van de persoonsgegevens waarvan zij het doel en de middelen voor de verwerking vaststelt. Zij wordt aangemerkt als de *verantwoordelijke* in de zin van de AVG. De feitelijke verwerking van persoonsgegevens wordt echter op allerlei plekken van de universiteit uitgevoerd.

Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term *governance*. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van de Universiteit, zoals de studenten, medewerkers en de samenleving. Een goede governance zorgt er voor dat alle belanghebbenden hun rechten en plichten kennen en er naar handelen.

5.1 VERDELING VAN VERANTWOORDELIJKHEDEN

Het College van Bestuur is eindverantwoordelijk voor alle gegevensverwerkingen van de Universiteit Twente. De verantwoordelijkheden worden in de lijn belegd, waarbij iedere medewerker overeenkomstig zijn rol een eigen verantwoordelijkheid heeft (zie hoofdstuk 4).

Privacy 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 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, binnen de grenzen van het redelijke.

Privacy is *ieders verantwoordelijkheid*. Van medewerkers, studenten, docenten en derden wordt verwacht dat ze zich integer gedragen en zorgvuldig omgaan met persoonsgegevens. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd[10].

5.2 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, FG, PCP, CERT-UT, werkoverleggen).

5.3 BEWUSTWORDING EN TRAINING

Beleid en 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 goed gedrag wordt aangemoedigd. Good practices kunnen worden gedeeld met anderen in de organisatie, bijvoorbeeld via de Cybersafety-website van de Universiteit Twente.

Onderdeel van de uitvoering van het privacybeleid 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 en de Security Managers.

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

5.4 CONTROLE EN NALEVING

De FG houdt toezicht op de naleving van de privacywetgeving en het privacybeleid, inclusief de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van personeel. Aanvullend hierop maken audits het mogelijk het privacybeleid 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 Universiteit Twente.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekort schieten, dan kan de Universiteit Twente de betrokken verantwoordelijke 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 Universiteit Twente 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 Universiteit verwerkt persoonsgegevens in overeenstemming met de principes zoals uitgewerkt in paragraaf 2.1 van dit beleid. Ter uitwerking van deze principes treft de Universiteit de in dit hoofdstuk genoemde maatregelen.

6.1 GRONDSLAG

De Universiteit Twente verwerkt slechts persoonsgegevens als er sprake is van één van de wettelijke gronden 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.

De verantwoordelijke omschrijft vooraf de doeleinden voor de verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. Persoonsgegevens worden niet verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

6.2 PRIVACYVERKLARING

De Universiteit verwerkt persoonsgegevens op een manier die ten aanzien van de betrokkene behoorlijk en transparant is. Dit houdt in dat de Universiteit aan de betrokkene inzichtelijk maakt in hoeverre en op welke manier diens persoonsgegevens verwerkt worden. Bij het verzamelen van de persoonsgegevens zal de Universiteit middels een privacyverklaring de betrokkene inlichten. De Universiteit Twente heeft hiervoor op haar website een algemeen privacy statement gepubliceerd. Voor specifieke situaties worden zo nodig aanvullende verklaringen opgesteld.

Het informeren van betrokkenen vindt plaats voorafgaand aan de verwerking, tenzij dit redelijkerwijs niet mogelijk is. Zie hiervoor ook paragraaf 8.1 van dit beleid.

6.3 BEWAARTERMIJNEN

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij worden verzameld of gebruikt. Persoonsgegevens dienen na het verlopen van de bewaartermijn[11] buiten het bereik van de actieve administratie gebracht te worden. De Universiteit Twente zal de persoonsgegevens na het verlopen van de bewaartermijn vernietigen of, indien de persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren.

6.4 PASSENDE BEVEILIGINGSMAATREGELEN

De Universiteit draagt zorg voor een adequaat beveiligingsniveau en neemt passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zijn er mede op gericht onnodige of onrechtmatige verzameling en verwerking van persoonsgegevens te voorkomen.

[11] Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of formele studieresultaten, maar kunnen ook zijn vastgelegd door de Universiteit Twente, b.v. in een overeenkomst tussen de Universiteit en de betrokkenen.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van de Universiteit.

6.5 DOCUMENTATIEPLICHT

De Universiteit heeft meerdere maatregelen getroffen om aantoonbaar te voldoen aan de wettelijke eisen uit de AVG, waaronder implementatie van dit privacybeleid.

Daarnaast dient elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens gemeld te worden bij de FG. De FG beoordeelt de rechtsgeldigheid van de verwerking en draagt zorg voor adequate documentatie van alle relevante gegevens.

Tevens voert de Universiteit zo nodig een Data Protection Impact Assessment uit. Dit dient tenminste plaats te vinden bij (onderzoeks)projecten, infrastructurele wijzigingen of aanschaf van nieuwe systemen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. Als uit de DPIA blijkt dat de verwerking een hoog risico oplevert en de Universiteit kan geen maatregelen nemen om dit risico te beperken, dan raadpleegt de Universiteit de toezichthoudende autoriteit voorafgaand aan de verwerking.

6.6 PRIVACY BY DESIGN EN PRIVACY BY DEFAULT

De Universiteit hanteert bij de implementatie van iedere verwerking de principes ‘Privacy by Design’ en ‘Privacy by Default’. 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. 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.

6.7 GEHEIMHOUDING

Bij de Universiteit worden alle persoonsgegevens als vertrouwelijk geclassificeerd. Iedereen is bekend met de vertrouwelijkheid van persoonsgegevens en handelt daarnaar.

Iedereen die kennisneemt van persoonsgegevens is verplicht tot geheimhouding hiervan, ook degenen die niet vallen onder een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift. De geheimhoudingsplicht geldt niet wanneer enig wettelijk voorschrift hen tot mededeling verplicht of de noodzaak tot mededeling voortvloeit uit hun taak.

6.8 BIJZONDERE PERSOONSGEGEVENS

Het verwerken van bijzondere persoonsgegevens is in beginsel verboden, tenzij er sprake is van één van de wettelijke uitzonderingen uit de AVG. Mogelijke uitzonderingen zijn onder meer ‘uitdrukkelijke toestemming van de betrokkene’ en ‘zwaarwegend algemeen belang’. Bovendien gelden zwaardere eisen voor de beveiliging van deze bijzondere persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

Onder bijzondere persoonsgegevens vallen de volgende gegevens:

- gegevens waaruit ras of etnische afkomst blijkt;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- gegevens waaruit lidmaatschap van een vakbond blijkt;
- genetische gegevens met het oog op de unieke identificatie van een persoon;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Voor twee soorten persoonsgegevens geldt dat zij niet onder de categorie bijzondere persoonsgegevens vallen, maar dat de verwerking en beveiliging ervan wel aan strenge eisen zijn gebonden:

a. verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten mag slechts onder toezicht van de overheid of binnen Europese of nationale wetgeving;
b. onder de Nederlandse wetgeving mag een nationaal identificatienummer (het BSN of het onderwijsnummer) alleen worden verwerkt als dat wettelijk is bepaald.

6.9 DOORGIFTE PERSOONSGEGEVENS AAN DERDEN

6.9.1 UITBESTEDEN VAN VERWERKING AAN EEN VERWERKER

Indien de Universiteit Twente persoonsgegevens laat verwerken door een verwerker, wordt de uitvoering van verwerkingen geregeld in een schriftelijke overeenkomst tussen de Universiteit Twente, de verantwoordelijke, en de verwerker.

6.9.2 DOORGIFTE PERSOONSGEGEVENS BINNEN DE EUROPESE ECONOMISCHE RUIMTE (EER)

De Universiteit verstrekt persoonsgegevens alleen aan een verwerker gevestigd binnen de EER, als de verwerking is gebaseerd op één van de grondslagen voor gegevensverwerking uit artikel 6 (zie paragraaf 6.1) van de AVG en als de verwerker voldoet aan de wettelijke vereisten uit de AVG. Wanneer de verwerking bijzondere persoonsgegevens bevat gelden hierbij ook de regels uit artikel 9 van de AVG.

6.9.3 DOORGIFTE PERSOONSGEGEVENS BUITEN DE EER

De Universiteit verstrekt persoonsgegevens alleen aan verwerkers die zich bevinden in een land buiten de EER, indien aan één van de volgende voorwaarden is voldaan:

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[12];
   - het Privacy Shield voor bedrijven in de Verenigde Staten, gepubliceerd door de Europese Commissie in samenwerking met de US Department of Commerce[13];
2. doorgifte vindt plaats op basis van passende waarborgen uit de AVG, artikel 46 en 47;
3. doorgifte vindt plaats op basis van één van de wettelijke uitzonderingen uit artikel 49 van de AVG.

6.9.4 DERDEN AAN WIE DE UNIVERSITEIT TWENTE PERSOONSGEGEVENS DOORGEEFT

De Universiteit Twente geeft aan onderstaande derden persoonsgegevens door (niet-limitatieve lijst):

- DUO
- Overheidsinstellingen
- Gemeenten
- Belastingdienst
- Stagebedrijven/organisaties
- Studentenwoningcorporaties
- Studieverenigingen
- Studentenverenigingen
- Sportverenigingen
- Cultuurverenigingen

6.10 VRAGEN- EN KLACHTENPROCEDURE

6.10.1 MELDING EN REGISTRATIE

Vragen of klachten in verband met (de verwerking van) persoonsgegevens kunnen gemeld worden bij de Functionaris Gegevensbescherming (fg@utwente.nl). Van vragen of klachten met een (potentieel) significante impact, wordt een register bijgehouden.

Iedereen, waaronder betrokkenen, verwerkers of derden, kan een vraag of klacht melden.

[12] Zie voor deze lijst: http://ec.europa.eu/justice/data-protection/internationaltransfers/adequacy/index_en.htm.
[13] Zie voor deze lijst: www.privacyshield.gov/list.

6.10.2 ZWAKKE PLEKKEN IN DE BEVEILIGING

Iedereen die een zwakke plek waarneemt in systemen of diensten van de Universiteit Twente meldt deze bij CERT-UT[14] (cert@utwente.nl). Van alle meldingen betreffende zwakke plekken in de beveiliging wordt een register bijgehouden.

6.10.3 AFHANDELING

Vragen, klachten en zwakke plekken in de beveiliging worden doorgezet naar de verantwoordelijke afdeling of persoon en vervolgens conform de daarvoor vastgestelde procedures zo snel mogelijk afgehandeld. Als de persoonsgegevens van betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van de Universiteit in gevaar zijn, wordt in ieder geval het College van Bestuur op de hoogte gesteld.

6.10.4 EVALUATIE

Het is van belang om te leren van de feedback die middels de vragen- en klachtenprocedure wordt geleverd. Registratie van significante vragen, klachten en zwakke plekken en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De rapportage hierover maakt daarom een vast onderdeel uit van de jaarrapportage van de FG (privacyjaarverslag).

[14] Computer Emergency Response Team Universiteit Twente

7 DATALEK

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

7.1 DATALEK

Van een datalek is sprake als er een inbreuk op de beveiliging van persoonsgegevens plaatsvindt, die leidt tot enige ongeoorloofde verwerking daarvan. Het kan hierbij bijvoorbeeld gaan om diefstal van een laptop, een in de trein vergeten USB-stick of een e-mail die naar de verkeerde persoon is verstuurd. Datalekken moeten worden gemeld bij de toezichthouder binnen 72 uur nadat de verwerkingsverantwoordelijke kennis heeft genomen van het datalek. In sommige gevallen moet een datalek ook bij de betrokkene(n) worden gemeld.

7.2 MELDING EN REGISTRATIE

Een datalek bij de Universiteit kan binnen de eigen organisatie ontstaan, maar ook bij een door de Universiteit 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 Universiteit via cert@utwente.nl.

Een melding van een (mogelijk) datalek dient zo spoedig mogelijk te worden gedaan. De volgende gegevens dienen doorgegeven te worden bij melding van een 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 Universiteit: wat is er gedaan om het incident op te lossen/in de toekomst te voorkomen?

Elk datalek en de afhandeling daarvan wordt bijgehouden in een register.

7.3 AFHANDELING

Indien sprake is van een datalek wordt dit afgehandeld zoals beschreven in de beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens[15], zodat de melding van het datalek tijdig de juiste personen en zo nodig de toezichthouder en betrokkenen bereikt. De wijze waarop de Universiteit omgaat met de melding en afhandeling van datalekken is beschreven in de procedure voor het afhandelen van datalekken[16].

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 het privacyjaarverslag en daarmee van de PDCA-cyclus.

[15] Beleidsregels meldplicht datalekken Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf.
[16] Zie www.utwente.nl/nl/cyber-safety/meld-incidenten/procedure-voor-het-afhandelen-van-datalekken.pdf.

8 RECHTEN VAN BETROKKENEN

De AVG geeft betrokkenen bepaalde rechten waarmee zij controle kunnen uitoefenen op de verwerking van hun persoonsgegevens. Een verzoek kan schriftelijk worden ingediend bij de Functionaris Gegevensbescherming (fg@utwente.nl).

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

- Melding aan betrokkene
  De Universiteit zorgt dat de informatie en communicatie op een beknopte, toegankelijke en begrijpelijke manier en in duidelijke en eenvoudige taal wordt verstrekt aan betrokkene. Het taalgebruik wordt afgestemd op de doelgroep.
- Termijn
  Op een verzoek van een betrokkene wordt zo spoedig mogelijk na indiening schriftelijk gereageerd, maar uiterlijk binnen vier weken. Hierbij zal de betrokkene in ieder geval worden geïnformeerd over het gevolg dat aan het verzoek is gegeven. Indien de termijn van vier weken redelijkerwijs niet haalbaar is, zal betrokkene daarvan binnen deze termijn op de hoogte worden gesteld. De Universiteit 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 Universiteit zorgt bij het verstrekken van de betreffende informatie voor betrouwbare vaststelling van de identiteit van de verzoeker. Hiertoe kan de Universiteit extra informatie vragen.
- Minderjarigen
  Een verzoek tot uitoefening van één van de rechten zoals beschreven 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 Universiteit zal ook naar deze wettelijke vertegenwoordiger worden verstuurd.

8.1 RECHT OP INFORMATIE

De betrokkene heeft het recht om door de Universiteit te worden geïnformeerd over bepaalde aspecten van de verwerking van zijn persoonsgegevens. De Universiteit informeert de betrokkene kosteloos 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.

a. Verkrijging direct van betrokkene

   De Universiteit verstrekt de betrokkene voorafgaand aan de verzameling van de gegevens tenminste de volgende informatie:

   - De contactgegevens van de verwerkingsverantwoordelijke en de FG.
   - De specifieke doeleinden van verwerking waarvoor de persoonsgegevens zijn bestemd en de grondslag voor de verwerking.
   - De gerechtvaardigde belangen van de verwerkingsverantwoordelijke of derde als de verwerking is gebaseerd op de grondslag ‘gerechtvaardigd belang’.
   - In voorkomend geval, het voornemen van de verwerkingsverantwoordelijke om de persoonsgegevens door te geven aan een derde land, welk land dit is en op welke grond de persoonsgegevens daarnaartoe worden verstuurd.
   - De periode gedurende welke de persoonsgegevens worden opgeslagen, of indien niet mogelijk, de criteria die dienen om deze termijnen te bepalen.
   - Het bestaan van het recht om de verwerkingsverantwoordelijke te verzoeken om inzage, rectificatie of wissen van de persoonsgegevens, beperking van de hem betreffende verwerking, alsmede het recht tegen de verwerking bezwaar te maken en het recht op dataportabiliteit.
   - Het recht om een klacht in te dienen bij de toezichthoudende autoriteit.
   - De ontvangers of categorieën van ontvangers van de persoonsgegevens.
   - Indien de verwerking is gebaseerd op de grondslag ‘toestemming’, het recht van de betrokkene om die toestemming te allen tijde in te trekken.
   - Of de persoonsgegevens nodig zijn voor de uitvoering van een overeenkomst of om te voldoen aan een wettelijke verplichting.

- Of de persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet dan de onderliggende logica, alsmede het belang en de te verwachte gevolgen van de verwerking voor de betrokkene worden gemeld.

b. 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 na verkrijging van de gegevens worden verstrekt, maar niet later dan vier weken, dan wel bij het eerste contact met de betrokkene.

8.2 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.
- Mededeling
  Indien gegevens worden verwerkt, bevat de mededeling van de Universiteit een volledig overzicht van de volgende gegevens:
  - Een omschrijving van de doeleinden van de verwerking
  - De categorieën van gegevens waarop de verwerking betrekking heeft.
  - Categorieën van ontvangers
  - Beschikbare informatie over herkomst van de gegevens.
  - De termijn van bewaring van gegevens of indien dat niet mogelijk is, de criteria om die termijn te bepalen.
  - Het recht van betrokkene om de verwerkingsverantwoordelijke te verzoeken om rectificatie of wissen van gegevens, beperking of bezwaar van verwerking alsmede het recht op dataportabiliteit.
  - Het recht van de betrokkene om een klacht in te dienen bij een toezichthoudende autoriteit.
  - Alle beschikbare informatie over de bron van de gegevens, als de gegevens niet bij de betrokkene zijn verzameld.
  - Of de persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet dan de onderliggende logica, alsmede het belang en de verwachte gevolgen van de verwerking voor de betrokkene worden gemeld.
  - De passende waarborgen die zijn getroffen, indien de gegevens worden doorgegeven aan een derde land.
- Kopie
  De betrokkene kan om een kopie van alle persoonsgegevens verzoeken. Deze 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
  Iedere eerste kopie kan kosteloos worden aangevraagd. Per additionele kopie kan de Universiteit een vergoeding van administratieve kosten in rekening brengen bij de betrokkene.
- Rechten en vrijheden van anderen
  De Universiteit zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen.

8.3 RECHT OP DATAPORTABILITEIT

- Gronden voor verzoek
  Iedere betrokkene kan een verzoek indienen bij de Universiteit om (kosteloos) zijn gegevens te verkrijgen in een gestructureerde, gangbare en machineleesbare vorm dan wel deze rechtstreeks

aan een andere verwerkingsverantwoordelijke over te laten dragen, zonder daarbij te worden gehinderd door de Universiteit, indien is voldaan aan de volgende voorwaarden:

1. de verwerking door de Universiteit 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 Universiteit zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen.

- Verwijderen van gegevens
  Indien een betrokkene zijn recht van dataportabiliteit heeft uitgeoefend in het kader van een verwerking ter uitvoering van een overeenkomst, mag de Universiteit niet besluiten de gegevens te wissen. Na het verstrijken van de bewaartermijn dient de Universiteit 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 Universiteit wel besluiten om de gegevens te wissen na uitoefenen van het recht.

8.4 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 Universiteit verzoeken deze gegevens te corrigeren, aan te vullen, te verwijderen of de verwerking te beperken. Bij het recht op beperking worden de persoonsgegevens tijdelijk afgeschermd en niet meer verwerkt door de Universiteit. De beperking wordt duidelijk in het bestand aangegeven.

- Kennisgeving
  Indien blijkt dat de opgenomen 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 functioneel beheerder als de verwerker zijn) deze gegevens verbeteren, permanent verwijderen, aanvullen dan wel beperken.

  Bovendien worden derden aan wie de gegevens zijn verstrekt, voorafgaand aan de rectificatie, aanvulling, verwijdering dan wel beperking 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 Universiteit deze mededeling heeft gedaan.

- Termijn voor uitvoering
  De gegevensbeheerder zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. De uitvoering hiervan geschiedt kosteloos voor de betrokkene.

8.5 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 door de Universiteit, 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 Universiteit of van een derde aan wie de gegevens worden verstrekt.

     Zie voor een beschrijving van de grondslagen, paragraaf 6.1.
     De Universiteit zal bij bezwaar de verdere verwerking in beginsel staken. Indien de Universiteit kan aantonen dat zijn 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 Universiteit (kosteloos) maatregelen die nodig zijn om de persoonsgegevens niet meer te verwerken voor de betreffende doeleinden.

2. Bij een verwerking met het doel ‘direct marketing’, heeft een betrokkene te allen tijde het recht om bezwaar te maken. De Universiteit zal bij bezwaar de verwerking voor direct marketing doeleinden direct (kosteloos) staken en gestaakt houden.

8.6 GEAUTOMATISEERDE BESLUITVORMING

- Gronden
  Betrokkenen hebben het recht om niet onderworpen te worden aan een besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking en waaraan voor hem rechtsgevolgen zijn verbonden. Onder een ‘besluit gebaseerd op een geautomatiseerde verwerking’ wordt verstaan een besluit dat is gemaakt zonder menselijke tussenkomst, bijvoorbeeld profilering.

  Slechts in de volgende situaties mag de Universiteit 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 Universiteit 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 Universiteit, het recht van de betrokkene om zijn standpunt kenbaar te maken, alsmede het recht om het besluit aan te vechten. Minderjarigen zullen nimmer worden onderworpen aan geautomatiseerde besluitvorming.

8.7 RECHTSBESCHERMING

- Algemene klachten
  Indien de betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit reglement jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij de Universiteit.

- Overige bezwaarmogelijkheden
  Naast de algemene interne klachtenprocedure, heeft de betrokkene die van mening is dat de Universiteit een hem rakende overtreding van de AVG heeft begaan, de volgende mogelijkheden.

  a. Verzoekschriftprocedure bij de kantonrechter
     Indien de Universiteit een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit beleid heeft afgewezen, kan de betrokkene een verzoekschriftprocedure starten bij de kantonrechter.

     Het verzoekschrift dient binnen zes weken na ontvangst van het antwoord van de Universiteit te worden ingediend bij de kantonrechter. Indien de Universiteit 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 worden gedaan.

  b. Bezwaar en beroep
     Indien de Universiteit een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit beleid heeft afgewezen en het besluit van de Universiteit is aan te merken als een besluit van een bestuursorgaan in de zin van artikel 6 lid 4 van de Algemene wet bestuursrecht (Awb), heeft de betrokkene de mogelijkheid een bezwaarschriftprocedure te starten. Een bezwaarschriftprocedure moet altijd gestart worden binnen zes weken na bekendmaking van een besluit van de Universiteit. Tegen de beslissing op bezwaar, staat beroep open bij de rechtbank.

  c. Verzoek tot handhaving bij toezichthoudende autoriteit
     Indien de Universiteit een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit beleid heeft afgewezen, heeft de betrokkene de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit, dan wel om een belangenorganisatie namens hem op te laten treden.

9 TOT SLOT

Het privacybeleid wordt na twee jaar geëvalueerd, daarbij wordt ook een controle op de effectiviteit van de maatregelen opgenomen.

Voor vragen of opmerkingen met betrekking tot dit beleid kunt u terecht bij de Functionaris Gegevensbescherming.

BIJLAGEN

1. DEFINITIES EN AFKORTINGEN

AVG: Algemene Verordening Gegevensbescherming.

Beleid: dit beleid met betrekking tot het verwerken van persoonsgegevens door de Universiteit Twente.

Betrokkene: een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon.

Verwerking: elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke: College van Bestuur van de Universiteit Twente die het doel en de middelen van de verwerking van persoonsgegevens vaststelt.

Verwerker: een door de Universiteit Twente ingeschakelde (derde) partij die ten behoeve van de Universiteit Twente, en op basis van diens schriftelijke instructies, persoonsgegevens verwerkt.

Derde: ieder ander, niet zijnde de betrokkene, de verwerkingsverantwoordelijke of de verwerker, of enig persoon die onder rechtstreeks gezag valt van de verwerkingsverantwoordelijke of de verwerker en gemachtigd is om persoonsgegevens te verwerken.

Datalek: een inbreuk op de beveiliging van persoonsgegevens, die leidt tot enige ongeoorloofde verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke datalekken onder.

Data Protection Impact Assessment (DPIA, gegevensbeschermingseffect beoordeling): een beoordeling die helpt bij het identificeren van privacy risico's en de handvatten levert om deze risico's te verkleinen tot een acceptabel niveau.

Minderjarige: iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt.

Privacy by Default: gegevensbescherming door standaardinstellingen. Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt.

Privacy by Design: gegevensbescherming door ontwerp. Het beheren van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij mechanismen zo zijn ontworpen dat zij zo veel mogelijk rekening houden met de privacy van betrokkenen. Hierbij wordt stelselmatig aandacht besteed aan allesomvattende waarborgen met betrekking tot nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.

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.

EER: Europese Economische Ruimte.

PDCA: Plan, Do, Check, Act. Verbetercyclus.

CERT-UT: Computer Emergency Response Team Universiteit Twente.

CFM: Campus Facility Management.

CvB: College van Bestuur.

FG: Functionaris voor de Gegevensbescherming.

LISA: Library, ICT Services and Archive

M&C: Marketing en Communicatie

PBV: Portefeuillehouder Bedrijfsvoering van een faculteit.

PCP: Privacy Contact Persoon van een dienst of faculteit.

UCB: Universitaire Commissie Bedrijfsvoering.

UT: Universiteit Twente.

2. VOORBEELDEN VAN DATALEKKEN

Voorbeelden van datalekken zijn:

- een kwijtgeraakte onversleutelde USB-stick met persoonsgegevens;
- een verloren of gestolen onversleutelde telefoon, laptop of tablet (privé of zakelijk) met persoonsgegevens of toegang tot een UT-account met persoonsgegevens;
- uitgeprinte documenten met persoonsgegevens die onbeheerd bij een printer liggen;
- anonieme enquêteresultaten die toch herleidbaar blijken te zijn tot respondenten;
- toegang tot persoonsgegevens waar je geen toegang toe zou moeten hebben;
- inbraak in een computer met persoonsgegevens of toegang tot een UT-account met persoonsgegevens door een hacker;
- rondsturen van een overzicht met namen, s-nr's en/of studieresultaten van studenten;
- rondsturen van een overzicht met namen, telefoonnummers en woonadressen van medewerkers;
- onbevoegden die camerabeelden kunnen inzien.

Voorbeelden van andere privacy incidenten zijn:

- gegevensverzameling die niet is gemeld bij de FG;
- onveilige werkwijze die makkelijk kan leiden tot datalekken;
- gegevensverzameling op grond van toestemming van betrokkene zonder dat die toestemming daadwerkelijk gevraagd of geregistreerd wordt.