Universitair Informatiemanagement

UNIVERSITEIT TWENTE.

Kenmerk: SB/UIM/15/0901/khv
Datum: 10 oktober 2016

Status: Definitief
Datum vastgesteld in CvB: 17-10-2016
Auteur: Wim Koolhoven/Jan Evers

Privacybeleid Universiteit Twente

Het Privacybeleid van de Universiteit Twente is conform het Model Beleid Verwerking Persoonsgegevens in het Hoger Onderwijs. Dit model is opgesteld door de SURF Projectgroep 'Voorbereiding Implementatie Algemene Verordening Gegevensbescherming' en SURFibo[1] en gepubliceerd onder de Creative Commons[2] licentie.

Daar waar substantiële voor de Universiteit Twente specifieke toevoegingen zijn aangebracht, is de tekst grijs weergegeven en waar nodig toegelicht.

[1] Informatiebeveiligers en privacy officers werkzaam in het hoger onderwijs overleggen in SCIPR (SURF Community voor Informatiebeveiliging en PRivacy, voorheen SURFibo). Het doel is de informatie-beveiliging en privacy bij hogescholen en universiteiten te verbeteren. Dit doet SCIPR o.a. door het ontwikkelen van beleid en leidraden.
[2] zie http://creativecommons.org/licenses/by/3.0/nl/

Privacyverklaring Universiteit Twente

De Universiteit Twente respecteert de persoonlijke levenssfeer van studenten, medewerkers en anderen. Informatie wordt niet langer bewaard dan nodig voor het doel waarvoor deze is verzameld en niet gebruikt voor doelen die hier niet mee verenigbaar zijn. De Universiteit Twente verwerkt persoonsgegevens conform de Wet bescherming persoonsgegevens (Wbp) en de Algemene verordening gegevensbescherming (Avg).

Voor de administratie van onderwijs en bedrijfsvoering worden bijvoorbeeld persoonsgegevens verzameld, zoals naam, e-mailadres, telefoonnummer, woonadres, gegevens over (voor)opleiding, studievoortgang en gegevens die betrekking hebben op overige studenten- en personeelsaangelegenheden. De gegevens worden door de betrokkenen zelf verstrekt, maar kunnen ook afkomstig zijn uit bronsystemen van derden, bijvoorbeeld de Belastingdienst, Studielink, de IND en het ABP.

Via de website worden gegevens verzameld, voornamelijk ten behoeve van de studentenwerving, zoals bijvoorbeeld aanmeldingen voor open dagen of het opvragen van informatie.

De Universiteit Twente verstrekt Persoonsgegevens alleen aan derden op basis van een wettelijke grondslag.

Voor wetenschappelijk onderzoek worden gegevens verzameld in overeenstemming met de VSNU en Federa gedragscodes (Federa is een samenwerkingsverband van onderzoekers in de gezondheidszorg), waar nodig na toetsing door de facultaire ethische commissie indien aanwezig en melding bij de functionaris voor de gegevensbescherming (FG).

Bij de verwerking van persoonsgegevens in bedrijfsvoering, onderzoek en administratie van onderwijs gaat de Universiteit Twente uit van het proportionaliteitsprincipe: de verwerking van persoonsgegevens moet proportioneel zijn aan het beoogde bedrijfsvoering- of onderzoeksdoel. Er wordt een goede afweging gemaakt om het juiste evenwicht te vinden tussen privacy en onderzoeksdoelstelling.

Persoonsgegevens worden adequaat beveiligd en zo zorgvuldig als mogelijk behandeld. Er is aandacht voor privacy binnen alle processen en activiteiten. Daartoe zijn bij alle diensten en faculteiten privacycontactpersonen (PCP’s) aangesteld die regelmatig overleg hebben met de FG.

Het onderhavige Privacybeleid geeft studenten, medewerkers en andere betrokkenen inzicht in hoe privacy geregeld is op de Universiteit Twente.

Wetenschappers van de Universiteit Twente doen onderzoek naar privacy en aanverwante onderwerpen. Bij de opzet en implementatie van het beleid wordt gebruik gemaakt van deze kennis.

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. De Wet bescherming persoonsgegevens (Wbp) is onlangs uitgebreid met een meldplicht datalekken, en op Europees niveau is recent de Algemene verordening gegevensbescherming (Avg) vastgesteld, als opvolger van de huidige richtlijn waarop de Wbp is gebaseerd. Alle reden voor de Universiteit Twente om een privacybeleid op te stellen.

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.

Definities en afkortingen staan in Bijlage A.

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 en dat persoonsgegevens veilig zijn bij de Universiteit Twente.

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 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 o.b.v. ISO 27002.[4] Het Juridisch Normenkader Cloudservices Hoger Onderwijs[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 in maatregelen te maken 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.

1.2 Totstandkoming

In 2015 heeft de IT-Board tweemaal over Privacy gesproken en richtinggevende uitspraken gedaan voor het opstellen van een Privacybeleid.

In het najaar van 2015 zijn via I-Beraad (houders instellingssystemen), ICT-Kwartaaloverleg (ICT-vertegenwoordigers faculteiten), UCB en ICT-SO (studentenoverleg) deelnemers gezocht voor een werkgroep. Het beleid is met de werkgroep opgesteld op basis van het landelijk model van SURF en de richtinggevende uitspraken van de IT-Board.

Vertegenwoordigers van FB, M&C, LISA, ITC, CTW, IGS, S&B en Student Union hebben meegewerkt in de werkgroep. Daarnaast hebben interviews plaatsgevonden met een aantal wetenschappers en betrokkenen bij ethische commissies. De privacycontactpersonen (PCP's) van de diensten die niet aan de werkgroep deelnamen zijn via het PCP-overleg betrokken. Het concept beleid is extern beoordeeld door Kienhuis-Hoving.

Het beleid is verder aangescherpt in afstemming met de voorzitter van de IT-Board en vervolgens met positief advies van de IT-Board ter vaststelling voorgelegd aan het College van Bestuur.

De vaststelling en publicatie van de Algemene verordening gegevensbescherming (Avg) heeft plaatsgevonden voordat het opstellen van het beleid werd afgerond, zodat het beleid nog getoetst kon worden aan de definitieve versie van de Avg.

[3] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging
[4] Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging
[5] SURF taskforce Cloud, vastgesteld door bestuur Platform ICT & Bedrijfsvoering 3 april 2014, te vinden via https://www.surf.nl/kennis-en-innovatie/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

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 een van de wettelijke grondslagen zoals genoemd in de Wet bescherming persoonsgegevens (Wbp).
- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
- Bij een verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens 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.
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- 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.
- Iedere betrokkene heeft een wettelijk recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke verwerkingen hem betreffende persoonsgegevens, en heeft in bepaalde gevallen het recht van verzet.
- Bij alle registraties die niet strikt noodzakelijk zijn voor een bedrijfsproces zal aan de betrokkene voor zover technisch mogelijk een eenduidige zogenaamde opt-out procedure worden aangeboden.

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 integriteitscodes voor wetenschappelijk onderzoek nageleefd en toegepast.

3.2 Wet Bescherming Persoonsgegevens

De Universiteit Twente heeft de wettelijke vereisten (waaronder het rechtmatig en zorgvuldig verwerken van persoonsgegevens en nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking van data c.q. persoonsgegevens) geïmplementeerd door middel van het Privacybeleid.

3.3 Archiefwet

De Universiteit Twente houdt zich aan de voorschriften ten aanzien van bewaartermijnen, zoals die bijvoorbeeld in de Archiefwet zijn vastgelegd, en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d.

3.4 Telecommunicatiewet

De Telecommunicatiewet beschrijft onder meer aan welke regels cookies op websites dienen te voldoen.

3.5 Auteurswet

De Auteurswet beschrijft onder meer dat het publiceren van afbeeldingen, foto’s en video’s niet toegestaan is wanneer een redelijk belang van de betrokkene zich daartegen verzet. Dit wordt ook wel het portretrecht genoemd.

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 aan functionarissen in de bestaande organisatie toegewezen.

Bij het onderzoek ligt de verantwoordelijkheid bij de onderzoeker, de onderzoeksleider en de betreffende faculteit.

4.1 Overlap met informatiebeveiliging

De Information Security Officer[6] en de Information 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 eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen de Universiteit Twente en stelt het beleid, de maatregelen en de procedures op het gebied van verwerking met dit Privacybeleid vast.

4.3 Portefeuillehouder privacy

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

4.4 Functionaris voor de gegevensbescherming

De Algemene Verordening Gegevensbescherming (Avg) verplicht de Universiteit Twente zelf 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 omtrent het toepassen van de Privacywetgeving. De FG draagt zorg voor de voorlichting over verwerking van persoonsgegevens aan medewerkers, studenten en leidinggevenden. De FG bevordert het privacybewustzijn van medewerkers en studenten, bijvoorbeeld door het onderhouden van een privacyportal op de website van de Universiteit Twente. Jaarlijks wordt er een privacyjaarverslag opgesteld.

De FG is aanspreekpunt en vraagbaak voor degenen die vragen hebben over de bescherming van persoonsgegevens en beheert het register van meldingen van verwerkingen van persoonsgegevens.

De FG heeft de rol van procesmanager van het Privacy Incident proces. Dat houdt in dat hij/zij de universiteitsbrede 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, kenmerk SB/UIM/15/0106/khv, https://www.utwente.nl/uim/informatiebeveiliging/informatiebeveilingsbeleid-ut.pdf

4.5 Systeemhouder

De systeemhouder[9] is er verantwoordelijk voor dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan het bedrijfsproces waar deze verantwoordelijk voor 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 ondersteund worden door de privacycontactpersoon (PCP) en de FG.

4.6 Directeur

De dienstdirecteur of directeur bedrijfsvoering (DBV) is verantwoordelijk voor de implementatie van het Privacybeleid binnen zijn of haar eenheid. De directeur is ook verantwoordelijk voor persoonsgegevens die vanuit zijn/haar eenheid in een instellingssysteem worden ingevoerd.

De directeur 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 Privacycontactpersoon

In samenspraak met de UCB is in 2015 besloten om ter ondersteuning van de taken van de FG een privacycontactpersoon (PCP) per eenheid (faculteit/dienst) aan te wijzen. De PCP onderhoudt het contact met de FG en adviseert de eenheid aangaande privacy. De PCP heeft als taak:

- er voor zorgen dat de gegevensverwerkingen gemeld zijn bij de FG;
- zorgdragen voor bewustwording en training;
- als privacy-vraagbaak te functioneren binnen de eigen eenheid;
- er voor zorgen dat voor alle nieuwe gegevensverwerkingen een Privacy Impact Assessment wordt uitgevoerd;
- het afstemmen met de dienstdirecteur of DBV over privacy-aangelegenheden;
- het namens de eenheid betrokken zijn bij de afhandeling van datalekken en andere incidenten.

De PCP kan hierin ondersteund worden door de FG. Wanneer een faculteit geen PCP benoemt dan vervult de DBV deze rol.

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 informeren en ondersteunen elkaar.

[9] zie verder de notitie "Houderschap van een instellingssysteem", kenmerk SB/UIM/15/2801/EVS, http://www.utwente.nl/uim/it-governance/houderschap-van-een-instellingssysteem.pdf

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. Dit is verder uitgewerkt in het databeleid van de betreffende eenheid of van de Universiteit Twente.[10]

De privacygevoeligheid en de ethische implicaties kunnen gevolgen hebben voor de wijze waarop met de onderzoeksdata moet worden omgegaan en 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.

4.10 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 te realiseren. De Universiteit Twente zal het belang hiervan benadrukken en inzicht vragen in hoe compliancy gerealiseerd is.

Gegevensverwerkingen van gelieerde instellingen kunnen niet gemeld worden bij de FG van de Universiteit Twente, maar dienen, voor zover zij niet binnen het Vrijstellingsbesluit[11] vallen, rechtstreeks bij de Autoriteit Persoonsgegevens (AP) gemeld te worden.

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

[10] Zie https://www.utwente.nl/ub/en/services/MAIN/research-datamanagement/rdm/datapolicy/
[11] Standaardverwerkingen die veel voorkomen waarvan algemeen bekend is dat zij plaatsvinden hoeven onder bepaalde voorwaarden niet gemeld te worden. Zie https://autoriteitpersoonsgegevens.nl/nl/melden/handreiking-vrijstellingsbesluit-wbp

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 Wet bescherming persoonsgegevens. 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 instelling, 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, Rollen en verantwoordelijkheden met betrekking tot Verwerking Persoonsgegevens.

Privacy is *een lijnverantwoordelijkheid***.** Dit betekent dat leidinggevenden de primaire verantwoordelijkheid dragen voor een zorgvuldige verwerking van persoonsgegevens op 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.

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-aspecten (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, securitymanagers, 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 m.b.t. privacy (en security) voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en goed gedrag wordt aangemoedigd. Good practices kunnen gedeeld worden met anderen in de organisatie, bijvoorbeeld via een privacyportal op de 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 Security Officer en de Security Managers.

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 medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Het verwerken van Persoonsgegevens is een continu proces. Technologische en 0rganisatorische 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

6.1 Grondslag, doelbinding en belangenafweging

Het Verwerken van Persoonsgegevens moet gebaseerd zijn op een van de wettelijke gronden zoals beschreven in artikel 8 van de Wet bescherming persoonsgegevens. 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 verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

De Universiteit Twente treft de nodige maatregelen om te zorgen dat Persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden Verwerkt, juist en nauwkeurig zijn.

Bij (onderzoeks)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door een Privacy Impact Assessment (PIA) uit te voeren.

De Universiteit Twente hanteert bij de implementatie de principes “Privacy by Design” en “Privacy by Default”.

6.2 Melden en documenteren van Verwerkingen

Een geheel of gedeeltelijk geautomatiseerde Verwerking van Persoonsgegevens dient gemeld te worden bij de FG van de Universiteit Twente. De FG beoordeelt de rechtsgeldigheid van de registratie en draagt zorg voor adequate documentatie.

De Verwerkingen worden voldoende gedocumenteerd en gepubliceerd op voor de betrokkenen toegankelijke media met vermelding van het doel van de registratieregistraties en de verantwoordelijken.

6.3 De organisatie van de beveiliging

De Universiteit Twente 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 c.q. onrechtmatige verzameling en Verwerking van Persoonsgegevens te voorkomen.

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

6.4 Geheimhouding

Bij de Universiteit Twente worden alle Persoonsgegevens als vertrouwelijk geclassificeerd. Een ieder behoort de vertrouwelijkheid van Persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de Persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

6.5 Bewaartermijnen/ vernietigingstermijnen per soort gegeven

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Persoonsgegevens dienen na het verlopen van de bewaartermijn[12] 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.

6.6 Bijzondere Persoonsgegevens

Het verwerken van bijzondere Persoonsgegevens is in beginsel verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van de Betrokkene of een zwaarwegend algemeen belang. Tevens gelden zwaardere eisen voor de beveiliging van deze Persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

Onder bijzondere Persoonsgegevens vallen gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens.

6.7 Doorgifte Persoonsgegevens aan Derden

6.7.1 Uitbesteden van Verwerking aan een Bewerker

Indien de Universiteit Twente Persoonsgegevens laat verwerken door een *Bewerker*, wordt de uitvoering van Verwerkingen geregeld in een schriftelijke overeenkomst tussen de Universiteit Twente, de Verantwoordelijke, en de Bewerker.

6.7.2 Doorgifte Persoonsgegevens binnen de Europese Unie

De Universiteit Twente verstrekt Persoonsgegevens alleen aan Derden, als deze doorgifte is gebaseerd op een wettelijke grondslag.

Met betrekking tot bijzondere persoonsgegevens worden deze niet aan derden verstrekt zonder expliciete toestemming van de betrokkene.

6.7.3 Doorgifte Persoonsgegevens buiten de Europese Unie (inclusief de EEA)

De Universiteit Twente verstrekt Persoonsgegevens alleen aan Derden die zich bevinden in een land buiten de Europese Unie indien dat land in zijn geheel of dat bedrijf/die instelling specifiek een *passend beschermingsniveau waarborgt*. Voor landen met een passend beschermingsniveau hanteert de Universiteit Twente de lijst van landen gepubliceerd door de Europese Commissie[13].

De Universiteit Twente verstrekt Persoonsgegevens alleen aan landen zonder passend beschermingsniveau op basis van een wettelijke uitzondering zoals genoemd in artikel 77 van de Wbp. Eén van die uitzonderingen is “ondubbelzinnige toestemming”: degene van wie Persoonsgegevens doorgegeven wordt, heeft ondubbelzinnige toestemming gegeven. Een andere wettelijke uitzondering is doorgifte op basis van een modelcontract (zoals opgesteld door de Europese Commissie). Bij wijzigingen van of aanvullingen op het modelcontract is een vergunning van de minister van Veiligheid en Justitie vereist. In alle gevallen is bij doorgifte van Persoonsgegevens aan een land buiten de Europese Unie een melding bij de AP verplicht.

[12] Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of formele studieresultaten, maar kunnen ook zijn vastgelegd door de UT, b.v. in een overeenkomst tussen de UT en de Betrokkenen.
[13] Zie voor deze lijst: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu#wanneer-mag-ik-toch-persoonsgegevens-doorgeven-naar-een-derde-land-zonder-passend-beschermingsniveau-1753

6.7.3.1 Derden aan wie de Universiteit Twente Persoonsgegevens doorgeeft (niet limitatieve lijst)

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

7 Incidenten met betrekking tot Persoonsgegevens

Iedere klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen de Universiteit Twente is een privacy incident. De bekendste vorm van zo'n incident is een datalek[14].

Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van incidenten of het vermoeden van incidenten in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

7.1 Melding en registratie

Medewerkers van de Universiteit Twente zijn verplicht om een (vermoedelijk) 'datalek' en andere privacy incidenten direct te melden. Incidenten worden vanwege de efficiency bij voorkeur gemeld via CERT-UT[15] of de LISA servicedesk. Indien de melder daar de voorkeur aan geeft kan dit ook vertrouwelijk bij de PCP of de FG, deze zullen de naam van de melder vertrouwelijk behandelen. Voorbeelden van datalekken staan in Bijlage C .

Van elk incident en de afhandeling daarvan wordt door CERT-UT een registratie bijgehouden. Meldingen worden vertrouwelijk behandeld. De melder kan er op vertrouwen dat het doen van een melding geen persoonlijke consequenties heeft voor de melder. Een melder dient zolang het incident nog niet is afgehandeld vertrouwelijk met de melding om te gaan en hierover niet te communiceren met betrokkenen of anderen.

7.2 Afhandeling

De afhandeling van incidenten heeft als doel het probleem op te lossen, de schade te beperken en de wetgeving na te leven. Normaliter is de Information Security Manager[16] degene die beoordeelt of er waarschijnlijk sprake is van een datalek. In dat geval worden in ieder geval de FG en de PCP betrokken in de verdere afhandeling. Vaak zal ook de betreffende leidinggevende betrokken worden. De FG is verantwoordelijk voor de afhandeling van privacy incidenten.

Als het incident een datalek betreft dan wordt conform de regels van de AP[17] bepaald of melding aan de AP verplicht is. De melding wordt afgestemd met het CvB. Een melding aan de AP dient onverwijld binnen 72 uur na constatering plaats te vinden.

Wanneer het informeren van betrokkenen verplicht is conform de regels van de AP of anderszins gewenst is, wordt de communicatie in samenspraak met M&C verzorgd. De melder wordt geïnformeerd over de afhandeling van het incident.

7.3 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.

---

[14] Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, spreken we van een datalek.
[15] Computer Emergency Response Team UT. Zie verder het Informatiebeveiligingsbeleid.
[16] De rol van de Information Security Manager is vastgelegd in het Informatiebeveiligingsbeleid
[17] De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). Beleidsregels voor toepassing van artikel 34a van de Wbp.
Zie https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

Bijlage A Definities en afkortingen

AP: Autoriteit Persoonsgegevens.

Avg: Algemene verordening gegevensbescherming. Verordening (EU) 2016/679. De Europese opvolger van de Wbp die vanaf mei 2018 van toepassing is.

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

Bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

CBP: College Bescherming Persoonsgegevens, de oude naam van de AP.

CERT-UT: Computer Emergency Response Team Universiteit Twente, zie het Informatiebeveiligingsbeleid.

CvB: College van Bestuur.

Datalek: Persoonsgegevens die in handen vallen van derden die geen toegang tot die gegevens (mogen) hebben.

DBV: Directeur Bedrijfsvoering van een faculteit.

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

FG: Functionaris voor de Gegevensbescherming.

PCP: Privacycontactpersoon van een dienst of faculteit.

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

PIA: Privacy Impact Assessment.

Privacy by default: Wanneer gebruikers de keuze wordt geboden tussen verschillende opties, dan geeft de standaard instelling de beste privacy garanties.

Privacy by design: Het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij stelselmatig aandacht wordt besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.

Privacy Impact Assessment / Gegevensbeschermingseffectbeoordeling: Een hulpmiddel dat helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau.

UT: Universiteit Twente.

UCB: Universitaire Commissie Bedrijfsvoering

Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Op de Universiteit Twente is het CvB verantwoordelijk, maar dit is gedelegeerd aan de houder van het betreffende informatiesysteem.

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling,

samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Wbp: Wet bescherming persoonsgegevens. Gebaseerd op Richtlijn 95/46/EG.

Bijlage B Voorbeelden van datalekken

Voorbeelden van datalekken zijn:

- een kwijtgeraakte onversleutelde USB-stick met persoonsgegevens;
- een verloren of gestolen onversleutelde telefoon/laptop/tablet (privé of zakelijk) met persoonsgegevens of toegang tot een UT-account met persoonsgegevens;
- uitgeprinte documenten met persoonsgegevens die onbeheerd bij een kopieerapparaat liggen;
- anonieme enquêteresultaten die toch herleidbaar blijken te zijn tot respondenten;
- toegang tot persoonsgegevens die herleidbaar zijn tot natuurlijke personen 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.

Bijlage C Privacyregels

Op deelgebieden zijn specifieke privacyregels noodzakelijk. Medewerkers kunnen zich beperken tot de voor hun relevante privacyregels. Door het formeel vaststellen van deze privacyregels wordt de implementatie toetsbaar.

Voor de volgende deelgebieden zijn specifieke privacyregels vastgesteld:

1. *Inventarisatie van gegevensverwerkingen*
2. *Website en Apps*
3. *Wetenschappelijk onderzoek*
4. *Administratie en Bedrijfsvoering*
5. *Cameratoezicht*
6. *Aandachtspunten Vertrouwelijkheid*

Privacyregels – Inventarisatie Gegevensverwerkingen

Inleiding

In het Privacybeleid wordt aangegeven dat er op deelgebieden specifieke privacyregels noodzakelijk zijn. Een van deze deelgebieden betreft de inventarisatie van gegevensverwerkingen.

Verantwoordelijkheid

1. Gegevensverwerkingen worden volgens artikel 27 Wbp en artikel 30 Avg gemeld bij de FG.
2. De systeemhouder, ondersteund door de PCP, draagt zorg voor deze melding.
3. De FG draagt zorg voor de inventarisatie van de meldingen van de gegevensverwerkingen.

Meldingen

4. Iedere melding bevat tenminste de volgende gegevens:
    - Functionele naam van het systeem;
    - Houder van het systeem;
    - Betrokken externe partijen;
    - Doel van de verwerking;
    - Welke categorieën van persoonsgegevens van welke categorieën van betrokkenen worden vastgelegd;
    - Te hanteren bewaartermijnen, dit kan per soort gegeven verschillen;
    - Welke bijzondere persoonsgegevens[18] worden vastgelegd;
    - Beschrijving van de genomen beveiligingsmaatregelen;
    - Lijst van organisaties aan wie persoonsgegevens worden verstrekt.
5. Bij het doel van de verwerking wordt ook de wettelijke grondslag vermeld:
    - Toestemming van de betrokkene;
    - Uitvoeren van een overeenkomst;
    - Een wettelijke verplichting;
    - Ter vrijwaring van een vitaal belang van de betrokkene;
    - Uitvoering van een publiekrechtelijke taak;
    - Gerechtvaardigd belang van de verantwoordelijk of derde aan wie gegevens zijn verstrekt.
6. De FG draagt zorg voor de kwaliteitscontrole van de meldingen.
7. Informatiesystemen die geen persoonsgegevens gebruiken worden niet gemeld.
8. Verwerkingen die onder het Vrijstellingsbesluit[19] vallen worden ten behoeve van het overzicht toch zoveel mogelijk gemeld bij de FG.

Transparantie

9. Een overzicht van de meldingen wordt door de FG gepubliceerd op de website.

---

[18] De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, vakbondslidmaatschap en strafrechtelijke gegevens is alleen toegestaan onder bepaalde voorwaarden, Wbp paragraaf 2.

[19] Standaardverwerkingen die veel voorkomen waarvan algemeen bekend is dat zij plaatsvinden hoeven onder bepaalde voorwaarden wettelijk gezien niet gemeld te worden. Vrijstellingsbesluit Wbp, *stb*. 2014, 520 (in werking getreden op 7 mei 2001), zie http://wetten.overheid.nl/BWBR0012461 Aangezien de UT wel een overzicht wil hebben van alle verwerkingen is een interne melding wel gewenst.

Privacyregels – Website en Apps

Inleiding

In het Privacybeleid wordt aangegeven dat er op deelgebieden specifieke privacyregels noodzakelijk zijn. Een van deze deelgebieden betreffen de websites en apps van de Universiteit Twente.

Verantwoordelijkheid

1. M&C is verantwoordelijk voor de implementatie van het Privacybeleid op de websites en in apps.
2. Websites op subdomeinen[20] vallen onder de verantwoordelijkheid van de betreffende eenheid of vereniging. M&C geeft hen proactief advies.
3. M&C informeert website-beheerders over de relevante privacyregels wanneer deze met formulieren persoonlijke informatie verzamelen.

Volgen van bezoekers

4. Bezoekers worden alleen gevolgd voor zover daar een goede reden voor is, hierbij wordt het proportionaliteitsprincipe toegepast.
5. Op de websites en in apps wordt duidelijk aangegeven hoe en met welk doel bezoekers gevolgd worden.
6. Op de websites en in apps wordt duidelijk vermeld welke gegevens worden verzameld.
7. Op de websites en in apps wordt duidelijk aangegeven hoe bezoekers de website kunnen bezoeken of de app kunnen gebruiken zonder gevolgd te worden.

Formulieren

8. Formulieren op de websites en in apps vragen niet meer persoonlijke informatie dan nodig is voor het doel waarvoor deze verzameld wordt.
9. Ieder formulier maakt duidelijk voor welk doel of welke doelen de gevraagde informatie gebruikt wordt.
10. Ieder formulier maakt deel uit van een informatiesysteem waarop de Privacyregels – Inventarisatie Gegevensverwerkingen van toepassing zijn.

IP-adressen

11. IP-adressen worden niet gebruikt om bezoekers te volgen.
12. IP-adressen worden gelogd en kunnen gebruikt worden om security-incidenten en/of technische storingen op te lossen.
13. IP-blokken kunnen gebruikt worden voor statistische analyses.

[20] Volgens het Namenbeleid voor websites en e-mailadressen UT https://www.utwente.nl/uim/voor-eindgebruikers/namenbeleid_ict_domeinen_ut.pdf zijn subdomeinen mogelijk, bijvoorbeeld voor verenigingen, projecten en evenementen.

Privacyregels – Wetenschappelijk onderzoek

Inleiding

In het Privacybeleid wordt aangegeven dat er op deelgebieden specifieke privacyregels noodzakelijk zijn. Een van deze deelgebieden betreft het wetenschappelijk onderzoek. Onderzoekers hebben graag een helder overzicht van de voor hen relevante privacyregels, dit overzicht wordt hieronder gegeven. Deze regels gelden ook voor studenten.

Wanneer een faculteit een ethische commissie heeft dan wordt geadviseerd de PCP in het reviewproces te betrekken.

Relevante documenten

1. Iedere onderzoeker die met persoonsgegevens werkt, dient kennis te nemen van de VSNU Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek.[21]
2. Iedere onderzoeker die met medische gegevens werkt, dient kennis te nemen van de Federa Gedragscode Gezondheidsonderzoek.[22]
3. Raadpleeg de website van LISA over Research Data Management.[23]

Aanvang onderzoek

4. Conform het Onderzoeksdatabeleid wordt een datamanagementplan opgesteld.
5. Wanneer identificerende gegevens van personen worden gebruikt wordt conform de Privacyregels – Inventarisatie Gegevensverwerkingen in samenspraak met de PCP een melding gedaan bij de FG.
6. Denk na over het anonimiseren of als dat niet mogelijk is pseudonimiseren van gegevens.[24]
7. Er worden heldere afspraken gemaakt hoe met persoonsgegevens wordt omgegaan. Dit wordt vastgelegd in het datamanagementplan.

Dataopslag

8. Wanneer gebruik wordt gemaakt van externe opslag of andere clouddiensten dan wordt er een bewerkersovereenkomst[25] afgesloten.
9. Bedenk dat persoonsgegevens niet zo maar buiten de EU opgeslagen mogen worden,
10. Voorkom datalekken door zorgvuldig met dataopslag om te gaan.
11. Wanneer vertrouwelijke informatie wordt vervoerd (bijvoorbeeld op een USB-stick of laptop) dan wordt versleuteling toegepast.
12. Wanneer vertrouwelijke informatie aan anderen wordt verstrekt (bijvoorbeeld via een clouddienst of per email) dan wordt versleuteling toegepast.
13. Voor toegang tot een datarepository wordt het Autorisatiebeleid[26] toegepast.

[21] zie http://www.vsnu.nl/code-pers-gegevens.html
[22] zie https://www.federa.org/code-goed-gedrag
[23] zie https://www.utwente.nl/ub/en/services/MAIN/research-datamanagement/
[24] artikel 89 lid 1 Avg: … Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt.
[25] LISA kan hierbij ondersteuning bieden. Zie ook https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html
[26] zie https://www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf

Privacyregels – Administratie en bedrijfsvoering

Inleiding

In het Privacybeleid wordt aangegeven dat er op deelgebieden specifieke privacyregels noodzakelijk zijn. Een van deze deelgebieden betreft de administratie en bedrijfsvoering. De Securityregels – Informatiesystemen welke zijn opgenomen als bijlage in het Informatiebeveiligingsbeleid[27] zijn onverkort van toepassing.

Verantwoordelijkheid

1. De houder[28] of eigenaar van een informatiesysteem is verantwoordelijk voor naleving van de privacyregels.

Verwerving

2. Voor of aan het begin van het project wordt er conform de Classificatierichtlijn Informatie en Informatiesystemen[29] een classificatie uitgevoerd, zodat de resultaten de vereisten voor het informatiesysteem kunnen meebepalen.
3. Bij het gebruik van cloudservices wordt het Juridisch normenkader cloudservices hoger onderwijs[30] van SURF toegepast.
4. Indien persoonsgegevens worden verwerkt dan wordt een Privacy Impact Assessment (PIA) uitgevoerd. De resultaten hiervan worden verwerkt in de business case voor het project. Er wordt getoetst in hoeverre het verwerken van Persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen.
5. Idealiter is de FG bij de uitvoering van de PIA aanwezig/betrokken. In ieder geval wordt het resultaat aan de FG ter toetsing toegestuurd.
6. Indien een externe bewerker wordt ingeschakeld, wordt een bewerkersovereenkomst[31] afgesloten.

Implementatie

7. De principes “Privacy by Design” en “Privacy by Default” worden gehanteerd. Dit betekent o.a. dat vanaf het begin van het ontwerpproces met privacy rekening wordt gehouden en dat dataminimalisatie wordt toegepast.
8. De houder meldt de gegevensverwerking bij de FG voordat het systeem in gebruik wordt genomen.
9. Bewaartermijnen worden vastgelegd, zodat persoonsgegevens niet langer worden bewaard dan noodzakelijk is.
10. Betrokkenen worden door de houder geïnformeerd over de gegevensverwerking.
11. De houder richt een proces in zodat tijdig, binnen vier weken, aan het recht op inzage en het recht op verbetering, aanvulling, verwijdering of afscherming voldaan kan worden
12. Voor testdoeleinden worden in principe geen productiegegevens gebruikt, behalve voor het reproduceren van geconstateerde problemen. Wanneer voor een acceptatietest productiegegevens worden gebruikt, dan dient de autorisatiematrix gelijk te zijn aan die van de productieomgeving.

---

[27] Zie https://www.utwente.nl/uim/informatiebeveiliging/informatiebeveilingsbeleid-ut.pdf
[28] zie ook http://www.utwente.nl/uim/it-governance/houderschap-van-een-instellingssysteem.pdf
[29] zie http://www.utwente.nl/uim/informatiebeveiliging/classificatierichtlijn-ut.pdf
[30] zie https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch-normenkader-cloudservices-hoger-onderwijs.pdf
[31] In het juridisch normenkader van SURF is een model bewerkersovereenkomst opgenomen.

Privacyregels – Cameratoezicht

Inleiding

In het Privacybeleid wordt aangegeven dat er op deelgebieden specifieke privacyregels noodzakelijk zijn. Voor het cameratoezicht op de Universiteit Twente zijn buiten de Privacyregels – Administratie en bedrijfsvoering de hieronder opgenomen regels van toepassing.[32]

Verantwoordelijkheid

1. FB is als houder van het cameratoezicht verantwoordelijk voor het naleven van de privacyregels bij het cameratoezicht op de Universiteit Twente.

Doel en transparantie

2. De gegevens worden uitsluitend gebruikt voor de volgende doeleinden:
   a. Bescherming van de veiligheid en gezondheid van natuurlijke personen;
   b. Beveiliging van de toegang tot gebouwen en terreinen;
   c. Bewaking van zaken die zich in gebouwen of op terreinen bevinden;
   d. Vastleggen van incidenten.
3. Camera's zijn duidelijk zichtbaar opgehangen of er wordt ter plekke, bijvoorbeeld middels stickers, aangegeven dat gebruik wordt gemaakt van camerabewaking.

Toegang

4. De live beelden zijn alleen toegankelijk voor de medewerkers die belast zijn met de beveiliging en bewaking op de Universiteit Twente.
5. Toegang tot opgenomen beelden is alleen mogelijk in een speciaal daartoe ingerichte ruimte.
6. Toegang tot opgenomen beelden hebben alleen het hoofd van de verantwoordelijke afdeling en diens plaatsvervanger.
7. Betreffende medewerkers hebben een geheimhoudingsplicht met betrekking tot gegevens die tot personen herleidbaar zijn.

Opslag

8. Opgenomen camerabeelden worden zo opgeslagen dat deze niet toegankelijk zijn voor anderen.
9. Opgenomen camerabeelden worden niet langer dan twee weken bewaard. Camerabeelden, opgenomen in opdracht van de dienst Beveiliging van de Universiteit Twente, worden maximaal 4 dagen bewaard.

Incidenten

10. Na een incident kan na het constateren dat relevant beeldmateriaal beschikbaar is, besloten worden deze beelden veilig te stellen en zo lang te bewaren als voor het betreffende onderzoek nodig is.

[32] Voor het cameratoezicht door de dienst Beveiliging geeft het Reglement Cameratoezicht Universiteit Twente 2011, https://www.utwente.nl/fb/diensten_abc/per_thema/huisvesting/cameratoezicht.pdf een verdere uitwerking van deze privacyregels.

11. In het geval er sprake is van een redelijk verdenking of vermoeden van een ongeoorloofde handeling kan na schriftelijke opdracht van het College van Bestuur gebruik gemaakt worden van verdekt geplaatste camera's zonder dat betrokkenen hierover worden geïnformeerd.
12. Beelden worden alleen aan derden verstrekt indien het belang van de Universiteit Twente dit vordert na een overeenkomstig besluit door het College van Bestuur. De politie kan de beelden alleen op vordering verkrijgen, of ná toestemming van de (hulp)officier van justitie.

Privacyregels – Aandachtspunten Vertrouwelijkheid

Begin 2015 is door een werkgroep van het I-Beraad, het overleg van houders van instellingssystemen, een notitie “Omgaan met Vertrouwelijkheid” uitgebracht. Deze notitie wil handvatten bieden aan de houders van informatie(systemen) die besluiten moeten nemen omtrent al of niet te nemen maatregelen.

Het belangrijkste onderdeel van deze notitie is een lijst met concrete aandachtspunten, die hieronder bijna ongewijzigd opgenomen wordt. Deze generieke aandachtspunten zullen per gegevensverwerkend proces vertaald moeten worden.

1. *Autorisatie*. Het is van belang zeker te zijn dat alleen die personen toegang hebben tot vertrouwelijke informatie die die gegevens ook nodig hebben. Implementatie van het Autorisatiebeleid[33] kan hiervoor zorgdragen. Attent zijn op het gebruik van een account van een ander, ook bij tijdelijke vervanging zoals bv. bij zwangerschapsverlof.
2. *Authenticatie*. Voorkomen dat iemand zich voor iemand anders kan uitgeven en bij vertrouwelijke informatie kan komen. Voorkom dat medewerkers wachtwoorden delen of opschrijven. Overweeg tweefactorauthenticatie.
3. *Toegang* van elders dan de vaste werkplek. Thuiswerken of werken op een andere locatie kan tot extra risico’s leiden. Dit is te voorkomen door te filteren op IP-adres.
4. *Invoer* van gegevens. Bedenk dat aantekeningen en tijdelijke documenten ook vertrouwelijke informatie kunnen bevatten. Zorg voor gecontroleerde afvoer of vernietiging van dergelijke papieren en bestanden.
5. *Bewerken* en raadplegen van gegevens. Wanneer een medewerker informatie opvraagt of toevoegt, kan vertrouwelijke informatie, als deze niet noodzakelijk is voor de handeling, worden verborgen of achter een extra knop gezet worden.
6. *Onderbreken* van het werk. Denk om het gebruik van screensavers en om het niet zichtbaar laten liggen van vertrouwelijke papieren.
7. *Uitwisselen* gegevens met andere systemen. Wissel niet meer gegevens uit dan noodzakelijk. Wanneer vertrouwelijke informatie wordt verstrekt, wees er dan zeker van dat die gegevens ook vertrouwelijk blijven. Maak duidelijke afspraken vooraf.
8. *Produceren* van rapportages. Per rapport zal bepaald moeten worden welke mate van vertrouwelijkheid er moet gelden. Wanneer bekend is dat een rapport vertrouwelijk is, dan kan dat er standaard op vermeld worden.
9. *Opslaan* van gegevens. Kritiek vertrouwelijke informatie hoort versleuteld opgeslagen te worden. Bij centrale opslag is dat van belang om te voorkomen dat hackers of beheerders toegang hebben. Bij decentrale opslag speelt meer het risico van virussen en diefstal. Papier met kritiek vertrouwelijke informatie, bijvoorbeeld een dossier, dient opgeslagen te worden in een afgesloten kast.
10. *Bewaren* van email. Het bewaren van vertrouwelijke informatie in het emailsysteem betekent dat deze informatie via ieder device, dus ook de telefoon en tablet, langdurig toegankelijk blijft. Denk bijvoorbeeld aan ziektemeldingen, sollicitatiebrieven en functionerings-gesprekken. Verwijder emails met vertrouwelijke informatie zo snel mogelijk.
11. *Archiveren* van informatie. Leg de bewaartermijn en de regels omtrent toegang en vernietiging vast.
12. *Afdrukken* van gegevens. Papier met kritiek vertrouwelijke informatie mag alleen geprint worden als de medewerker er zelf bijstaat, mag niet blijven rondslingeren, mag niet zomaar meegenomen worden en moet na gebruik gecontroleerd afgevoerd of vernietigd worden.
13. *Meenemen* van digitale gegevens. Informatie kan op USB-stick, harde schijf, laptop, etc. meegenomen worden. Bedenk eerst of alle informatie wel nodig is, kan de vertrouwelijke

[33] Autorisatiebeleid Universiteit Twente, kenmerk SB/UIM/13/0819/khv, zie http://www.utwente.nl/uim/informatiebeveiliging/autorisatiebeleid-universiteit-twente.pdf

informatie niet weggelaten worden? Kritiek vertrouwelijke informatie hoort versleuteld opgeslagen te worden.

14. *Raadplegen* van informatie op mobiele apparatuur. Zoals beschreven in de notitie Gebruik van “eigen” apparatuur en applicaties[34] kunnen afhankelijk van de classificatie extra beveiligingsmaatregelen worden getroffen.
15. *Werken* in publieke ruimtes. Andere personen kunnen van scherm of papier meelezen. Voorkom dit bij het raadplegen van vertrouwelijke informatie. Denk hierbij aan gang, kantine, cafés, restaurants, wachtruimtes, trein, vliegtuig, etc.
16. *Bespreken* van informatie. Bedenk bij het bespreken van informatie, ook bij het gebruik van een telefoon, dat anderen mee kunnen luisteren.
17. *Versturen* van informatie. Controleer of de betreffende persoon deze informatie wel nodig heeft, probeer de verstrekte informatie te minimaliseren. Controleer of we als Universiteit Twente deze informatie wel aan betreffende persoon mogen verstrekken. Wanneer vertrouwelijke informatie per email of anderszins digitaal verstuurd wordt, dan dient dit versleuteld te gebeuren.
18. *Audittrail*. Middels een logfile moet na te gaan zijn wie toegang tot welke vertrouwelijke informatie heeft gehad.
19. *Diefstal* van informatie. Wanneer papier met vertrouwelijke informatie of een informatiedrager (USB-stick, tablet, etc.) wordt verloren, welke procedures gelden er dan? Enerzijds minimaliseren verdere schade, door wachtwoord aan te passen etc.. Wat verder te doen wordt verder in de procedure Meldplicht Datalekken uitgewerkt.
20. *Schrijven* van procedures. Neem de rollen van medewerkers op in procedures en niet de namen van individuen.
21. *Uitbreiden* of nieuw ontwerpen/aanschaffen van applicaties. Bedenk vooraf welke beveiligingsaspecten een rol spelen. De Classificatierichtlijn en een PIA kunnen hierbij helpen. Halverwege een project met extra eisen komen zorgt voor hogere kosten.
22. *Testen* van applicaties. Voor het testen van een applicatie wordt vaak met de live-data gewerkt, die is immers realistisch. Maar voor de meeste tests kan de kritiek vertrouwelijke informatie prima weggelaten worden. Dit kan door bepaalde velden in een database met andere informatie te overschrijven of te verhaspelen en geen originele vertrouwelijke documenten te gebruiken.
23. *Uitbesteden* van werk of gebruik van clouddiensten. Maak heldere afspraken en als er persoonsgegevens worden uitgewisseld sluit dan een bewerkersovereenkomst af.

[34] Gebruik van “eigen” apparatuur en applicaties, kenmerk SB/UIM/12/1018/khv, zie http://www.utwente.nl/uim/voor-eindgebruikers/Gebruik_van_eigen_apparatuur_en_applicaties.pdf