Privacybeleid Hogeschool Utrecht

Auteur
Privacymanager
Dienst IM&ICT

Datum
4 juli 2024

Versie
3.2.1

Versiebeheer

Versie	Datum	Auteur	Verwerking
1.0	15 mei 2018	Roos Roodnat	Publicatie op HU.nl
2.0	Maart 2022	Rinske Plomp	Actualisatie privacybeleid
2.1	25 juli 2022	Rinske Plomp (review Eric van den Bos, Annelies de Jeu, Roos Roodnat)	Aanpassing opzet privacybeleid na review : conform opbouw en format IBB
2.2	24 maart 2023	Rinske Plomp	Actualisering adhv wijzigingen beleid na juli 2022
3.0	17 aug 2023	Rinske Plomp (review Roos Roodnat, Marcel van de Kolk, Rene Anker)	Actualisatie n.a.v. aangepast Informatiebeveiligingsbeleid
3.1	14 april 2024	Rinske Plomp (review Roos Roodnat, Han Wouters, Eelko van Leeuwen)	Actualisatie n.a.v nieuwe ontwikkelingen
3.2	12 juni 2024	Roos Roodnat	Bespreekpunten CvB vergadering doorgevoerd
3.2.1	4 juli 2024	Roos Roodnat	Bespreekpunten CvB/HSR doorgevoerd

Distributielijst

Versie	Datum	Ontvanger	Doel
3.0	29 aug 2023	CvB	Doorgeleiden
3.1	11 juni 2024	CvB	Doorgeleiden
3.2	3 juli 2024	HSR	Instemming
3.2.1	9 juli 2024	CvB	Vaststelling

Inhoud

1 Inleiding

Hogeschool Utrecht is een kennisinstelling. Onderwijs, onderzoek en de beroepspraktijk zijn de belangrijkste processen in een hogeschool. Opslag en verwerking van persoonsgegevens is noodzakelijk voor het geven van onderwijs en het doen van onderzoek. Voor studenten, medewerkers en andere betrokkenen bij Hogeschool Utrecht, is het van belang dat dit met de grootste zorgvuldigheid gebeurt. Hogeschool Utrecht hecht dan ook veel waarde aan het beschermen van de persoonsgegevens die aan haar worden verstrekt. Het is de verantwoordelijkheid van elke medewerker en student om daar zorgvuldig mee om te gaan en te voldoen aan de privacywetgeving (Algemene Verordening Gegevensbescherming). Gedrag en deskundigheid op het gebied van privacy bepalen voor een groot deel hoe veilig we omgaan met persoonsgegevens.

Samen met bedrijven en instellingen werken onze studenten, docenten, onderzoekers, medewerkers, management, medezeggenschap en bestuur aan de professionalisering en innovatie van de beroepspraktijk. De grenzen tussen instellingen zijn daarbij steeds minder belangrijk. Dit betekent dat we onszelf verder zullen moeten ontwikkelen tot een open netwerkorganisatie. Dat brengt ook veiligheidsrisico's met zich mee. We hebben tegelijkertijd een maatschappelijke verplichting en morele en wettelijke verantwoordelijkheid om een veilige leer- en werkomgeving te bieden voor alle betrokkenen. In dat spanningsveld vinden wij een doordachte aanpak voor integrale veiligheid belangrijk.

Integrale veiligheid betekent in de HU dat we veiligheid gerelateerde vraagstukken binnen de instelling in samenhang aanpakken en dat we voor alle domeinen op het gebied van integrale veiligheid redeneren vanuit hetzelfde strategisch kader. Die visie geeft ons richting bij de keuzes die we maken t.a.v. de verschillende domeinen van integrale veiligheid op tactisch en operationeel niveau.

De HU onderscheidt verschillende veiligheidsdomeinen: Informatieveiligheid, sociale veiligheid, fysieke veiligheid en crisismanagement. De bescherming van persoonsgegevens valt samen met informatiebeveiliging en kennisveiligheid onder het domein informatieveiligheid. De directeur IM&ICT draagt HU breed de verantwoordelijkheid voor het domein informatieveiligheid.

1.1 Doel privacybeleid

Het privacybeleid van Hogeschool Utrecht heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren. Hierbij moet een goede balans worden gevonden tussen privacy, functionaliteit en veiligheid. De kaders en instrumenten in het beleid geven Hogeschool Utrecht inzicht in haar werkwijze en verhogen daarmee ook de bewustwording van het belang en de noodzaak van het beschermen van persoonsgegevens, onder medewerkers en studenten.

Met het beschrijven van de maatregelen in dit Privacybeleid neemt Hogeschool Utrecht de verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet en -regelgeving (de AVG en de UAVG).

Beleidsinstrumenten en beleid zijn slechts het begin. Om privacy onderdeel te laten zijn van onze dagelijkse werkwijze is er een sterke privacy-organisatie, waarbij elk instituut, kenniscentrum en dienst een eigen privacy-officer heeft. Collega's kunnen bij hen terecht met vragen en advies. Het

belangrijkste is dat zowel medewerkers en studenten zich bewust zijn dat zij met persoonsgegevens werken en weten hoe zij dit zorgvuldig kunnen doen. Hier is steeds opnieuw aandacht voor nodig.

Dit privacybeleid is een aanpassing van het privacybeleid dat in mei 2018, dus bij het van kracht worden van de AVG, is vastgesteld. In dit privacybeleid zijn de processen verder geactualiseerd en is de inrichting van de privacy-organisatie vernieuwd.

Meer specifieke doelstellingen van het privacybeleid zijn:

- Voldoen aan wettelijke vereisten en verantwoording (DPIA, Verwerkingenregister, Verwerkersovereenkomsten)
- Ondersteuning en advies bieden voor betrokkenen om hun rechten uit te oefenen (bijvoorbeeld een inzageverzoek).
- Het bieden van concrete richtlijnen en formats voor zowel de onderwijs als onderzoekspraktijk om zorgvuldig met persoonsgegevens om te gaan (uitgewerkt op operationeel niveau).
- Het vergroten van de awareness onder alle medewerkers en studenten
- Het correct afhandelen van meldingen van een datalek

1.2 Reikwijdte privacybeleid

1.2.1 Privacybeleid Hogeschool Utrecht

Het privacybeleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen waaronder in ieder geval alle medewerkers, studenten, gasten, alumni, studiekiezers, bezoekers, respondenten en externe relaties (inhuur/outsourcing) vallen.

De bescherming van persoonsgegevens is voor Hogeschool Utrecht onderdeel van Integrale Veiligheid en verhoudt zich altijd tot alle veiligheidsdomeinen: informatieveiligheid, sociale veiligheid, gebouwveiligheid integriteit en fysieke beveiliging en crisismanagement. De veiligheidsorganisatie schenkt voortdurend aandacht aan deze raakvlakken en zoekt zowel planmatig als inhoudelijk afstemming.

1.2.2 Derde partijen

De HU heeft contracten met andere organisaties in de vorm van partnerships, deelnemingen, delen van middelen etc. Op basis van risicoanalyse wordt voorafgaand aan de samenwerking vastgesteld aan welke informatiebeveiligingseisen partijen dienen te voldoen om een veilige uitwisseling en/of verwerking van gegevens mogelijk te maken. Deze eisen worden opgenomen in een programma van eisen. De afspraken dienen vervolgens expliciet in het contract te worden vastgelegd, en naleving van deze afspraken dient periodiek geëvalueerd te worden.

Wanneer Hogeschool Utrecht persoonsgegevens laat verwerken door een externe verwerker, dan wordt de uitvoering van verwerkingen geregeld in een verwerkersovereenkomst. Deze verwerkersovereenkomst is onderdeel van het contract dat de HU sluit met de leverancier of samenwerkingspartner. Als er sprake is van een gezamenlijke verantwoordelijkheid voor de verwerking wordt dit ook vastgelegd in een overeenkomst. De HU hanteert daarbij de formats die in gezamenlijkheid met SURF zijn vastgesteld.

De verwerkersovereenkomsten worden geregistreerd in het centrale verwerkingsregister. De monitoring en audit op de afspraken die in de verwerkersovereenkomst zijn vastgelegd, vindt ook vanuit dit register plaats.

Hogeschool Utrecht verstrekt persoonsgegevens alleen aan een Verwerker gevestigd *binnen* de EER, als de verwerking is gebaseerd op een van de grondslagen voor gegevensverwerking uit artikel 6 of artikel 9 AVG en als de Verwerker voldoet aan de wettelijke vereisten uit de AVG:

Hogeschool Utrecht verstrekt persoonsgegevens alleen aan Verwerkers die zich bevinden in een land *buiten* de EER, indien 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 Hogeschool Utrecht:

- De algemene lijst van landen met passend beschermingsniveau gepubliceerd door de Europese Commissie[1.]
- Het Standard Contractual Clause(SCC) voor bedrijven die voorheen onder het Privacy Shield vielen. Het SCC is modulair opgebouwd en kan worden toegepast in verschillende rollen en daarmee ook tussen gezamenlijke verwerkersverantwoordelijken. Doorgifte vindt plaats op basis van passende waarborgen uit de AVG, artikel 46 en 47.
- Doorgifte vindt plaats op basis van een van de wettelijke uitzonderingen uit artikel 49 van de AVG.

1.3 Samenwerking

De AVG is relatief jonge wetgeving. Dit vereist normvinding, kennisontwikkeling en een voortdurend aanscherpen van processen op basis van casuïstiek. De Privacy organisatie kiest er dan ook voor om nauw samen te werken en af te stemmen met de Onderwijs sector. Hiertoe neemt zij actief deel aan de volgende netwerken:

- SURF: SCIPR community
- IVHO: Integraal Veiligheidsoverleg Hoger Onderwijs
- FG netwerk Vereniging Hogescholen
- Netwerk AVG en Onderwijs
- Netwerk Privacymanagers Hogescholen

De formats en richtlijnen die door deze netwerken voor het onderwijs worden ontwikkeld zijn belangrijke vertrekpunten bij implementaties binnen de HU.

2 Uitgangspunten en Beleidsprincipes

2.1 Beleidsuitgangspunten

Algemeen beleidsuitgangspunt is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hogeschool Utrecht houdt zich aan de uitwerking van de AVG en daaraan gerelateerde wetgeving als de UAVG en Archiefwet.

Rechtmatig

[1] Deze kunt u vinden via de volgende link http://ec.europa.eu/justice/data-protection/internationaltransfers/adequacy/index_en.htm.

Hogeschool Utrecht verwerkt slechts persoonsgegevens als er sprake is van een van de grondslagen zoals beschreven in artikel 6 van de AVG:

a) Toestemming van de betrokkene.
b) Noodzakelijk voor de uitvoering van een overeenkomst met de betrokkene.
c) Noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
d) Noodzakelijk om de vitale belangen van de betrokkene of een ander natuurlijk persoon te beschermen.
e) Noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van uitoefening van openbaar gezag.
f) Noodzakelijk voor de behartiging van het gerechtvaardigd belang van de verwerkings-verantwoordelijke of een derde.

Doelbinding

Bij de verwerking dient een goede balans te worden aangebracht tussen het belang van Hogeschool Utrecht om persoonsgegevens te verwerken en het belang van betrokkene. Dit laatste ter eerbiediging van zijn persoonlijke levenssfeer en om in vrijheid eigen keuzes te kunnen maken met betrekking tot zijn persoonsgegevens.

Bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens is in beginsel verboden, tenzij er sprake is van een van de wettelijke uitzonderingen uit de AVG, waar onder meer 'uitdrukkelijke toestemming van de betrokkene' en een 'zwaarwegend algemeen belang' onder vallen, of een specifieke bepaling in de UAVG. Deze bepaling geldt bijvoorbeeld bij het bieden van zorg en begeleiding en het treffen van voorzieningen als de gezondheidstoestand van studenten dit noodzakelijk maakt.

Tevens 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:

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

Dataminimalisatie

Alleen die persoonsgegevens die noodzakelijk zijn voor onze taken, worden verwerkt. Ook geldt dat alleen mensen die de gegevens nodig hebben om hun taken uit te voeren, inzage in de gegevens mogen hebben.

Bewaartermijnen
Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Hogeschool Utrecht 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. Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of bij formele studieresultaten. De selectielijst Hoger Onderwijs dient daarbij als uitgangspunt. Bewaartermijnen kunnen ook zijn vastgelegd in een verwerkersovereenkomst of in een overeenkomst tussen Hogeschool Utrecht en de betrokkenen.

Veilig en betrouwbaar (Privacy by design)
Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen (beschikbaarheid, integriteit en vertrouwelijkheid). Bij de verwerking van persoonsgegevens in projecten en systemen wordt het principe van privacy by design toegepast. Er worden niet meer persoonsgegevens verwerkt dan noodzakelijk en toegang is beperkt tot degene die hier rechten toe hebben.

Transparant
De HU voldoet aan de verplichtingen vanuit de AVG als het gaat om verantwoording en transparantie, zoals het bijhouden van verwerkingenregister, het opstellen van privacyverklaringen en het uitoefenen van rechten van betrokkenen. Alle informatie is te vinden op de pagina Weten&Regelen, Privacy en Security op EEN HU en voor externen op de website HU/privacy.

Rechten betrokkenen
Voor het verwerken van persoonsgegevens is in een aantal situaties de toestemming van de betrokkene vereist. Dat is het geval wanneer er geen sprake is van een wettelijke taak of een gerechtvaardigd belang. Belangrijke voorwaarden voor toestemming zijn dat de betrokkene goed geïnformeerd is, vrijwillig toestemming geeft en weet wat zijn rechten zijn. Eén van zijn rechten is bijvoorbeeld dat hij de toestemming weer kan intrekken.

De privacywet (AVG) geeft alle mensen waarvan persoonsgegevens worden verwerkt specifieke rechten. Iedereen heeft het recht om de persoonsgegevens die Hogeschool Utrecht van hem of haar verzamelt; in te zien, te wijzigen indien deze niet juist of incompleet zijn. In specifieke situaties kunnen betrokkenen gegevens ook laten verwijderen of de verwerking beperken (stil te zetten). Mensen die deze rechten willen uitoefenen, kunnen zich richten tot de privacydesk van Hogeschool Utrecht (via Askprivacy@hu.nl). Deze rechten zijn verder uitgewerkt in hoofdstuk 2.3.8 en 2.3.9

In de bijlage 1 worden begrippen uit de AVG nader uitgelegd.

2.2 In acht genomen wet- en regelgeving

Hogeschool Utrecht geeft uitvoering aan haar privacybeleid aan de hand van wettelijke kaders zoals vanzelfsprekend de (U)AVG, maar ook de WHW (Wet op het Hoger onderwijs en Wetenschappelijk onderzoek) en de Archiefwet. Belangrijke richtlijnen om dit beleid te concretiseren zijn de Selectielijst Hoger Onderwijs voor wat betreft dataretentie. Daarnaast bieden ISO en SURF richtlijnen voor verdere aanscherping en concretisering van het beleid.

Relevante wetgeving en richtlijnen

De voornaamste voor de HU van toepassing zijnde wet- en regelgeving met impact op het privacy- en informatiebeveiligingsbeleid zijn:

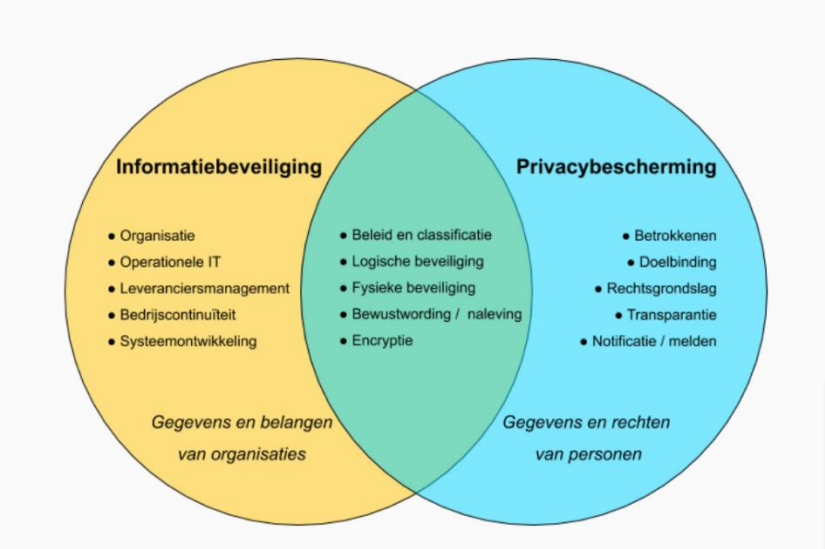
- Algemene Verordening Gegevensbescherming (AVG)

- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
- Selectielijst Hoger Onderwijs
- Privacy audit SURF (volwassenheidsniveaus per cluster verplichtingen)
- Ai verordening EC
- Gepubliceerde aanbevelingen/richtlijnen Autoriteit Persoonsgegevens
- Gepubliceerde aanbevelingen/richtlijnen SURF
- Wet op de geneeskundige behandelovereenkomst (WGBO) / Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)/ Wet cliëntenrechten zorg (Wcz);
- Wet op het Hoger Onderwijs en Wetenschappelijk onderzoek (WHW);
- Archiefwet;
- Auteurswet.

In de bijlage 2 wordt de relevante wet- en regelgeving nader toegelicht.

2.3 Principes AVG

Voor bescherming van persoonsgegevens is het voorwaardelijk dat de informatiesystemen waarin deze verwerkt worden, goed beveiligd zijn. Er is daarom ook overlap in de principes van zowel informatiebeveiliging als privacy. In onderstaande figuur worden de verschillen én raakvlakken verhelderd.



Bron: wat hebben privacy en informatiebeveiliging met elkaar te maken? - Axxemble

In het informatiebeveiligingsbeleid (Hogeschool Utrecht, 2019) zijn deze principes, inclusief de implicaties en verantwoordelijkheden uitgewerkt. De belangrijkste principes in dit informatiebeveiligingsbeleid, die ook zeer relevant zijn voor privacybescherming, zijn:

- Informatiebeveiliging is risico gebaseerd
- Security by Design
- Security by Default
- Data heeft één eigenaar
- Informatietoegang is rol gebaseerd

In dit hoofdstuk van het privacybeleid wordt specifiek ingegaan op de principes die vooral de bescherming van persoonsgegevens raken.

2.3.1 De Hogeschool informeert betrokkenen over de verwerking van persoonsgegevens

Rationale	HU behoort iedereen van wie persoonsgegevens worden verwerkt, te informeren welke persoonsgegevens worden verwerkt, op basis van welke grondslag en hoe deze gegevens worden beschermd. Dit wordt uitgelegd in de privacyverklaring. HU heeft privacyverklaringen voor diverse betrokkenen, zoals onze studenten, medewerkers, alumni en cursisten. Bij grote projecten waar (nieuwe) persoonsgegevens worden verwerkt, wordt een privacyverklaring voor specifiek dat doel opgesteld. De privacyverklaringen zijn gepubliceerd op Weten&Regelen op Een HU en op de regelementensite en worden bij nieuwe medewerkers en cursisten actief onder de aandacht gebracht.
Implicaties	• Data-eigenaren, projectleiders horen bij de initiatiefase te beoordelen of een privacyverklaring noodzakelijk is. • Hiertoe kunnen zij advies vragen bij hun privacy-officer of de privacymanager • De privacy-officer of -manager stelt een concept privacyverklaring op aan de hand van een vast format. • De FG adviseert over de concept tekst. • Privacyverklaringen dienen op een toegankelijke manier gepubliceerd te worden, en betrokkenen worden hierop geattendeerd, bijvoorbeeld bij het verzoek om toestemming.
Accountable	• CvB
Responsible	• HU-directeur
Consulted	• Privacy-officer, Privacymanager, FG
Informed	• Projectleiding

2.3.2 Hogeschool Utrecht houdt een verwerkingsregister bij

Rationale	Elke organisatie is verplicht een register bij te houden waarin alle verwerkingen met persoonsgegevens zijn geregistreerd. Dit geldt dus voor alle HU-processen waarbij persoonsgegevens worden verwerkt, ook als daar geen verwerkersovereenkomst voor hoeft te worden afgesloten. Het register dient op verzoek van de Autoriteit Persoonsgegevens opgeleverd te worden. Het register is niet alleen een verantwoordingsinstrument maar biedt tevens inzage in de verwerkingen bij een datalek of een inzageverzoek. Daarnaast is het het centrale register voor de afgesloten verwerkersovereenkomsten. Informatie over het verwerkingsregister is te vinden op Een HU.
Implicaties	• De organisatieonderdelen (data-eigenaren) zijn zelf verantwoordelijk voor het bijhouden van hun verwerkingen. • De beheerder van het verwerkingsregister ondersteunt de privacy-officers en monitort samen met de privacymanager de volledigheid en kwaliteit van het register. • In het register proberen we zoveel mogelijk aan te sluiten op de terminologie van de HU-processen. • De FG beoordeelt de rechtsgeldigheid van de verwerkingen.
Accountable	• CvB
Responsible	• HU-directeur

Consulted	• Privacy-officer, Privacymanager, FG
Informed	• Proces of systeemeigenaren van een verwerking, projectleiders

2.3.3 Privacy by design

Rationale	Privacy by design betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of ICT-omgeving rekening wordt gehouden met de beveiliging en bescherming van (persoons)gegevens. Dit is een wettelijke verplichting vanuit de AVG, maar voorkomt ook herstelwerkzaamheden achteraf.
Implicaties	• De business proceseigenaar is ervoor verantwoordelijk dat bij elk nieuw project/IT-systeem/innovatie vanaf de start de security eisen (non-functional requirements) worden meegenomen. • Door middel van een (pré)DPIA worden risico's voor de bescherming van persoonsgegevens gedetecteerd en mitigerende maatregelen benoemd. • De FG geeft advies over de uitgevoerde DPIA en de te nemen maatregelen. Bij zware inbreuk op persoonsgegevens legt de FG het advies voor aan de Autoriteit Persoonsgegevens. • Voor de live-gang wordt de toepassing van de security eisen getoetst en/of getest door of namens team Team Strategy & Compliance van de dienst IM&ICT. • Het principe van 'minste rechten' wordt gehanteerd. Dat betekent dat ernaar wordt gestreefd om niet meer rechten te verlenen dan nodig zijn voor adequate functie- en bedrijfsuitoefening • Waar van toepassing worden persoonsgegevens geanonimiseerd. • In test- en acceptatie omgeving worden geen persoonsgegevens uit de productie-omgeving gebruikt. • De business proceseigenaar past risico-afweging informatiebeveiliging en de principes van administratieve organisatie (AO) toe bij de inrichting van taken verantwoordelijkheden en bevoegdheden.
Accountable	• Business Proces Eigenaar
Responsible	• Business Proces Eigenaar
Consulted	• Privacy-officer, FG • Dienst Business Control • Team Processen, dienst IM&ICT • Team Strategy & Compliance, dienst IM&ICT
Informed	• Functioneel beheerder, Technisch beheerder

2.3.4 Privacy by default

Rationale	Privacy by default betekent dat in elke configuratie die wordt geïmplementeerd voor aanwezige security opties de meest veilige optie wordt geactiveerd. Dit is een wettelijke verplichting vanuit de AVG en voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens.
Implicaties	• De baseline van de standaardconfiguratie moet worden vastgelegd. • Het principe bij initiële inrichting van een informatiesysteem is "gesloten, tenzij…. " • Afwijking van de initiële inrichting moet volgens het principe "pas toe of leg uit." • Controle hierop wordt geborgd in het changemanagement proces.
Accountable	• Eigenaar van een technische component (dienst, applicatie, server, netwerkcomponent etc.)

Responsible	• Eigenaar van een technische component (dienst, applicatie, server, netwerkcomponent etc.)
Consulted	• Team Strategy & Compliance, dienst IM&ICT
Informed	• Functioneel beheerder, Technisch beheerder

2.3.5 HU heeft een laagdrempelige datalekprocedure

Rationale	Van een datalek is sprake als er een inbreuk op de beveiliging van persoonsgegevens plaatsvindt, die leidt tot ongeoorloofde verwerking. Datalekken moeten binnen **72** uur na ontdekking worden gemeld bij de Autoriteit Persoonsgegevens en in sommige gevallen ook bij de betrokkene (zie ook Hoofdstuk 5). Een Datalek kan binnen de eigen organisatie ontstaan, maar ook bij een door Hogeschool Utrecht ingeschakelde verwerker. Een datalek dient zo spoedig mogelijk intern te worden gemeld via het meldingsformulier. Indien een melder anoniem wil blijven is het ook mogelijk telefonisch contact op te nemen met de FG. Op EEN HU wordt uitgelegd wat een datalek is en waarom het belangrijk is (een vermoeden van) een datalek altijd te melden.

Implicaties	• Medewerkers moeten, indien zij een (mogelijk) datalek waarnemen of denken zelf onderdeel te zijn van een datalek, een melding maken door het meldingenformulier dat te vinden is op EEN HU en op HU Wegwijs in te vullen. Dit formulier komt automatisch terecht bij de privacydesk en in de mailbox van de FG.
	• Het is ook mogelijk dat er een datalek plaatsvindt bij een door Hogeschool Utrecht ingeschakelde verwerker. De verwerker zal overeenkomstig de afgesloten verwerkersovereenkomst het Datalek melden aan de FG van Hogeschool Utrecht.
	• Andere betrokkenen kunnen direct een mail sturen aan de FG. De contactgegevens staan vermeld op de website van de HU bij privacy.
	• Bij melding van een datalek, gaat het in ieder geval om de volgende informatie:
	  ○ Wie heeft er gemeld?
	  ○ Wat is er gemeld?
	  ○ Waar kwam de melding vandaan?
	  ○ Om welke gegevens gaat het?
	  ○ Van hoeveel betrokkenen zijn gegevens (mogelijk) gelekt?
	  ○ Hoe heeft het incident plaatsgevonden?
	  ○ Welke systemen zijn betrokken bij/geraakt door het incident?
	  ○ Wanneer heeft het incident plaatsgevonden?
	• Afhankelijk van de oorzaak van het datalek en de impact wordt een onderzoeksteam samengesteld. Als er direct securitymaatregelen genomen dienen te worden wordt er nauw samengewerkt met de collega's van security (CERT) of nemen zij de leiding in het onderzoek.
	• Betreft het een datalek met zeer hoge impact, dan wordt opgeschaald naar een crisisteam en wordt ook het CvB en de woordvoerder ingeschakeld.
	• De FG en de directeur van het betreffende organisatie-onderdeel worden op de hoogte gehouden en betrokken bij de besluitvorming. Indien het gaat om

	een security probleem wordt ook de directeur IM&ICT betrokken in de verdere afhandeling. • Indien het datalek impact heeft op betrokkenen, worden zij geinformeerd. • Alle datalekken worden geregistreerd in een register. De FG maakt jaarlijks een rapportage van de datalekken en de oorzaak daarvan. Hierin staat ook een duiding en advies voor te nemen maatregelen om een datalek zoveel mogelijk te voorkomen. De privacy-officers brengen deze rapportage en het advies onder de aandacht bij van hun eigen MT. • Om meldingen te stimuleren en medewerkers en studenten zich vrij te laten voelen een datalek te melden, zal de communicatie met de melder altijd constructief verlopen. • Medewerkers kunnen een datalek altijd melden op eigen initiatief, er is geen overleg of toestemming van een leidinggevende noodzakelijk. • Het bewust niet melden van een datalek met grote consequenties voor de organisatie (opzettelijke nalatigheid, plichtsverzuim), kan tot maatregelen richting medewerker leiden zoals opgenomen in CAO artikel P3.
Accountable	• CvB
Responsible	• Directeur/Data-eigenaar (in de HU praktijk: business proceseigenaar)
Consulted	• FG, Privacymanager, Privacy-officer, Information Security-officer, JZ, woordvoerder
Informed	• Medewerkers betrokken bij het datalek (het systeem / proces waar het datalek heeft plaats gevonden). • Melder • Betrokkenen indien het datalek risico's voor hun persoonsgegevens met zich mee brengt.

2.3.6 Een DPIA wordt uitgevoerd bij nieuwe verwerkingen en systemen

Rationale	Hogeschool Utrecht voert een Data Protection Impact Assessment (DPIA) uit, bij (onderzoeks)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen die waarschijnlijk een hoog risico vormen voor de rechten en vrijheden van personen. In sommige gevallen worden ook bestaande projecten en systemen geëvalueerd via een DPIA. Na drie jaar wordt een DPIA herhaald en worden eventuele nieuwe risico's en wijzigingen in kaart gebracht. SURF voert in het kader van Vendor Compliance DPIA's uit op systemen die door vele onderwijsinstellingen worden gebruikt. Waar SURF een DPIA uitvoert, sluit Hogeschool Utrecht aan bij de bevindingen en bepaalt de maatregelen die voor HU noodzakelijk zijn. Daar waar het gaat om AI toepassingen, zal gezamenlijk met andere expertises binnen de HU (denk aan ethiek, digitalisering) een IAMA (Impact Assessment Mensenrechten en Algoritme) of een vragenset uit de IAMA eveneens worden betrokken in de beoordeling.
Implicaties	• De privacy-officer beoordeelt aan de hand van een Pre-DPIA of een DPIA noodzakelijk is. Zo nodig wint hij/zij advies in bij de privacymanager. • De FG adviseert de data-eigenaar tot het uitvoeren van een DPIA. • De privacy-officer organiseert de DPIA voor de eigen projecten, altijd in opdracht van de data-eigenaar. • De privacymanager is verantwoordelijk voor de uitvoering van de DPIA als het gaat om HU-brede projecten en adviseert de privacy-officers bij hun DPIA.

	• Bij de DPIA worden de diverse stakeholders betrokken (projectleiding, security, functioneel beheer, betrokkene). • Bij uitbreiding naar een IAMA zullen ook de betreffende expertises worden betrokken. • De FG brengt vervolgens advies uit over te nemen maatregelen op basis van de rapportage. • Als blijkt dat een verwerking een hoog risico vormt en indien Hogeschool Utrecht niet in staat is de gewenste maatregelen te nemen, raadpleegt de FG voorafgaand aan de verwerking, de toezichthoudende autoriteit. • HU maakt gebruik van het DPIA-format van de Rijksoverheid en heeft voor haar eigen organisatie een procedure vastgesteld.
Accountable	• CvB
Responsible	• HU-directeur
Consulted	• Privacy-officer • FG • Stakeholders die deelnemen aan de DPIA (security, betrokkenen, functioneel beheer)
Informed	• Collega's die betrokken zijn bij het systeem/proces

2.3.7 Privacywetgeving is uitgelegd in eenduidige en goed vindbare instructies

Rationale	Iedereen behoort bewust te zijn van de waarde van informatie en privacy van betrokkenen en daarnaar te handelen. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Van zowel medewerkers, studenten als derden wordt verwacht dat ze bewust omgaan met informatie en bijdragen aan de veiligheid van de geautomatiseerde systemen en de daarin opgeslagen (persoons)gegevens. Omdat kennis van zowel privacy als informatiebeveiliging voorwaardelijk zijn, worden awareness activiteiten altijd vanuit beide disciplines gezamenlijk opgepakt. Voor casuïstiek kunnen medewerkers en studenten terecht bij hun privacy-officer. Indien wenselijk kan de vraag ook voorgelegd worden aan de privacydesk of aan de privacymanager. Adviesaanvragen kunnen gaan over casuistiek als mag ik de reden van ziekteverzuim vragen, tot vragen over een advies bij projecten en nieuwe systemen.
Implicaties	• Bij instroom van nieuwe medewerkers en studenten is aandacht voor de bewustwording van de risico's, de HU beveiligingsprocedures en de omgang met persoonsgegevens. O.a. via de brochure voor nieuwe medewerkers en het introductieprogramma op Een HU. • Voor alle gebruikers van de HU informatievoorzieningen zijn *ICT Gedragsregels* en een *gedragscode omgang met data* beschikbaar via Een HU. Deze code is van toepassing op zowel studenten, medewerkers als derden. • Er is een afwegingskader privacy dat een aantal belangrijke vuistregels van de AVG doorloopt en daarbij ondersteunt in het geven van advies. • Op Een HU staan alle belangrijke instructies op Weten&Regelen/Privacy en Security. Er is in mijnTalent een e-learning Privacy beschikbaar voor vaste medewerkers. • Medewerkers en derden tekenen voor het veilig omgaan met informatie en informatiedragers.

	• De HU organiseert regelmatig cybersecurity en privacy awareness activiteiten voor de diverse doelgroepen: studenten, medewerkers, leidinggevenden en partners van de HU. • Via een privacynieuwsbrief en blogs op EEN HU-informatieveiligheid worden actuele ontwikkelingen en publicaties onder de aandacht gebracht. • Schending van wetgeving, voorschriften en regels op gebied van informatiebeveiliging kan leiden tot sanctionerende maatregelen, door of namens het CvB.
Accountable	• CvB
Responsible	• HU-directeur, Privacymanager
Consulted	• Privacy-officers, Information Security Officer, JZ
Informed	• Alle medewerkers, studenten en partners van de HU

2.3.8 Betrokkenen kunnen hun privacyrechten uitoefenen

Rationale	<u>Toestemming</u> Voor het verwerken van persoonsgegevens is in een aantal situaties de toestemming van de betrokkene vereist. Dat is het geval wanneer er geen sprake is van een wettelijke taak of een gerechtvaardigd belang. Het gaat dan bijvoorbeeld om het interviewen van respondenten of het filmen van een behandeling voor een praktijkles. Ook bij het gebruik van filmpjes of foto's voor plaatsing in een bericht in een nieuwsbrief of op een website is toestemming vereist. Belangrijke voorwaarden voor toestemming zijn dat de betrokkene goed geïnformeerd is, vrijwillig toestemming geeft en weet wat zijn rechten zijn. Eén van zijn rechten is bijvoorbeeld dat hij de toestemming weer kan intrekken .
	
	<u>Rechten betrokkenen</u>
	
	De privacywet (AVG) geeft alle mensen waarvan persoonsgegevens worden verwerkt specifieke rechten. Iedereen heeft het recht om de persoonsgegevens die Hogeschool Utrecht van hem of haar verzamelt;
	• in te zien.
	• te wijzigen indien deze niet juist of incompleet zijn.
	• te laten verwijderen in de volgende gevallen:
	  ○ als de gegevens niet langer nodig zijn voor het doel waarvoor ze zijn verzameld;
	  ○ als een gegeven toestemming intrekt wordt ingetrokken en deze toestemming de enige grondslag is waarop de verzameling is gebaseerd;
	  ○ als de persoonsgegevens onrechtmatig zijn verzameld.
	• de verwerking van de persoonsgegevens te beperken (stil te laten zetten). De gegevens mogen dan alleen nog worden verwerkt in de volgende gevallen:
	  ○ met toestemming;
	  ○ voor het instellen, uitoefenen of onderbouwen van een rechtsverordening;
	  ○ ter bescherming van de rechten van anderen.
	Een verzoek ter uitoefening van bovengenoemde rechten kan schriftelijk worden ingediend bij askprivacy@hu.nl.

Implicaties	• Hogeschool Utrecht draagt er zorg voor dat de informatie en communicatie over deze rechten op een beknopte, toegankelijke en begrijpelijke manier wordt verstrekt aan betrokkene. • Op een verzoek (bijv. inzage) van een betrokkene wordt zo spoedig mogelijk, doch uiterlijk binnen een maand na indiening, schriftelijk gereageerd. Hierbij zal de betrokkene in ieder geval in kennis worden gesteld van het gevolg dat aan het verzoek is gegeven. • Indien de termijn van een maand redelijkerwijs niet haalbaar is, zal betrokkene daarvan binnen deze termijn op de hoogte worden gesteld. Hogeschool Utrecht zal in dat geval binnen twee maanden na het verstrijken van de eerste termijn gevolg geven aan het verzoek van de betrokkene. • Hogeschool Utrecht draagt bij het verstrekken van de betreffende informatie zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker. Hiertoe kan Hogeschool Utrecht extra informatie vragen. • Een verzoek tot uitoefening van een van de rechten door een minderjarige, een betrokkene die onder curatele is gesteld of ten behoeve van wie een bewind of mentorschap is ingesteld, moet worden ingediend door diens wettelijk vertegenwoordiger. Een reactie door Hogeschool Utrecht zal ook naar deze wettelijke vertegenwoordiger worden verstuurd. • De betrokkene kan om een kopie van alle persoonsgegevens verzoeken. Deze kopie dient in een gangbare elektronische vorm te worden verstrekt, tenzij de betrokkene expliciet om een papieren kopie verzoekt. Iedere (eerste) kopie kan kosteloos worden aangevraagd. • Hogeschool Utrecht zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen. • Persoonsgegevens waarvan de bewaartermijn al is verstreken, maar die HU nog wel in haar bezit heeft, moeten ook worden verstrekt. • Deze rechten zijn ook van toepassing op persoonsgegevens die worden opgeslagen in niet officiële documenten, zoals een mailbericht of een verslag.
Accountable	• CvB
Responsible	• HU Directeuren
Consulted	• FG, Privacymanager, Privacy-officer, JZ, IM&ICT bij zoekopdrachten
Informed	• Alle medewerkers, studenten en partners van de HU

2.3.9 Klachten en bezwaarprocedure

Rationale	Naast de in 2.3.8 beschreven rechten, heeft de betrokkene de volgende mogelijkheden als hij van mening is dat Hogeschool Utrecht de AVG niet of onvoldoende heeft nageleefd. *Verzoekschriftprocedure bij de kantonrechter* Indien Hogeschool Utrecht afwijzend heeft beslist op een verzoek zoals beschreven bij de uitoefening van rechten, of het verzoek van de betrokkene heeft afgewezen, kan de betrokkene een verzoekschriftprocedure starten bij de kantonrechter. *Verzoek tot handhaving bij toezichthoudende autoriteit* Indien Hogeschool Utrecht afwijzend heeft beslist op een verzoek zoals beschreven bij 2.3.8, of Hogeschool Utrecht heeft het verzoek van de betrokkene 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.
Implicaties	• Het verzoekschrift dient binnen zes weken na ontvangst van het antwoord van Hogeschool Utrecht ingediend te worden bij de kantonrechter.

	• Indien Hogeschool Utrecht niet binnen de gestelde termijn heeft geantwoord op het verzoek van betrokkene, moet het verzoekschrift binnen zes weken na afloop van die termijn worden ingediend. Indiening van het verzoekschrift hoeft niet door een advocaat te geschieden.
Accountable	• CvB
Responsible	• HU-directeur
Consulted	• Privacymanager, Privacy-officer, FG, JZ
Informed	• Alle medewerkers, studenten en partners van de HU

2.3.10 Alle IT-voorzieningen worden via het standaard change-proces in gebruik genomen

Rationale	Met de verdere digitalisering van zowel onderwijs als onderzoek, maar ook het thuiswerken en online samenwerken, is er behoefte aan voortdurende innovatie. Het gebruik van nieuwe tools en apps is daarbij een logische stap. De tools verwerken echter mogelijk persoonsgegevens van docenten en studenten, geven deze door aan derden of plaatsen cookies. Alleen al door in te loggen met het HU-account worden gegevens vanuit het HU-profiel gedeeld. Het is dan ook niet toegestaan niet goedgekeurde apps te gebruiken, ook (juist) niet als ze gratis zijn.
Implicaties	• Collega's die een nieuwe app willen aanschaffen dienen dit binnen de juiste privacy- en securitykaders te doen. Zij moeten daarvoor een Aanvraagformulier invullen. • De aanvraag wordt beoordeeld door de Business IT consultant bij IM&ICT op meerwaarde, beschikbaarheid van vergelijkbare apps, functionaliteit in applicatielandschap en beheer. In overleg met de collega's van privacy en security wordt beoordeeld of de leverancier voldoet aan de juiste eisen. • Met bovengenoemde collega's is een proces aanvraag applicaties vastgesteld en gepubliceerd op EEN HU. • Met betrokken leverancier dient een verwerkersovereenkomst te worden opgesteld. • In die gevallen waar afgeweken wordt van de HU richtlijnen, moet het comply or explain register worden ingevuld. De betreffende directeur is daarmee verantwoordelijk voor de risico's die ontstaan bij de afwijking. • Een overzicht met toegestane en goedgekeurde applicaties wordt beschikbaar gesteld.
Accountable	• CvB
Responsible	• HU-directeur
Consulted	• BIT consultant, information security-officer, privacymanager • Inkoopadviseurs • Privacy-officer • FG
Informed	• Medewerkers van de HU

2.3.11 Privacybescherming is een continu proces

Rationale	De omgeving verandert continu; cyberdreigingen nemen toe en af; processen veranderen, medewerkers en studenten veranderen etc. Nieuwe projecten en verwerkingen dienen zich aan. Eenmalig de maatregelen bepalen en

	implementeren is onvoldoende om een veilig klimaat te behouden. Informatiebeveiliging en privacybeleid heeft alleen zin indien dit een continu proces is van het nemen van maatregelen, bewustzijn en controles. Hogeschool Utrecht werkt vanuit een risicogerichte aanpak voor alle veiligheidsdomeinen. Binnen het domein Informatieveiligheid zijn voor privacy, informatiebeveiliging en kennisveiligheid, risico's gedefinieerd, ingeschat en mitigerende maatregelen geformuleerd. Deze maatregelen zijn opgenomen in het jaarplan Informatieveiligheid. Risico's zijn bepaald voor de gebieden Compliance (waarbij het normenkader van SURF wordt toegepast), Governance, Awareness en Incidentenafhandeling. Daarnaast voeren we een aantal standaard herzieningen en evaluaties uit.
Implicaties	• Procedures en richtlijnen regelmatig (minimaal 2 jaarlijks) herzien. • Privacyprocedures en -beleidsdocumenten zijn onderworpen aan een PDCA-cyclus • Audits (waaronder het SURF normenkader) en assessments maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit (controleerbaarheid) en mogelijkheden voor verbetering vast te stellen • Privacybeleid wordt periodiek geëvalueerd door de FG via assessments en binnen de bestaande privacy-overleggen. Verbetermaatregelen worden vervolgens door de privacy-organisatie geïnitieerd. • FG rapporteert in kwartaal en jaarrapportage de belangrijkste actuele ontwikkelingen, bevindingen en signalen • Verbeteringen van maatregelen, - procedures en -beleid worden planmatig doorgevoerd
Accountable	• CvB
Responsible	• HU Directeur, privacymanager
Consulted	• FG
Informed	• Privacy-officer

3 Privacy-organisatie

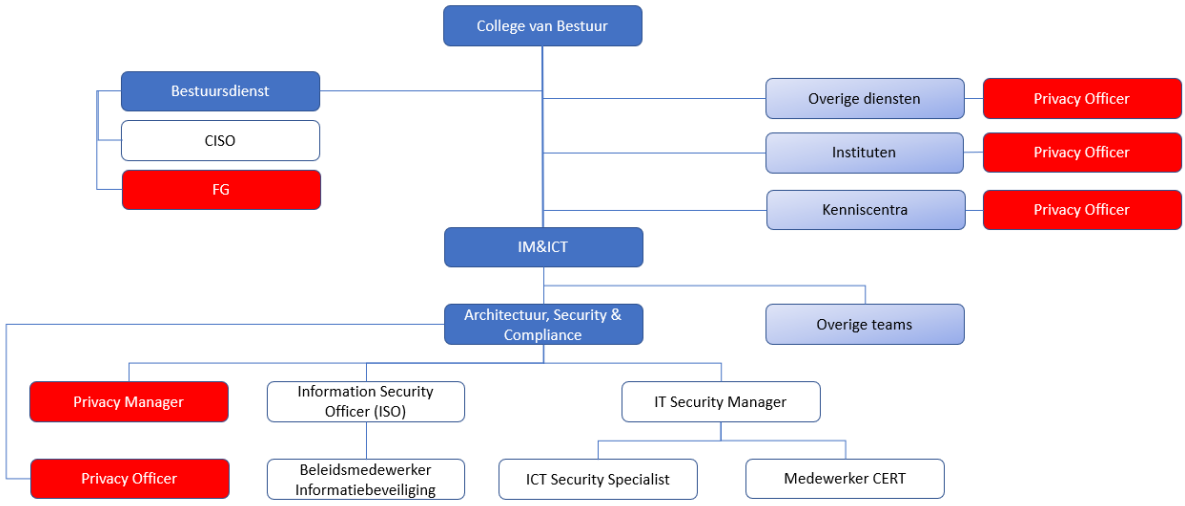
3.1 Verantwoordelijkheid Privacybeleid

Het CvB is eindverantwoordelijk voor het privacybeleid en heeft dit beleid vastgesteld. De dienst IM&ICT stelt het privacybeleid op, is verantwoordelijk voor implementatie binnen het IM&ICT-domein, en ondersteunt waar nodig de directies bij uitvoering en implementatie van het beleid buiten IM&ICT. De Functionaris Gegevensbescherming (FG) is de interne toezichthouder ten aanzien van de naleving van het privacybeleid en daarmee de bescherming van persoonsgegevens. De Chief Information Security Officer (CISO) ziet toe en toetst op juiste naleving van het securitybeleid door de HU.

3.2 Rollen, taken en verantwoordelijkheden

Het CvB is integraal verantwoordelijk voor de beveiliging van informatie (en dus persoonsgegevens) binnen de werkprocessen van de HU. De directeuren zijn verantwoordelijk voor het (laten) toepassen van de kaders zoals gesteld in het privacybeleid binnen hun dienst, instituut of kenniscentrum.

In onderstaande overzicht zijn de verschillende rollen en hun functionele relaties weergegeven.



3.2.1 De Functionaris Gegevensbescherming (FG)

De FG werkt op strategisch niveau binnen de bestuursdienst en is onder andere verantwoordelijk voor het toetsen van privacybescherming op basis van landelijke en Europese wet- en regelgeving, landelijke normenkaders en het SURF-normenkader, conform de behoeften en de risicobereidheid van de HU. Vanuit haar onafhankelijke rol heeft de FG een rechtstreekse escalatielijn naar het CvB. De FG wordt door de HU tijdig betrokken bij alle processen waarbij persoonsgegevens worden verwerkt. Hogeschool Utrecht heeft de FG aangemeld bij de Autoriteit Persoonsgegevens.

Assessments uit het bestuurlijk vastgesteld Jaarplan van de FG maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. Onafhankelijke accountants voeren externe controles uit. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk afgestemd op met de normale Planning & Control cyclus. Daarnaast neemt de HU deel aan de benchmarks van SURF op het gebied van Informatieveiligheid en Privacy.

3.2.2 Privacymanager

Hogeschool Utrecht heeft een privacymanager aangesteld om het privacybeleid binnen de HU te coördineren en er zorg voor te dragen dat de HU in de breedte compliant is aan de AVG en de gestelde kaders. De privacymanager maakt deel uit van de dienst IM&ICT.

De taken van de privacymanager houden in:

- advisering bij HU-brede projecten en beleid
- het aansturen van de privacy-organisatie; zorgen dat privacy-officers over de juiste en actuele kennis beschikken.
- verbeteren en actualiseren van processen en verantwoording (o.a. het verwerkingsregister)
- betrekken juiste stakeholders (bijv. Inkoop, IM&ICT) en verbinden met de privacy-organisatie
- in samenwerking met de IT securitymanager en de privacy-officers de awareness vergroten onder medewerkers en studenten.

Daar waar informatiebeveiliging en privacy elkaar raken, werkt de privacymanager nauw samen met de IT securitymanager.

3.2.3 Privacy-officer

Elk instituut, dienst en kenniscentrum heeft een collega die de rol van privacy-officer op zich heeft genomen en hier ook capaciteit voor heeft gekregen. De privacy-officers zijn het aanspreekpunt voor hun eigen organisatie-onderdeel. Zij geven advies bij privacyvraagstukken en privacydilemma's en informeren de organisatie actief over belangrijke AVG-onderwerpen en richtlijnen. Denk hierbij aan het afsluiten van een verwerkersovereenkomst of het bijhouden van het verwerkingsregister. Naast de basistaken hebben de meeste privacy-officers ook een specialisatie, bijvoorbeeld key-user van de privacy-tools, adviseur bij het uitvoeren van een DPIA of het opstellen van een verwerkersovereenkomst. Daarnaast nemen privacy-officers deel aan projecten die over specifieke verbeterthema's gaan (bijv. proces uitvragen toestemming, stage en AVG).

Alle privacy-officers en de privacymanager vormen gezamenlijk de privacyorganisatie. Zij komen frequent samen om het privacybeleid verder inhoud te geven en casuïstiek uit te wisselen. Belangrijke

signalen of onderwerpen uit de eigen organisatie worden besproken indien ze voor de gehele HU van belang zijn. Ook werkt de privacy-organisatie aan nieuwe richtlijnen of informatie die vervolgens binnen het eigen organisatie-onderdeel wordt gedeeld. De FG informeert de privacy-organisatie over belangrijke vraagstukken waar zij advies over heeft uitgebracht en over onderwerpen die HU breed spelen of binnen SURF-verband worden opgepakt. Ook betrekt zij de privacy-organisatie waar nodig in haar assessments.

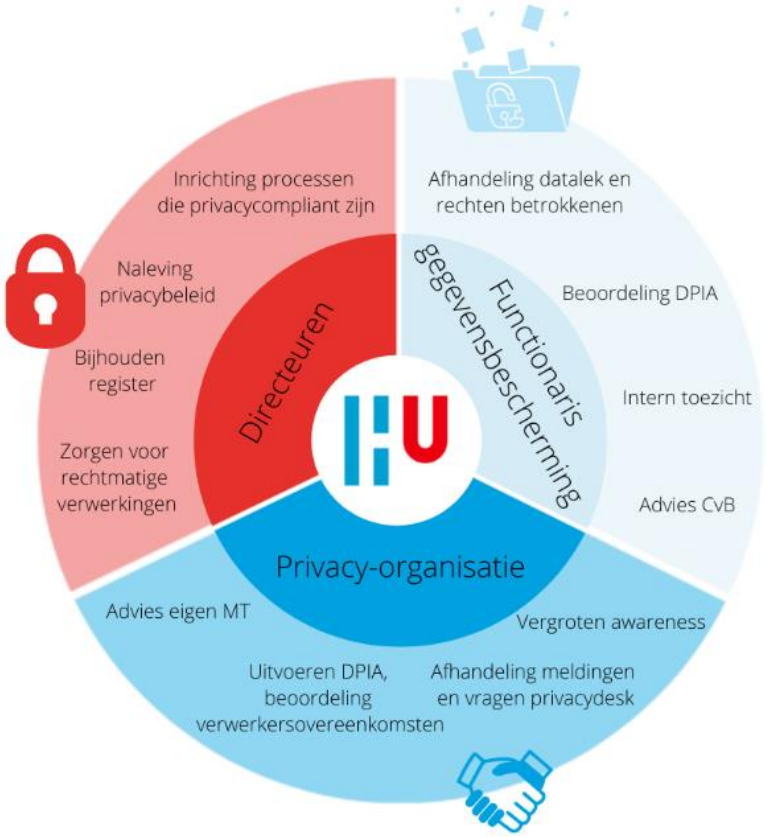
Collega's en studenten kunnen vragen stellen of een melding doen (datalek) bij de privacydesk, via Askprivacy@hu.nl. Deze vragen worden beantwoord door de privacy-officers

3.2.4 Directeuren hebben eigen verantwoordelijkheid

Het creëren van bewustwording en de naleving van het beleid is onderdeel van de integrale bedrijfsvoering in de instituten, diensten en kenniscentra. Iedere directeur en leidinggevende heeft – zoals geregeld in het BBR – de volgende taken:

- in de rol van eigenaar van persoonsgegevens zorgdragen voor rechtmatige verwerkingen;
- het bijhouden van een actueel overzicht van verwerkingen;
- het ondersteunen van de afhandeling van (datalek)meldingen en verzoeken van betrokkenen;
- zorgen dat aangeschafte tools en diensten voldoen aan privacywetgeving;
- tekenbevoegd voor privacy overeenkomsten aangaande eigen onderdeel.

De directeur dient er voor te zorgen dat medewerkers en studenten op de hoogte zijn van de belangrijkste privacy-richtlijnen door passende werkprocessen te ontwikkelen en beheren en medewerkers te scholen/informeren. De eigen privacy-officer kan hierbij ondersteunen en adviseren.



3.2.5 Samenwerking binnen de HU

Bij de aanschaf van nieuwe diensten en applicaties wordt privacy-advies ingewonnen en vindt er afstemming plaats met Security, Sourcing, BIT consultants en Inkoop. Bijvoorbeeld over het programma van eisen en het opstellen van verwerkersovereenkomsten.

De afdeling Juridische Zaken (JZ) wordt regelmatig geraadpleegd bij casuïstiek of bij het uitwerken van AVG-wetgeving in richtlijnen. Bij de start van projecten en nieuwe verwerkingen zowel HU breed als bij een organisatie-onderdeel, adviseert de privacy-officer of privacymanager over de privacyvereisten als een DPIA of privacyverklaring.

CERT staat voor Computer Emergency Response Team. Dit team heeft een operationele taak om de impact van security incidenten te minimaliseren en ondersteuning te bieden om het beveiligingsniveau in technische zin op het gewenste niveau terug te brengen na een beveiligingsincident. Wanneer een mogelijk datalek (mede)veroorzaakt wordt door een security incident of wanneer een security-incident implicaties heeft voor de persoonsgegevens, werken collega's beide disciplines nauw samen om het datalek te onderzoeken en maatregelen te nemen.

Bij HU brede projecten waarbij (nieuwe) persoonsgegevens worden verwerkt, wordt de privacymanager en de privacy-officer van het betreffende organisatie-onderdeel om advies gevraagd.

3.2.6 Overlegstructuur

Op Tactisch en Operationeel niveau vindt structureel overleg plaats met de privacy-officers, en JZ. De privacy-officer van IM&ICT neemt deel aan de Change Advisory Board (CAB) om zo ook de AVG compliance van IT wijzigingen te kunnen beoordelen.

Jaarlijks wordt door de expertgroep informatieveiligheid een risicoanalyse gemaakt voor het veiligheidsdomein. Na weging van de gedefinieerde risico's worden de activiteiten voor het aanstaand jaarplan vastgesteld. De activiteiten worden vervolgens in de eerste lijn uitgevoerd.

Om de samenhang met andere veiligheidsdomeinen te borgen, vindt conform het Strategisch kader integrale veiligheid afstemming plaats in periodieke risicodialogen op operationeel, tactisch en strategisch niveau.

De directeur IM&ICT neemt deel aan het tactisch veiligheidsoverleg. Hier treffen de directeuren met een HU brede verantwoordelijkheid voor een veiligheidsdomein elkaar voor de afstemming van beleid en risicomanagement.

In het Governance overleg informatieveiligheid waarin zowel de experts vanuit Privacy en Informatiebeveiliging als MT leden IM&ICT deelnemen, wordt de voortgang van de Jaarplannen en belangrijke HU brede ontwikkelingen besproken.

3.2.7 RACI matrix

In de onderstaande RACI-matrix zijn de verschillende rollen uit voorgaande paragraaf beschreven met de bijbehorende verantwoordelijkheden.

	CvB	FG	Directeur / Data-eigenaar	Directeur IM&ICT	Privacy Manager	Privacy-officer	ISO
Privacystrategie / visie	A/I	C	C/I	R	R	C	C
Formuleren privacybeleid	A/I	C	I	R	R	C	C
Formuleren privacyrichtlijnen[1]	A	C	I	R	R	C	C
Opstellen Jaarplan Privacy	I	C	R	A	R	C	I
Uitvoeren beleid & richtlijnen	A/I	C/I	R	-	C	C	C
Risico-analyse en DPIA	A	C	R	-	R	C	C
Privacy assessments 1e en 2e lijn(toetsen naleving beleid)	A/I	R2	I	I	R1	C	I
Afhandeling datalekken	A/I	C	R/I	I	C	C	C
Afhandeling verzoeken betrokkenen	A	C	R/I	I	C	C	I
Verwerkingenregister bijhouden	A	I	R	-	C	C	-
Privacy bewustwording	A	C/I	R	R	C	C	C

Responsible, **A**ccountable, **C**onsulted, **I**nformed

Directeur IM&ICT heeft in dit model twee rollen; als directeur en data-eigenaar (zoals elke directeur) van IM&ICT en als directeur met informatieveiligheid in portefeuille (conform strategisch kader Integrale Veiligheid).

4 Goedkeuring, evaluatie en wijziging privacybeleid

Het CvB stelt het privacybeleid vast dat door de Directeur IM&ICT wordt voorgedragen. Het HU privacybeleid volgt de kaders van het HU-beleid en wordt iedere 3 jaar herzien, of na een substantiële verandering van het HU beleid.

4.1 Planning Strategy & Compliance

Aan het begin van het studiejaar wordt door de manager Strategy & Compliance een jaarplan gemaakt, waarin op hoofdlijnen de planning voor privacy wordt beschreven. Het jaarplan privacy dat door de privacymanager wordt opgesteld is afgestemd op dit jaarplan, de aanbevelingen uit assessments van de FG en de jaarlijkse risico-analyse Privacy binnen het domein Informatieveiligheid (zie ook hoofdstuk 2.3.11). Het jaarplan Privacy wordt gedeeld met de FG en privacy-officers. De privacy-officers stellen ieder hun eigen jaarplan op dat besproken wordt met hun eigen MT.

4.2 Rapportages

De FG rapporteert in een halfjaarsrapportage aan het CvB over belangrijke actuele ontwikkelingen, uitgevoerde assessments en signalen, bijvoorbeeld naar aanleiding van datalekken of casuïstiek.
De dienst IM&ICT rapporteert in de IR rapportage aan het CvB over de realisatie van het jaarplan en actuele ontwikkelingen.
Een samenvatting van deze rapportages wordt gedeeld met de privacy-officers en geagendeerd in het privacy-overleg met alle privacy-officers. Privacymanager en FG bespreken wekelijks de belangrijkste bevindingen en voortgang op projecten.

4.3 Controle en naleving

De uitvoering van het privacybeleid wordt jaarlijks geëvalueerd. Dit gebeurt in het najaar in het kader van het jaarlijks accountantsonderzoek en wordt zoveel mogelijk afgestemd met de normale Planning & Controlecyclus.

De toezichthoudende activiteiten van de FG bestaan uit het beoordelen van opzet, bestaan en werking van privacybescherming bij bestaande verwerkingen van persoonsgegevens en het beoordelen van de risicoschatting en rechtmatigheid van nieuwe verwerkingen. Risicovolle verwerkingen worden getoetst met een Data Protection Impact Assessment (DPIA). De FG ziet toe op de kwaliteit van de uitvoering en geeft advies over de aangedragen risico's en maatregelen. De FG monitort de maatregelen die worden genomen naar aanleiding van een datalek. De bevindingen worden opgenomen in het datalekregister.
De FG stelt een jaarplan op voor assessments – het toetsen van een aantal privacyprocessen. Denk aan het hanteren van bewaartermijnen; het proces van de DPIA of het opnemen van privacy in het curriculum. Directeuren zijn verantwoordelijk voor de uitvoering van de adviezen die uit zo een assessment volgen. Zij worden gevraagd hierover te rapporteren.

5 Melding en afhandeling privacy-incidenten

5.1 Definities

Een privacy-incident (datalek) is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Ieder datalek dient na vaststelling binnen 72 uur aan de Autoriteit Persoonsgegevens worden gemeld. De HU heeft hiervoor een proces vastgesteld (2.3.5). De Privacydesk en de Functionaris Gegevensbescherming zien toe op de kwaliteit en tijdigheid hiervan. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van betrokkenen zijn uitgezonderd van deze meldplicht. Voorbeelden van een datalek zijn:

- Het versturen van een brief/e-mail met persoonsgegevens naar de verkeerde persoon;
- het kwijtraken van gegevensdragers/documenten met persoonsgegevens (NB ook wanneer deze beveiligd zijn met een wachtwoord);
- diefstal van gegevensdragers/documenten met persoonsgegevens;
- ongeautoriseerde toegang tot persoonsgegevens, bijvoorbeeld medewerkers die ongeautoriseerd persoonsgegevens van studenten inzien of kwaadwillende hackers die zichzelf toegang verschaffen; documenten/dossiers met persoonsgegevens die door onzorgvuldigheid kunnen worden ingezien.

5.2 Incidenten bij de Hogeschool Utrecht

Medewerkers en studenten kunnen incidenten met betrekking tot informatiebeveiliging melden aan de Centrale Service Desk (CSD). Privacy gerelateerde incidenten (bijv. datalekken) kunnen worden gemeld bij Privacy Helpdesk van de HU en bij de Functionaris Gegevensbescherming. Zodra een privacy incident zijn oorzaak vindt of implicaties heeft voor informatiebeveiliging, zullen beide disciplines betrokken zijn in de afhandeling van het incident. Raakt het privacy incident alleen de verwerking van persoonsgegevens, maar heeft het verder geen betrekking op de informatiebeveiliging dan handelt de privacy-organisatie het incident verder af. Zie hiervoor ook bovenstaande datalekprocedure in 2.3.5.

Om een datalek goed en zorgvuldig af te handelen is er een procedure datalekken vastgesteld, met daarbij ook de onderzoeksaanpak en verantwoordelijkheidsverdeling, de benodigde instructies en formats.

Als een bedrijfsproces, de financiën of de goede naam van de HU in gevaar zijn, wordt via de lijn beoordeeld of ook het CvB en woordvoering ingelicht dient te worden.

5.3 Incidenten bij leveranciers

Informatiebeveiligingsincidenten bij leveranciers kunnen een impact hebben op de HU. In afspraken met leveranciers dient vastgelegd te worden hoe en wanneer de HU geïnformeerd wordt over de aard en afhandeling van informatiebeveiligingsincidenten bij de betreffende leverancier. In de verwerkersovereenkomst staan daarom standaard afspraken over de verplichtingen van de leverancier

bij de ontdekking van een datalek en de contactgegevens van de FG om deze zo snel mogelijk op de hoogte te stellen. Als verwerkingsverantwoordelijke ligt de meldplicht aan de Autoriteit Persoonsgegevens en indien nodig aan betrokkene bij Hogeschool Utrecht.

6 Sancties

6.1 Overtredingen privacybeleid

Gedragscode Data en Privacy

In de gedragscode Data en Privacy staat aangegeven welk gedrag van de medewerkers en studenten wordt verwacht. Het gaat dan bijvoorbeeld om veilig mailen van vertrouwelijke data, het gebruiken van goedgekeurde apps en het vertrouwelijk houden van persoonsgegevens. De ICT gedragsregels gaan specifiek in op het gebruik van devices, wachtwoorden, omgang met sociale media en melden van incidenten.

Inbreuk beveiliging persoonsgegevens

De HU neemt (onder voorwaarden) geen juridische stappen tegen melders van (mogelijke) veiligheidsgaten in informatiesystemen. Het doel hiervan is om kwetsbaarheden in systemen gemeld te krijgen voordat men hiervan misbruik kan/gaat maken, of de kwetsbaarheid wereldkundig maakt. Door het tijdig melden van kwetsbaarheden kan HU tijdig maatregelen ter voorkoming van misbruik nemen. Binnen de HU zal het melden van kwetsbaarheden actief worden gepromoot.

Het formulier 'Melding inbreuk veiligheid persoonsgegevens' vermeldt ook dat het melden van een datalek nooit gevolgen mag hebben voor een medewerker. Dit is dan ook het uitgangspunt. Ook is het mogelijk voor medewerkers om een anonieme melding te maken, om de drempel voor de melder zo laag mogelijk te maken. Voor het doen van een melding is het voor de medewerker niet noodzakelijk om vooraf toestemming te vragen of vooraf af te stemmen met andere collega's.

Een medewerker kan niet zomaar worden ontslagen of aansprakelijk worden gesteld, wel kan HU maatregelen treffen als aantoonbaar is dat de medewerker opzettelijk of bewust roekeloos heeft gehandeld. Bijvoorbeeld:

- het met opzet of bewust roekeloos veroorzaken van een datalek,
- het opzettelijke verzwijgen van een datalek terwijl men had kunnen verwachten dat dit grote consequenties voor de organisatie heeft,
- het onrechtmatig omgaan met persoonsgegeven of bedrijfsvertrouwelijke gegevens; zoals bijvoorbeeld het bewust delen met derden (denk aan een opdrachtnemer die offerte wil uitbrengen en kan profiteren van inzage in bedrijfsgegevens)

In deze situaties zal gekeken moeten worden naar het arbeidsrecht. In de CAO voor het hoger beroepsonderwijs, welke van toepassing is voor de HU, zijn verschillende artikelen opgenomen welke van toepassing zijn en onderdeel uitmaken van de arbeidsovereenkomst.

Zo zijn de medewerkers van de HU verbonden aan het beginsel van goed werknemerschap en ook aan de geheimhoudingsplicht.
Artikel P-3 van de CAO vermeldt 'de werkgever kan de werknemer die niet doet dan wel nalaat wat een goed werknemer in gelijke omstandigheden behoort te doen of na te laten en/of zich schuldig maakt aan plichtsverzuim een disciplinaire maatregel opleggen'. In een situatie waarin niet wordt voldaan aan het beginsel van goed werknemerschap of de geheimhoudingsplicht kan in overleg met HR en JZ beoordeeld worden welke maatregelen passend zijn.

Daarnaast is het belangrijk te melden dat wanneer een medewerker een datalek niet meldt, dit ook gevolgen kan hebben voor de medewerker maar ook voor de HU. De Autoriteit Persoonsgegevens kan de HU bijvoorbeeld een boete opleggen wegens het niet melden van een datalek.

Schending informatiebeveiliging

Bij schending van de regels ten aanzien van informatiebeveiliging kunnen door of namens het CvB maatregelen worden getroffen. Maatregelen kunnen bijvoorbeeld zijn de blokkering van de toegang tot het netwerk of specifieke netwerkdiensten. In geval de HU bij overtreding van intellectuele eigendomsrechten of andere regelgeving wordt aangesproken, dan wel bij schending van rechten van anderen, kan de HU eventuele schade verhalen op de schadeveroorzakende gebruiker. Indien schade wordt geleden als gevolg van misbruik van computer- en netwerkvoorzieningen kan de HU deze ook verhalen op de schadeveroorzakende gebruiker.

Bijlage 1: Begrippenlijst

***AVG**:* Algemene Verordening Gegevensbescherming.

***Autoriteit Persoonsgegevens (AP)**:* de Nederlandse toezichthoudende autoriteit op de verwerking van persoonsgegevens.

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

***Datalek**:* een inbreuk op de beveiliging van persoonsgegevens, die leidt tot enige ongeoorloofde verwerking daarvan. Een datalek kan zowel opzettelijk als onopzettelijk veroorzaakt zijn.

Data Privacy Impact Assessment (DPIA) (gegevensbeschermingseffectbeoordeling): 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.

***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.

Gezamenlijke verwerkingsverantwoordelijkenovereenkomst: een verwerkersovereenkomst waarbij er sprake is van twee verwerkersverantwoordelijken die gezamenlijke doeleinden hebben bij een verwerking. Denk bijvoorbeeld aan een onderzoeksproject waar meerdere partijen gegevens verwerken voor hetzelfde (onderzoeks)doel.

Minderjarige: iedere persoon die de leeftijd van 18 jaar nog niet heeft bereikt.

Persoonsgegeven: elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.

Privacy by Default: 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: Het beheer van een verwerkingsproces 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.

Privacyverklaring (Privacystatement):Een bericht waarin in begrijpelijke taal aan betrokkenen wordt uitgelegd welke persoons-gegevens worden verwerkt en op welke manier.

Privacyshield: Het privacyshield bood een garantie dat een leverancier (in de VS) voldeed aan de vereisten vanuit de GDPR (de Engelse afkorting voor AVG). Inmiddels is dit Privacyshield door het Europese Hof ongeldig verklaard, omdat de privacygaranties, onder andere vanwege nationale wetgeving in de VS, niet konden worden gerealiseerd.

Profilering: elke vorm van geautomatiseerde verwerking 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

Standard Contractual Clause (SCC): Verwerkersovereenkomst voor bedrijven (in de VS) buiten de EER, waarvoor geldt dat hun wettelijke regelingen niet dezelfde waarborg bieden als de GDPR. Een SSC is modulair opgebouwd en kan ook van toepassing zijn bij een gezamenlijk verwerkingsverantwoordelijkenovereenkomst.

Verwerker: een door Hogeschool Utrecht ingeschakelde partij die ten behoeve van Hogeschool Utrecht, en op basis van haar schriftelijke instructies, persoonsgegevens verwerkt.

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 HU: het College van Bestuur van Hogeschool Utrecht dat het doel en de middelen van de verwerking van persoonsgegevens vaststelt.

Bijlage 2: Wet- en Regelgeving

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

Algemene Verordening Gegevensbescherming (AVG)
Sinds 2012 is er op Europees niveau gewerkt aan nieuwe wetgeving over privacy, de AVG. In mei 2016 is deze verordening officieel gepubliceerd en is een implementatietermijn van 2 jaar gaan lopen. Dit betekent dat vanaf 26 mei 2018 iedereen die persoonsgegevens verwerkt binnen Europa zich aan deze verordening moet houden. Naleving van de beveiligingsmaatregelen en verwachte gedrag leidt tot voldoen aan de wet.

De Algemene Verordening gegevensbescherming vraagt extra aandacht voor de verwerking van bijzondere persoonsgegevens, waaronder gezondheidsgegevens. Een zorginstelling is dan ook verplicht de gegevens van haar cliënten in het dossier adequaat te beschermen. In feite zijn genoemde NEN-normen hierdoor al jarenlang (sinds 2005) impliciet verplicht voor de zorgsector in het kader van de beveiliging van persoonsgegevens. De norm voor informatiebeveiliging in de zorg is daarom van toepassing op alle zorgaanbieders en organisaties in de zorg- en welzijnssector die persoonlijke gezondheidsinformatie beheren (zoals de HU), ongeacht de aard en omvang van het bedrijfsproces.

Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
De AVG is een Europese verordening. Dat houdt in dat de AVG niet nog eens apart hoeft te worden opgenomen in Nederlandse wetgeving. De AVG legt wel de verplichting op aan EU-lidstaten om bepaalde zaken te regelen (zoals de oprichting van een nationale autoriteit die toezicht houdt), en geeft hen tevens de mogelijkheid om bepaalde normen en regels uit de AVG verder in te vullen. De Uitvoeringswet Algemene Verordening Gegevensbescherming vult deze normen en regels in voor de nederlandse situatie. De UAVG is onder meer de wettelijke basis voor de inrichting, taken en verantwoordelijkheden van de Autoriteit Persoonsgegevens, maar bevat ook nadere bepalingen voor de verwerking van bijzondere persoonsgegevens (gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid)

Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW)
De HU heeft een kwaliteitszorgsysteem (ITK), 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.

Wet op de geneeskundige behandelovereenkomst (WGBO)
De WGBO (BW-boek 7, afdeling 5, art. 446-468), omtrent rechten en plichten voor zowel hulpverlener als cliënt, is van toepassing op het verwerken van gegevens door de zorginstelling die de hulpverlener in het kader van de behandeling van de cliënt heeft verkregen. Die wet verplicht hem de noodzakelijke gegevens vast te leggen in zijn dossier over de cliënt.

Archiefwet
De HU houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is periodiek onderdeel van de externe accountants-rapportages.

Auteurswet
De HU verspreidt geen originele werken zonder dat daarvoor toestemming is verkregen van de eigenaar van de auteursrechten. Dit impliceert ook dat de HU het gebruik van software zonder het bezitten van de juiste licenties tegen gaat.

Wet Computercriminaliteit III
De Wet Computercriminaliteit III richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat “enige beveiliging” vereist is alvorens er sprake kan zijn van het eventueel strafrechtelijk vervolgen van delicten jegens de onderwijsinstelling en het eventueel vrijwaren van bestuurders van de instelling.

Naleving van dit informatiebeveiligingsbeleid en implementatie van de maatregelen zoals benoemd in de Normenkader IB Hoger Onderwijs) bij de HU leidt tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van de Wet Computercriminaliteit III.

Indien er aanvallen op HU plaatsvinden die de beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit III, zal de HU in beginsel aangifte doen, tenzij de aanval uitdrukkelijk bedoelt was om zwakke plekken in de beveiliging van de HU-systemen aan te tonen, er niet actief misbruik gemaakt is van de vastgestelde zwakheden en de HU tijdig op de hoogte is gesteld van de activiteiten en de resultaten. Het MT IM&ICT en HU-CERT-coördinator adviseren hierover aan het CvB. Het CvB kan het besluit tot aangifte nemen.

Indien de informatiemiddelen van de HU door medewerkers, studenten, partners of andere derden misbruikt voor het plegen van strafbare feiten zal de HU in beginsel aangifte doen. . Het MT IM&ICT en HU-CERT-coördinator adviseren hierover aan het CvB. Het CvB kan het besluit tot aangifte nemen.

Overige richtlijnen en landelijke afspraken
Zoals eerder gesteld, het informatiebeveiligingsbeleid bij de HU is gebaseerd op het SURF Normenkader. De HU voldoet aan de volgende richtlijnen en landelijke afspraken:

- Nederlandse gedragscode wetenschappelijke integriteit (NGWI), 2018
- Normenkader Hoger Onderwijs, 2017
- Gebruiksovereenkomst SURFnet, 2018
- Risk analysis higher education institutions, 2017

Bijlage 3: Lijst met afkortingen

AVG: Algemene Verordening Gegevensbescherming

UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming

DPIA: Data Protection Impact Assessment

EER: Europese Economische Ruimte

SCC: Standard Contractual Clause

SCIPR: SURF Community voor Informatiebeveiliging en Privacy

IVHO: Integrale Veiligheid Hoger Onderwijs

FG: Functionaris Gegevensbescherming

WHW: Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

ISO: International Organization of standardization

EC: Europese Commissie

CERT: Computer Emergency Response Team

CISO: Chief Information Security Officer

JZ: Juridische Zaken

PDCA: Plan-Do-Check-Act

BIT-consultant: Business Information Technology-consultant

AP: Autoriteit Persoonsgegevens

CSD: Centrale Service Desk

ISO: Information Security Officer