Maastricht University

Beleid Verwerking Persoonsgegevens
Universiteit Maastricht

Maastricht University

Datum: 29 mei 2018

Colofon

Dit beleid verwerking Persoonsgegevens is gebaseerd op het *Beleid Verwerking Persoonsgegevens in het Hoger Onderwijs* versie 2.0 maart 2018.

Auteurs

Raoul Winkens, Functionaris Gegevensbescherming/Data Protection Officer
Bart van den Heuvel, Corporate Information Security Officer

Inhoudsopgave

1 Inleiding

Verwerking van Persoonsgegevens is noodzakelijk voor de (bedrijfs)processen van instellingen van onderwijs en onderzoek. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van Persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en andere Betrokkenen bij de Universiteit Maastricht (hierna UM), maar ook aan de UM zelf. De UM hecht dan ook veel waarde aan het beschermen van de Persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop Persoonsgegevens worden verwerkt. Het op een juiste manier verwerken van Persoonsgegevens is de verantwoordelijkheid van het bestuur van de UM.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt de UM 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.

1.1 Definities

AVG: Algemene verordening gegevensbescherming[1]

Beheerseenheid: Zoals gedefinieerd in het Bestuurs- en Beheersreglement UM artikel 1.1 sub 1 onder m en artikel 6.2.
1. Elke faculteit vormt een beheerseenheid;
2. Het bureau en de servicecentra vormen afzonderlijke beheerseenheden;
3. Onderzoekinstituten/onderzoekscholen, onderwijsinstituten, schools en graduate schools die in een faculteit zijn ingesteld of waarvan een faculteit penvoerend is, maken deel uit van de desbetreffende facultaire beheerseenheid.

Beleid: dit beleid met betrekking tot het verwerken van Persoonsgegevens aan de UM.

Betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft.

Bijzondere Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG.

Datalek: inbreuk op de technische en organisatorische beveiliging van de UM die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Bij een datalek zijn Persoonsgegevens blootgesteld aan verlies en/of onrechtmatige Verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

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.

Functionaris Gegevensbescherming (FG) / Data Protection Officer (DPO): de persoon die door de UM is aangewezen om intern toezicht te houden op naleving van privacy wetgeving. Deze is aangemeld bij en opgenomen in het FG-register van de Autoriteit Persoonsgegevens. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie bij de UM een en ander nader uitgewerkt in de Regeling Functionaris Gegevensbescherming UM.

Gegevensbeschermingseffectbeoordeling / Data Protection Impact Assessment (DPIA): een beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

[1] De Algemene verordening gegevensbescherming is op 25 mei 2016 in werking getreden en per 25 mei 2018 van kracht.

Informatiebeveiliging: Het totaal van technische en organisatorische maatregelen die noodzakelijk zijn om de beschikbaarheid, integriteit en de vertrouwelijkheid van (persoons)gegevens te waarborgen,

Minderjarige: in het kader van privacywetgeving binnen Nederland is een minderjarige iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt.

Ontvanger:een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een Derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk van de Europese Unie NL persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn.

Persoonsgegeven: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

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 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.

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

Toestemming van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de Betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de UM Persoonsgegevens verwerkt.

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

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

1.2 Reikwijdte en doelstelling van het Beleid

Het Beleid heeft betrekking op het verwerken van Persoonsgegevens van alle Betrokkenen binnen de UM, waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur/outsourcing), alsmede op andere Betrokkenen waarvan de UM Persoonsgegevens verwerkt.

In het Beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de UM alsmede op de daaraan ten

grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het Beleid van toepassing op niet-geautomatiseerde verwerking van Persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein Informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder Persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.
Het Beleid bij de UM heeft als doel om de kwaliteit van de Verwerking en de beveiliging van Persoonsgegevens te optimaliseren, waarbij een goede balans gezocht wordt 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 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 UM.

Doelstelling van het Beleid voor de UM is concreet het volgende:

- Het bieden van een kader: het Beleid biedt een kader om (toekomstige) Verwerkingen van Persoonsgegevens te toetsen aan een vastgestelde ‘best practice’ of norm; en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.
  Het stellen van normen: de basis voor de beveiliging van Persoonsgegevens is ISO 27001.[2] Maatregelen worden op basis van ISO 27002[3] en ‘best practices’ in het hoger onderwijs genomen. Als best practices worden intern bij de UM de door de SCIPR community van SURF ontwikkelde normen- en toetsingskaders Informatiebeveiliging en Privacy gehanteerd. Het Juridisch Normenkader Cloudservices Hoger Onderwijs[4] wordt gehanteerd als best practice voor cloud services en andere outsource contracten.
- Het nemen van de verantwoordelijkheid: door het College van Bestuur door de uitgangspunten en de organisatie van de Verwerking van Persoonsgegevens vast te leggen voor de hele organisatie.
- Daadkrachtige implementatie van het beleid door de portefeuillehouder Verwerking Persoonsgegevens 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.

[2] Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging
[3] Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging
[4] https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html

2 Beleidsprincipes Verwerking Persoonsgegevens

2.1 Beleidsuitgangspunt en -principes

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 aangebracht tussen het belang van de UM om Persoonsgegevens te verwerken en het belang van Betrokkene ter eerbiediging van zijn persoonlijke levenssfeer en om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.
Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

- Een Verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 6 van de AVG (“rechtmatigheid”).
- Persoonsgegevens worden alleen verwerkt op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat het voor Betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier er Persoonsgegevens worden verwerkt. Informatie en communicatie hierover moet eenvoudig toegankelijk en begrijpelijk zijn (“behoorlijkheid en transparantie”).
- Persoonsgegevens worden alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het gaat hier om specifieke en gerechtvaardigde doeleinden, die zijn vastgelegd en omschreven voordat men begint met de Verwerking. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (“doelbinding”).
- 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 (“minimale gegevensverwerking”).
- Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (“minimale gegevensverwerking”).
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn (“juistheid”).
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen (“integriteit en vertrouwelijkheid”).
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen (“opslagbeperking”).
- Iedere Betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke Verwerkingen hem betreffende Persoonsgegevens, en heeft het recht van bezwaar, zoals geformuleerd in hoofdstuk 8 van dit Beleid.
- Bij alle Verwerkingen die gebaseerd zijn op toestemming van de Betrokkene zal het intrekken van de toestemming net zo eenvoudig zijn als het geven ervan.
- Indien het voor een specifieke toepassing niet noodzakelijk is om Persoonsgegevens te herleiden tot het individu zal zoveel mogelijk het principe van anonimiseren worden toegepast.

3 Wet- en regelgeving

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

3.1 Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

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

3.2 Algemene verordening gegevensbescherming

De UM 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 Persoonsgegevens) geïmplementeerd op basis van het Beleid. Hiermee wordt tevens uitvoering gegeven aan de Uitvoeringswet Algemene verordening gegevensbescherming.

3.3 Archiefwet

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

3.4 Telecommunicatiewet

De maatregelen die de UM genomen heeft om aan de privacywetgeving te voldoen zijn tevens toereikend om de bescherming van de persoonlijke levenssfeer van gebruikers op de openbare netwerken van de UM te waarborgen. De regelgeving van de Telecommunicatiewet met betrekking tot het bevoegd aftappen en de bewaarplicht zijn separaat geïmplementeerd.

4 Rollen en verantwoordelijkheden met betrekking tot Verwerking Persoonsgegevens

Om de Verwerkingen van Persoonsgegevens gestructureerd en gecoördineerd op te pakken wordt bij de UM een aantal rollen onderkend die aan functionarissen binnen organisatie zijn toegewezen.

4.1 College van Bestuur

Het College van Bestuur (hierna: “CvB”) is eindverantwoordelijk voor de rechtmatige en zorgvuldige Verwerking van Persoonsgegevens binnen de UM en stelt het beleid, de maatregelen en de procedures op het gebied van Verwerking vast.

4.2 Portefeuillehouder Verwerking Persoonsgegevens

De portefeuillehouder Verwerking Persoonsgegevens is het bestuurslid dat Privacy en Informatiebeveiliging in portefeuille heeft. Hij of zij is eindverantwoordelijk voor Verwerking van Persoonsgegevens binnen de UM. In de dagelijkse operatie kan de portefeuillehouder zijn Chief Information Officer (hierna: “CIO”) hiervoor mandateren.

4.3 Functionaris gegevensbescherming

De UM heeft een interne toezichthouder op de Verwerking van Persoonsgegevens aangesteld. Deze toezichthouder wordt Functionaris Gegevensbescherming genoemd (hierna: “FG”). De FG zal door de UM tijdig worden betrokken bij alle aangelegenheden waar Persoonsgegevens bij komen kijken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen de UM. De UM zal de FG aanmelden bij de toezichthoudende autoriteit.

De taken van de FG zullen inhouden:

- het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG;
- het toezien op de naleving van de AVG en andere relevante privacywetgeving.
- het toezien op de naleving van dit privacybeleid door de UM;
- het toezien op een Data Protection Impact Assessment;
- het ten minste jaarlijks rapporteren over de naleving van de AVG;
- het samenwerken met de toezichthoudende autoriteit;
- fungeren als eerste aanspreekpunt voor de toezichthoudende autoriteit.

Een en ander nader uitgewerkt in de Regeling Functionaris Gegevensbescherming UM.

4.4 Corporate Information Security Officer

De UM heeft centraal een Corporate Infomation Security Officer (hierna: “CISO”) aangesteld om advies te geven over en toezicht te houden op de Informatiebeveiliging binnen de UM.

4.5 Systeemeigenaar

De systeemeigenaar is er verantwoordelijk voor dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan het proces waar deze verantwoordelijk voor is en voldoet aan het Beleid. Dit betekent dat de systeemeigenaar er voor zorgt dat zowel nu, als in de toekomst, de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving. Bij afwijkingen wordt door de CISO/FG geadviseerd over toepasselijke maatregelen voor gebruik waarover door CIO / CvB wordt besloten.

4.6 Proces/Verwerkingseigenaar

De proces-/verwerkingseigenaar is er verantwoordelijk voor dat processen en verwerkingen voldoen aan het Beleid. Dit betekent dat de proces/verwerkingseigenaar ervoor zorgt dat zowel nu, als in de toekomst, het proces blijft beantwoorden aan wet- en regelgeving.

4.7 Leidinggevende

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

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het Beleid;
- toe te zien op de naleving van het Beleid door zijn medewerkers;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen;

4.8 Informatiemanager

De informatiemanager heeft in het kader van dit Beleid de volgende taken op het gebied van privacy en Verwerkingen van Persoonsgegevens:

- Lokale privacy officer: Binnen de elk van de vier domeinen Education, Research, Operations & Technology[5] fungeert de informatiemanager als lokaal aanspreekpunt op het gebied van privacy en Verwerkingen van Persoonsgegevens.
- De informatiemanager heeft regelmatig contact met de Functionaris Gegevensbescherming over ontwikkelingen binnen zijn domein op het gebied van privacy en Verwerkingen van Persoonsgegevens.
- De informatiemanager levert jaarlijks een bijdrage aan de rapportage van de FG over de naleving van de AVG binnen de UM.

[5] Aangezien de UM nog in een overgangsfase van werken zit, zullen de Informatiemanagers van de Beheerseenheden voorlopig deze rol vervullen.

5 Implementatie Beleid

Het CvB van de UM is verantwoordelijk voor Verwerkingen van de Persoonsgegevens waarvan zij het doel en de middelen voor de Verwerking vaststelt. Zij wordt aangemerkt als de **Verwerkingsverantwoordelijke** in de zin van de AVG. De feitelijke Verwerking van Persoonsgegevens wordt echter op allerlei lagen van de UM 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 UM, zoals , werknemers, studenten, andere afnemers en de samenleving als geheel. Een goed governance-beleid draagt zorg voor de rechten van alle Betrokkenen.

5.1 Verdeling van de verantwoordelijkheden

- Het zorgvuldig verwerken van Persoonsgegevens dient gezien te worden als **een lijn-verantwoordelijkheid**: dat betekent dat de lijnmanagers (afdelingshoofden/centrale stafdiensten) de primaire verantwoordelijk 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 te communiceren met alle relevante partijen.

- Het zorgvuldig omgaan met Persoonsgegevens is tevens **ieders verantwoordelijkheid**. Er wordt van medewerkers en studenten verwacht dat ze zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies van de UM of van Betrokkenen. Het is mede om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.

5.2 Inpassing in de instellingsgovernance /Afstemming met aanpalende beleidsterreinen

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 en gegevensbescherning. Het strategisch niveau wordt ingevuld in het I-Board. Binnen de kaders die door het CvB zijn meegegeven, is het I-board verantwoordelijk voor de implementatie en handhaving van de AVG.

Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld in het Informatiemanagersoverleg. Dit is in de huidige situatie het I4MU- overleg.

Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Het operationeel niveau wordt ingevuld in het Discipline Overleg ICT (DO-ICT).

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. Noodzakelijk is het om bij de UM het bewustzijn voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag wordt aangemoedigd.
Onderdeel van het Beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en andere Betrokkenen. Deze campagnes worden centraal aangestuurd door het CvB of haar gemandateerde(n), zo mogelijk in afstemming met andere beveiligingscampagnes en aansluitend bij landelijke campagnes in het hoger onderwijs.

Verhoging van het bewustzijn is verder de verantwoordelijkheid van de Beheerseenheden zelf, waarbij ze ondersteund worden door de FG en de Corporate Information Security Officer.

5.4 Controle en naleving

Audits maken het mogelijk het Beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de Corporate Information Security Officer en de interne auditor de controle op het rechtmatig en zorgvuldig Verwerken van Persoonsgegevens.

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 UM.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan de UM 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 organisatorische ontwikkelingen binnen en buiten de UM maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het Beleid.

6 Rechtmatige en zorgvuldige Verwerking van Persoonsgegevens

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

6.1 Grondslag

De UM verwerkt slechts Persoonsgegevens als er sprake is van een van de wettelijke gronden zoals beschreven in artikel 6 AVG:

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

De UM hanteert bij de implementatie van iedere Verwerking de principes “Privacy by Design” en “Privacy by Default”.

6.2 Privacyverklaring

De UM verwerkt Persoonsgegevens op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat de UM aan de Betrokkene inzichtelijk maakt in hoeverre en op welke manier diens Persoonsgegevens verwerkt worden. Bij het verzamelen van de Persoonsgegevens zal de UM middels een privacyverklaring de Betrokkene inlichten. Inlichting zal plaatsvinden voorafgaand aan de Verwerking, tenzij dit redelijkerwijs niet mogelijk is. Zie nader paragraaf 8.1 van dit Beleid.

6.3 De organisatie van de Informatiebeveiliging

De UM draagt zorg voor een adequaat beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer om Persoonsgegevens te beveiligen tegen verlies en/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 UM. De UM maakt hiervoor gebruik van een vastgestelde classificatie methodiek en een methode voor Gegevensbeschermingseffectbeoordeling.

6.4 Geheimhouding

Bij de UM worden alle Persoonsgegevens als vertrouwelijk geclassificeerd. Eenieder 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 kennisnemen, 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, in overeenstemming met het uitgewerkte bewaarbeleid van de UM. Persoonsgegevens dienen na het verlopen van de bewaartermijn[6] buiten het bereik van de actieve administratie gebracht te worden. De UM 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. De UM hanteert het Basisselectiedocument Wetenschappelijk Onderwijs als uitgangspunt voor bewaar- en vernietigingstermijnen.

Wanneer verwerking van een Persoonsgegeven plaatsvindt op basis van toestemming en de betrokkene trekt zijn toestemming in dan zal het Persoonsgegeven alleen nog verwerkt worden om aan een wettelijke plicht te voldoen. Bestaat een dergelijke plicht niet dan wordt het gegeven verwijderd, dan wel geanonimiseerd.

6.6 Documentatieplicht

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

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

Tevens voert de UM een Data Protection Impact Assessment uit, bij (onderzoeks)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. Als hieruit blijkt dat de Verwerking een hoog risico zou betekenen indien de UM geen maatregelen neemt om het risico te beperken, raadpleegt de UM voorafgaand aan de Verwerking, de toezichthoudende autoriteit.

6.7 Bijzondere Categorieën 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. 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.

Voor twee soorten Persoonsgegevens geldt dat zij niet onder de categorie Bijzondere Persoonsgegevens vallen, maar dat de Verwerking en beveiliging ervan wel aan strenge eisen zijn gebonden:

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

6.8 Doorgifte Persoonsgegevens

6.8.1 <u>Uitbesteden van Verwerking aan een Verwerker</u>

Indien de UM Persoonsgegevens laat verwerken door een *Verwerker*, wordt de uitvoering van Verwerkingen geregeld in een schriftelijke overeenkomst tussen de UM en de Verwerker.

[6] Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of bij formele studieresultaten, maar ze kunnen ook zijn vastgelegd door de UM, bijvoorbeeld in een overeenkomst tussen de UM en de Betrokkenen.

6.8.2 Doorgifte Persoonsgegevens binnen de Europese Economische Ruimte (hierna 'EER')

De UM verstrekt Persoonsgegevens alleen aan een Ontvanger (zijnde Verwerker, Verwerkingsverantwoordelijke of Derde) gevestigd binnen de EER, als de Verwerking is gebaseerd op een van de grondslagen voor gegevensverwerking uit artikel 6 en voldoet aan artikel 9 AVG indien nodig en als de Ontvanger voldoet aan de wettelijke vereisten uit de AVG.

6.8.3 Doorgifte Persoonsgegevens buiten de EER

De UM verstrekt Persoonsgegevens alleen aan Ontvangers die zich bevinden in een land buiten de EER, indien aan een van de volgende voorwaarden is voldaan:

1. Het derde land, gebied, welbepaalde sector in een derde land, of de internationale organisatie in kwestie biedt volgens de Europese Commissie een passend beschermingsniveau.

Als passend beschermingsniveau hanteert de UM:

- De algemene lijst van landen met passend beschermingsniveau gepubliceerd door de Europese Commissie[7];
- Het Privacy Shield voor bedrijven in de Verenigde Staten, gepubliceerd door de Europese Commissie i.s.m. de US Department of Commerce[8].

2. Doorgifte vindt plaats op basis van **passende waarborgen** uit de AVG, artikel 46 en 47.
3. Doorgifte vindt plaats op basis van een van de **wettelijke uitzonderingen** uit artikel 49 van de AVG.

6.9 Vragen- en klachtenprocedure

6.9.1 Melding en registratie

Vragen of klachten in verband met (de verwerking van) Persoonsgegevens kunnen gemeld worden bij privacy@maastrichtuniversity.nl. Van vragen of klachten met een (potentiele) significante impact, zal een register bijgehouden worden.

Vragen en klachten kunnen worden gemeld door eenieder, waaronder Betrokkenen, Verwerkers of Derden.

6.9.2 Zwakke plekken in de beveiliging

Werknemers en studenten zullen waargenomen zwakke plekken in systemen of diensten registreren en direct rapporteren bij de servicedesk ICTS van de UM. Van alle meldingen betreffende zwakke plekken in de beveiliging zal een register bijgehouden worden.

6.9.3 Afhandeling

Vragen, klachten en zwakke plekken in de beveiliging worden doorgezet naar de verantwoordelijke afdeling of persoon en vervolgens conform de daarvoor vastgestelde procedures zo snel mogelijk afgehandeld.
Als de Persoonsgegevens van Betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van de UM ernstig in gevaar zijn, wordt in ieder geval het College van Bestuur en ook de FG als Juridische Zaken op de hoogte gesteld.

[7] Deze kunt u vinden via de volgende link https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[8] Deze kunt u vinden via de volgende link https://www.privacyshield.gov/list.

6.9.4 Evaluatie

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

7 Datalekken

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

7.1 Datalek

Van een Datalek is sprake als er een inbreuk op de beveiliging van Persoonsgegevens plaatsvindt, die leidt tot enige ongeoorloofde Verwerking daarvan. Het kan hierbij bijvoorbeeld gaan om een diefstal van een laptop, een in de trein vergeten usb-stick of een e-mail die naar de verkeerde persoon is verstuurd. Alle Datalekken moeten intern gemeld worden. Sommige Datalekken moeten worden gemeld bij de toezichthoudende autoriteit binnen 72 uur na ontdekking daarvan en in sommige gevallen ook bij de Betrokkene.

7.2 Melding en registratie

Een Datalek kan bij de UM zowel binnen de eigen organisatie ontstaan, maar ook bij een door de UM ingeschakelde Verwerker. De volgende situaties moeten hierbij worden onderscheiden:

a. *Medewerker*: medewerkers moeten, indien zij een (mogelijk) Datalek waarnemen of vermoeden zelf onderdeel te zijn van een Datalek, contact opnemen met de servicedesk ICTS van de UM bij voorkeur gebruik makend van het formulier “Report possible UM data leak”[9].
b. *Verwerker:* het is ook mogelijk dat er een Datalek plaatsvindt bij een door de UM ingeschakelde Verwerker. De Verwerker zal overeenkomstig de afgesloten verwerkersovereenkomst het Datalek melden aan de UM.
c. *Andere personen:* indien een ander dan een medewerker of een Verwerker een (mogelijk) Datalek waarneemt of zelf onderdeel is van een Datalek, dient contact opgenomen te worden met de servicedesk ICTS van de UM via servicedesk-icts@maastrichtuniversity.nl.

Een melding van een (mogelijk) Datalek dient zo spoedig mogelijk te worden gemaakt. De volgende gegevens dienen doorgegeven te worden bij melding van een Datalek:

- Wie meldt er?
- Wat is er gemeld en hoe is dit gebeurd? Geef een korte samenvatting.
- Waar kwam de melding vandaan?
- Om welke data (gegevens) gaat het?[10]
- Is de data versleuteld of anderszins beveiligd?
- Welke groep mensen zijn geraakt door het incident en hoeveel personen zijn getroffen?
- Wat zijn de gevolgen van het incident voor de data?
- Welke systemen zijn betrokken bij/geraakt door het incident?
- Wanneer heeft het incident plaatsgevonden?
- Indien de melding is gedaan door een medewerker van de UM: wat is er gedaan om het incident op te lossen/in de toekomst te voorkomen?

Elk Datalek en de afhandeling daarvan zal worden bijgehouden in een register.

7.3 Afhandeling

[9] https://servicedesk.icts.maastrichtuniversity.nl/tas/public/ssp/

[10] Bijvoorbeeld: Naam, Geslacht, geboortedatum en/of leeftijd, BSN, Contactgegevens, Toegangs- of identificatiegegevens, Financiële gegevens, (Kopieën van) paspoorten of andere legitimatiebewijzen, Locatiegegevens, Gegevens over iemands gezondheid, Genetische gegevens, Biometrische gegevens.

Indien sprake is van een Datalek wordt deze conform de in de relevante wet- en regelgeving opgenomen specifieke bepalingen over Datalekken afgehandeld, zoals beschreven in de beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens[11], zodat de melding van het Datalek tijdig de juiste personen, en uiteindelijk de toezichthouder en Betrokkenen bereikt.

Als de Persoonsgegevens van Betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van de UM ernstig in gevaar zijn, wordt in ieder geval het College van Bestuur en ook de FG en Juridische Zaken op de hoogte gesteld.

7.4 Besluitvorming

Nadat er een melding heeft plaatsgevonden van een (mogelijk) Datalek overeenkomstig de voorgaande paragrafen, zal de FG een zwaarwegend advies uitbrengen omtrent de verplichting om te melden aan de toezichthoudende autoriteit en de Betrokkene. Het CvB (doorgaans middels haar gemandateerden) zal verantwoordelijk zijn voor het besluit om al dan niet de melding te maken. Bij afwijking van het advies van de FG door gemandateerde zal er altijd onmiddellijk een escalatie naar het CvB plaatsvinden voor definitieve besluitvorming.

7.5 Evaluatie

Het is van belang om te leren van Datalekken om de waarschijnlijkheid van toekomstige Datalekken te verkleinen. Registratie van Datalekken en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van Persoonsgegevens. De rapportage over Datalekken met betrekking tot Persoonsgegevens maken daarom een vast onderdeel uit van de jaarrapportage van het College van Bestuur en van de FG.

[11] Beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

8 Rechten van Betrokkenen

De AVG geeft Betrokkenen bepaalde rechten waarmee zij controle kunnen uitoefenen op de Verwerking van hun Persoonsgegevens. Een verzoek tot uitoefening van deze rechten kan digitaal worden ingediend via https://www.maastrichtuniversity.nl/nl/over-de-um/algemene-privacyverklaring-um/jouw-rechten of schriftelijk worden ingediend bij de UM via privacy@maastrichtuniversity.nl of per post via Universiteit Maastricht, Postbus 616, 6200 MD Maastricht t.a.v. de FG.

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

Melding aan Betrokkene
De UM draagt er zorg voor dat de informatie en communicatie op een beknopte, toegankelijke en begrijpelijke manier en in duidelijke en eenvoudige taal wordt verstrekt aan Betrokkene. De taal zal worden afgestemd op de doelgroep. De UM zal standaard in het Nederlands antwoorden en indien nodig in het Engels.

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

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

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

8.1 Recht op informatie

De Betrokkene heeft het recht om door de UM te worden geïnformeerd over bepaalde aspecten van de Verwerking van zijn Persoonsgegevens. De UM informeert de Betrokkene kosteloos over de Verwerking van diens Persoonsgegevens, zowel in de situatie waarin de Persoonsgegevens direct bij de Betrokkene zijn verzameld, als wanneer ze langs een andere route zijn verkregen.

A. Verkrijging direct van Betrokkene
De UM verstrekt de Betrokkene voorafgaand aan de verzameling van de gegevens, tenminste de volgende informatie indien de gegevens direct bij de Betrokkene worden verzameld:

- De identiteit en contactgegevens van de Verwerkingsverantwoordelijke en, in voorkomend geval, de FG.
- De specifieke doeleinden van Verwerking waarvoor de Persoonsgegevens zijn bestemd alsook de rechtsgrond voor de verwerking.
- De gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of Derde als de Verwerking is gebaseerd op de rechtsgrond ‘gerechtvaardigd belang’.
- In voorkomend geval, het voornemen van de Verwerkingsverantwoordelijke om de Persoonsgegevens door te geven aan een derde land, welk land dit is en op welke grond de Persoonsgegevens daarnaartoe worden verstuurd.
- De periode gedurende welke de Persoonsgegevens worden opgeslagen, of indien niet mogelijk, de criteria die dienen om deze termijnen te bepalen.
- Het bestaan van het recht om de Verwerkingsverantwoordelijke te verzoeken om inzage, rectificatie of verwijdering van de Persoonsgegevens, beperking van de hem betreffende

verwerking, alsmede het recht tegen de Verwerking bezwaar te maken en het recht op dataportabiliteit.
- Het recht om een klacht in te dienen bij de toezichthoudende autoriteit.
- De ontvangers of categorieën van ontvangers van de Persoonsgegevens.
- Indien de Verwerking is gebaseerd op de grondslag 'toestemming', het recht van de Betrokkene om die toestemming te allen tijde in te trekken.
- Of de Persoonsgegevens nodig zijn voor de uitvoering van een overeenkomst of om te voldoen aan een wettelijke verplichting.
- Of de Persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet de onderliggende logica, alsmede het belang en de te verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.

B. Verkrijging niet direct van Betrokkene

Als de Persoonsgegevens niet direct bij de Betrokkene zelf zijn verzameld maar langs een andere route, zal aan de Betrokkene, in aanvulling op de hiervoor genoemde punten, de volgende informatie worden verstrekt:
- De categorieën van Persoonsgegevens.
- De bron waar de Persoonsgegevens vandaan komen
- Deze informatie zal zo snel mogelijk, maar niet later dan vier weken, na de verkrijging van de gegevens, dan wel bij het eerste contact met de Betrokkene, worden verstrekt.

8.2 Recht op inzage

Verzoek

Iedere Betrokkene heeft het recht om te informeren of zijn Persoonsgegevens worden verwerkt en, als dat het geval blijkt, het recht op inzage in hem betreffende verwerkte Persoonsgegevens.

Mededeling

Indien gegevens worden verwerkt, bevat de mededeling van de UM een volledig overzicht van de gevraagde gegevens, dit kan mogelijk zijn:
- Een omschrijving van de doeleinden van de Verwerking.
- De categorieën van gegevens waarop de Verwerking betrekking heeft.
- Categorieën van ontvangers.
- Beschikbare informatie over herkomst van de gegevens.
- De termijn van bewaring van gegevens of indien dat niet mogelijk is, de criteria om die termijn te bepalen.
- Het recht van Betrokkene om de Verwerkingsverantwoordelijke te verzoeken om rectificatie of wissen van gegevens, beperking of bezwaar van Verwerking alsmede het recht op dataportabiliteit.
- Het recht van de Betrokkene om een klacht in te dienen bij een toezichthoudende autoriteit.
- Alle beschikbare informatie over de bron van de gegevens, als de gegevens niet bij de Betrokkene zijn verzameld.
- Of de Persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet de onderliggende logica, alsmede het belang en de verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.
- De passende waarborgen die zijn getroffen, indien de gegevens worden doorgegeven aan een derde land.

Kopie

De Betrokkene kan om een kopie van alle Persoonsgegevens verzoeken. Deze kopie dient in een gangbare elektronische vorm te worden verstrekt, tenzij het verzoek op papier is gedaan of de Betrokkene expliciet om een papieren kopie verzoekt. Het inzagerecht geeft geen aanspraak op een kopie of afschrift van het document waarop de gegevens zijn vastgelegd. Het doel van het inzagerecht is Betrokkene in staat te stellen om kennis te nemen van de Persoonsgegevens die de UM van Betrokkene Verwerkt en te controleren of ze juist zijn en rechtmatig zijn Verwerkt door de UM.

Kosten

Iedere eerste kopie kan kosteloos worden aangevraagd. Per additionele kopie zal de UM een redelijke vergoeding van administratieve kosten in rekening brengen bij de Betrokkene.

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

8.3 Recht op dataportabiliteit

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

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

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

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

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

8.4 Recht op rectificatie, aanvulling, verwijdering of beperking van de Verwerking

Verzoek tot rectificatie, aanvulling, verwijdering of beperking
Iedere Betrokkene kan met betrekking tot over hem opgenomen Persoonsgegevens bij de UM van deze gegevens verzoeken die te corrigeren, aan te vullen, te verwijderen of de Verwerking te beperken. Bij het recht op beperking worden de Persoonsgegevens tijdelijk afgeschermd en niet meer verwerkt door de UM. De beperking wordt duidelijk in het bestand aangegeven.

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

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

8.5 Recht van bezwaar

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

1. In verband met zijn of haar persoonlijke omstandigheden, mag iedere Betrokkene bezwaar maken tegen Verwerking bij de UM, als deze Verwerking plaatsvindt op grond van a) de vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag van de

Verwerkingsverantwoordelijke, of b) de behartiging van het gerechtvaardigd belang van de UM of van een Derde aan wie de gegevens worden verstrekt.

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

2. Bij een Verwerking met het doel 'direct marketing', heeft een Betrokkene te allen tijde het recht om bezwaar te maken. De UM zal bij bezwaar de Verwerking van Persoonsgegevens voor direct marketing doeleinden onmiddellijk (kosteloos) staken en gestaakt houden.

8.6 Geautomatiseerde besluitvorming

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

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

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

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

8.7 Rechtsbescherming

Algemene klachten
Indien de Betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit Beleid jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij het College van Bestuur van de UM.

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

A. <u>Bezwaar en beroep</u>

Indien de UM afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of de UM heeft het verzoek van de Betrokkene afgewezen, en het besluit van de UM is aan te merken als een besluit van een bestuursorgaan in de zin van artikel 6 lid 4 van de Awb, heeft de Betrokkene de mogelijkheid een bezwaarschriftprocedure te starten. Een bezwaarschriftprocedure moet altijd gestart worden binnen 6 weken na bekendmaking van een besluit van de UM. Tegen de beslissing op bezwaar, staat beroep open bij de rechtbank.

B. <u>Verzoekschriftprocedure bij de kantonrechter</u>

Indien de UM afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of de UM heeft het verzoek van de Betrokkene afgewezen, heeft de Betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter.

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

C. Verzoek tot handhaving bij toezichthoudende autoriteit

Indien de UM afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of de UM 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.

9 Tot slot

Dit beleid is vastgesteld door het CvB van de Universiteit Maastricht dd. 29 mei 2018, na instemming van de Universiteitsraad.
Een review van het beleid maakt onderdeel uit van de jaarlijkse plan-do-check-act cyclus van de UM. Daarin is ook een controle op de effectiviteit van de maatregelen opgenomen.

Aanpassingen van dit beleid worden aangekondigd via een Instellingsbrede email en de meest recente versie is gepubliceerd op https://www.maastrichtuniversity.nl/privacy

Voor vragen of opmerkingen met betrekking tot dit beleid kunt u terecht bij privacy@maastrichtuniversity.nl.

Versiebeheer:

Datum:	Versie:
29 mei 2018	1.0
9 oktober 2019	1.1