Richtlijn Digitale Soevereiniteit - UMC
Versie: 1.0 **Datum:** 27-02-2026|**Auteur:** [UMC, Afdeling Informatiebeveiliging/IT-beleid]

---

1. Inleiding
Deze richtlijn beschrijft de principes en kaders voor het waarborgen van digitale soevereiniteit van AUMC voor de ICT- voorzieningen, data en overige digitale assets van AUMC of waarvoor AUMC verantwoordelijk is.

Wat is digitale soevereiniteit?
Er worden verschillende definities gebruikt voor digitale soevereiniteit. De een ruimer dan de ander. Wat altijd wel terugkomt in de definities is dat het gaat om het vermogen van een land, overheid, organisatie of bedrijf om zelfstandig, onafhankelijk, zelfbesturend te beslissen over zijn/haar ICT-voorzieningen en infrastructuur, data, technologieën en overige digitale assets.

Digitale soevereiniteit betekent voor AUMC het vermogen om onafhankelijk te beslissen over de keuze, inzet, het gebruik en beheer, de beveiliging van, toegang tot, controle over de digitale ICT-voorzieningen en infrastructuur, data en overige digitale assets van UMC of waarvoor UMC verantwoordelijk is en/of die UMC gebruikt in haar bedrijfsprocessen. Dit, met inachtneming van wet- en regelgeving, ethische normen, de privacy en overige rechten van patiënten, onderzoeksdeelnemers en medewerkers etc. Vorenstaande, met het bieden van bescherming tegen het van toepassing zijn van externe jurisdicties en/of de controle en toegang van buitenlandse overheden of machten als en voor zover die niet in overeenstemming zijn of op gespannen voet staan met de nationale wet- en regelgeving, wet- en regelgeving van de Europese Unie, internationale (mensenrechten) verdragen waarbij Nederland is aangesloten of normen die horen bij een democratische rechtstaat[1].

Digitale soevereiniteit wordt in de literatuur en spraakgebruik ook opgedeeld in o.a. de volgende deelgebieden: data soevereiniteit, operationele soevereiniteit, technologische soevereiniteit. Bij gebruik van het begrip digitale soevereiniteit in dit document zijn de hiervoor genoemde deelgebieden inbegrepen. Een nadere toelichting op deze deelgebieden is aangegeven in de definities bij paragraaf 3 hieronder.

Waarom is het waarborgen van digitale soevereiniteit van AUMCnodig?
In een tijdperk van toenemende digitalisering, globalisering van IT-diensten en voortdurende ontwikkeling van nieuwe technologieën is het cruciaal dat AUMCde controle behoudt over haar data, digitale ICT-infrastructuur/voorzieningen en overige digitale assets. Dit is essentieel voor de continuïteit, vertrouwelijkheid

[1] Normen van een democratische rechtsstaat zijn onder andere rechtsgelijkheid, rechtszekerheid, scheiding der machten en democratische besluitvorming. Dit betekent dat alle burgers gelijk behandeld worden voor de wet, dat overheidsmacht beperkt en gebonden is aan regels, dat de macht is verdeeld over verschillende organen, en dat burgers invloed hebben op politieke beslissingen via vrije verkiezingen.

en integriteit van onze kerntaken: hoogwaardige patiëntenzorg, baanbrekend wetenschappelijk onderzoek, academisch onderwijs en maatschappelijke valorisatie en voor het kunnen beschermen van de (privacy)rechten van de patiënten, onderzoeksdeelnemers, medewerkers, stagiaires, studenten en overige personen van wie AUMCpersoonsgegevens verwerkt.

Het is van belang om in het vizier te hebben dat digitale soevereiniteit niet altijd volledig te realiseren is. Ten aanzien van digitale systemen, ICT-voorzieningen, data, en overige assets van AUMC die volledig op eigen locaties en in eigen beheer zijn, zal digitale soevereiniteit makkelijker volledig kunnen worden gewaarborgd. AUMC kan in deze gevallen makkelijk zelf onafhankelijk hierover beslissen, maar in de gevallen waarbij AUMC gebruik maakt of moet maken van digitale ICT-voorzieningen of diensten van derden kan dat moeilijker zijn. In deze gevallen kan wel op een risico gebaseerde wijze de digitale soevereiniteit voor een groot deel worden gewaarborgd door o.a. per dienst of leverancier de risico's te identificeren en daarvoor passende technische, organisatorische beheersmaatregelen te treffen, waaronder contractuele afspraken (bijvoorbeeld over eigendom en gebruik van data, gegevenslocatie, toegang door derden, beveiliging en exit-mogelijkheden).

Doordat o.a. Informatie- en communicatietechnologie (ICT) niet een kernactiviteit is van [Naam UMC], de complexiteit van technologie toeneemt, er een chronisch tekort is aan (gespecialiseerd) ICT-personeel, en de kosten voor ICT, incl. dataverwerking en opslag steeds toenemen, is AUMC deels genoodzaakt om haar ICT uit te besteden aan gespecialiseerde partijen (vaak hyperscaler (buitenlandse) bedrijven) die schaalbare en flexibele ICT-oplossingen kunnen aanbieden tegen lagere kosten. Dit heeft wel een keerzijde in de zin dat er afhankelijkheid ontstaat van derden waaraan wordt uitbesteed, wat op gespannen voet kan komen te staan met het waarborgen van de digitale soevereiniteit. Uitbesteding aan derden leidt tot afhankelijkheid van derden, verlies van controle en ruimte om zelf te beslissen en keuzes te maken. Dit kan risico's met zich meebrengen op o.a. het gebied van continuïteit van bedrijfsvoering, beveiliging, compliance, exit (vendorlock-in). Ook ontstaat het risico van toegang tot en controle over onze data door overheden van andere landen die mogelijk niet handelen overeenkomstig wet- en regelgeving van Nederland en de Europese Unie, Internationale mensenrechten verdragen en/of normen van een democratische rechtstaat. Dit besef heeft geleid tot de uitwerking van deze richtlijn digitale soevereiniteit. Deze richtlijn geeft handvatten om door middel van risico gebaseerde benadering – zoals terug te vinden in de Europese digitale wetgeving – de digitale soevereiniteit van AUMC zoveel mogelijk te waarborgen.

Ook bij de Nederlandse overheid en de Europese Unie is het besef van het belang van digitale soevereiniteit doorgedrongen. De Nederlandse overheid en de Europese Unie zetten maatregelen in gang om (ook voor de toekomst) de digitale soevereiniteit van Nederland en de Europese Unie te waarborgen.[2]

2. Doelstellingen

Deze richtlijn heeft als doel:

a) Het definiëren van de principes van digitale soevereiniteit van AUMC.
b) Het minimaliseren van (rest)risico's gerelateerd aan externe afhankelijkheden op het gebied van ICT en gebruik van overige digitale technologieën[3].
c) Het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van data en ICT-voorzieningen van AUMC of waarvoor AUMC verantwoordelijk is.
d) Het ondersteunen van een risicogebaseerde benadering bij de inkoop en implementatie van ICT-voorziening en/of IT-dienstverlening.

---

[2] - De Nederlandse digitaliseringsstrategie De Nederlandse Digitaliseringsstrategie)
- Digitaal kompas 2030: de Europese aanpak voor het digitale decennium- Brussel, 9.3.2021/COM(2021) 118 final (EUR-Lex - 52021DC0118 - EN - EUR-Lex)

[3] Digitale technologieën zijn technologieën die digitale data (informatie die is opgeslagen als enen en nullen) kunnen lezen, verwerken, opslaan en overdragen. Dit omvat een breed scala aan technologieën, zoals computers, smartphones, software, het internet, en ook geavanceerdere toepassingen als kunstmatige intelligentie (AI), het Internet of Things (IoT), en cloud computing. Het doel is om informatie efficiënter te verwerken en te delen.

e) Het bevorderen van transparantie en controle over verwerking van data, waaronder persoonsgegevens.

3. Definities

De begrippen aangegeven in de definities hieronder, hebben ook indien zij in deze richtlijn met een kleine letter aanvangen, dezelfde betekenis als aangegeven in de definities hieronder.

a) **Digitale soevereiniteit:** Het vermogen van AUMC om onafhankelijk te opereren en controle uit te oefenen over data, ICT- voorzieningen, en digitale technologieën van [Naam UMC], die AUMC gebruikt of waarvoor AUMC verantwoordelijk is en de vrijheid om daarover te beslissen en daarin keuzes te maken, inclusief keuzes over in te schakelen leveranciers en partners waarmee samen wordt gewerkt. Dit impliceert ook onafhankelijkheid van en bescherming tegen controle door externe jurisdicties, buitenlandse overheden of machten (inclusief bescherming tegen hun toegang tot data en ICT-voorzieningen van AUMC als en voor zover dat in strijd is of op gespannen voet staat met de wetgeving van Nederland en de Europese Unie en ethische principes (waaronder de normen van de democratische rechtstaat).

b) **Data:** alle gegevens waaronder persoonsgegevens volgens de AVG en overige informatie in digitale of fysieke vorm.

c) **Data-soevereiniteit:** verwijst naar de controle over de opslag, verwerking, toegang en zeggenschap over de verwerking van data van AUMC of waarvoor AUMC verantwoordelijk is. Het waarborgt dat data onderworpen is en blijft aan de regels van de jurisdictie waaronder AUMC valt.

d) **Operationele soevereiniteit:** de mate waarin AUMC of een door AUMC ingeschakelde leverancier op instructie van AUMC of een samenwerkende partner van AUMC(mede) ten behoeve van AUMC controle heeft over de operationele processen van AUMC of waarvoor AUMC verantwoordelijk is, om zo de digitale soevereiniteit van AUMC te waarborgen. Dit omvat o.a. toezicht op en het uitvoeren van updates, patches en incidentmanagement.

e) **Technologische soevereiniteit:** de mate waarin AUMC continuïteit en controle over haar technologische toekomst kan waarborgen. Het betreft de noodzaak voor langdurige autonomie bij het gebruik van specifieke technologieën.

f) **Kritieke data (verwerking):** gegevens(verwerking) en/of processen die op basis van de BIV-classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid) als hoog- of zeer hoog-risicovol of hoog + medisch zijn aangemerkt. Dit betreft met name bijzondere persoonsgegevens (zoals medische gegevens), gevoelige onderzoekdata, overige privacygevoelige gegevens, intellectueel eigendom en strategische bedrijfsinformatie. Niet alle persoonsgegevens of financiële gegevens zijn automatisch kritisch; leidend is de classificatie volgens de regels van de UMCNL Standaard Dataclassificatie en -labelling, binnen de UMCNL vastgestelde richtlijn voor Data Governance.

g) **Kritieke infrastructuur:** IT-systemen en diensten die essentieel zijn voor de primaire processen van AUMC(patiëntenzorg, onderzoek, onderwijs en bedrijfsvoering).

h) **AVG**: Algemene verordening gegevensbescherming.

i) **DPIA:** Data Protection Impact Assessment, namelijk: een gegevensbeschermingseffectbeoordeling bedoeld in artikel 35 van de AVG.

j) **ICT- voorzieningen**: alles dat kan worden gerekend tot of onderdeel uitmaakt van het geheel van alle ICT-voorzieningen die nodig zijn om de bedrijfsprocessen van AUMC te laten draaien (inclusief de ICT-infrastructuur) en alles op het gebied van informatie- en communicatietechnologie dat wordt gebruikt bij de bedrijfsprocessen van AUMC(dit kan zijn de tastbare hardware, zoals computers, servers, als de immateriële software en diensten, zoals softwaretoepassingen, netwerken en cloudopslag); en digitale technologieën.

k) **Ongeoorloofde doorgifte van data:**

1) doorgifte van persoonsgegevens die niet voldoet aan de AVG;
2) doorgifte in strijd met het kennisveiligheidsbeleid van UMC;
3) doorgifte van data aan partijen in externe jurisdicties of landen met overheden waar Intellectuele eigendomsrechten mogelijk niet worden geëerbiedigd of die als statelijke actor worden genoemd in het dreigingsbeeld van nationale coördinator terrorismebestrijding en veiligheid (DBSA).

Onder doorgifte van persoonsgegevens of data wordt ook gerekend het toegang verschaffen tot de data aan een partij van buiten de EER (inclusief remote access).

l) **EER:** Europese Economische Ruimte: de lidstaten van de Europese Unie plus drie landen van de Europese Vrijhandelsassociatie (EVA): IJsland, Liechtenstein en Noorwegen.

4. Principes van Digitale Soevereiniteit

De volgende principes vormen de basis van de digitale soevereiniteitsstrategie van [Naam UMC]:

4.1 Data Lokalisatie, toegang tot data en controle (Data-soevereiniteit):

a) **Standaard locatie voor kritieke data**: Kritieke data dienen binnen de EER te worden opgeslagen en verwerkt, met uitsluiting van toegang tot de data door partijen buiten de EER, waar de digitale soevereiniteit van AUMC mogelijk niet kan worden gewaarborgd. Dit, om te waarborgen dat de data uitsluitend onderworpen is aan de regels van de Europese Unie en Nederland en daarbuiten niet verblijft. Het gaat hier bijvoorbeeld om fysieke datalokalisatie die geen bescherming biedt tegen extraterritoriale wetgeving (zoals de Amerikaanse CLOUD Act), indien VS leveranciers betrokken zijn die vallen onder de Cloud Act. Bij de selectie van leveranciers moet daarom hiermee nadrukkelijk rekening worden gehouden en moeten beheersmaatregelen worden getroffen om te zorgen persoonsgegevens worden verwerkt volgens de eisen van de wetgeving van Nederland en de Europese Unie, waaronder de AVG.

b) **Locatie voor niet kritieke data:** ook niet kritieke data moet bij voorkeur worden opgeslagen en verwerkt binnen de Europese Unie.

c) De opslag en verwerking van data (ongeacht of het kritieke data is of niet) moet te allen tijde voldoen aan de eisen van wet- en regelgeving en beleid van AUMC die daarop van toepassing is.

d) **Transparantie over de verwerkingsketen van de data en de ICT-infrastructuur**: Er dient volledige transparantie te zijn over de achterliggende onderaannemers/leveranciers/verwerkers/ samenwerkende partijen die de data zullen verwerken, inclusief die daartoe toegang zullen hebben, hun identiteit en verwerkingsactiviteit m.b.t. de data en de ICT-voorzieningen die zij daarvoor zullen gebruiken, de fysieke locatie(s) van (verwerking van) de data, locaties/landen vanuit waar betrokken partijen toegang kunnen hebben tot de data, de jurisdicties van de betreffende locaties/landen. Dit is nodig om in control te zijn, teneinde te kunnen voldoen aan de van toepassing zijnde wettelijke eisen, zoals de AVG-informatieplicht om de betrokkenen tot wie data herleidbaar is te informeren, de AVG-verwerkingsregisterplicht, om risico's van datalekken te kunnen beheersen, cybersecurity, beveiliging te kunnen onderzoeken en voorkomen en de nodige beheersmaatregelen daarvoor te kunnen treffen en om schadelijke of nadelige invloed of toegang en/of controle van buitenlandse overheden of machten te voorkomen.

e) **Zeggenschap op data:** AUMC behoudt te allen tijde zeggenschap over de data waarvoor AUMC verantwoordelijk is en/of verwerkingsverantwoordelijke is volgens de AVG en moet te allen tijde in staat zijn haar AVG-plichten die gelden voor persoonsgegevens en overige plichten van privacybescherming na te komen, ongeacht waar de data wordt opgeslagen of verwerkt.

f) **Bevordering bewustwording medewerkers.** AUMC draagt zorg voor de bevordering van de bewustwording van medewerkers over digitale soevereiniteit, over wat AUMC verstaat onder digitale soevereiniteit, de inhoud van deze richtlijn en geeft haar medewerkers handvatten die zij kunnen hanteren en de nodige middelen om de digitale soevereiniteit van AUMC te waarborgen.

4.2. Leveranciersmanagement en afhankelijkheid (Operationele soevereiniteit):

a) **Leveranciersdiversiteit**: AUMC houdt rekening met een beperking van overmatige afhankelijkheid van één enkele leverancier voor kritieke IT-diensten of componenten.

b) **Due diligence**: Voorafgaand aan het sluiten van contracten over een ICT-voorziening en de implementatie van de ICT-voorziening is een due diligence vereist bij de selectie van IT-leveranciers, waarbij niet alleen functionaliteit, kosten, financiële stabiliteit en vermogen om te kunnen leveren en de eisen van de AVG worden beoordeeld, maar ook de aspecten van digitale soevereiniteit, inclusief de bescherming tegen externe jurisdicties en schadelijke of nadelige invloeden van buitenlandse overheden of machten[4].

c) **Contractuele afspraken**: Contracten met (IT)-leveranciers dienen expliciete clausules te bevatten over: zeggenschap op data- datalokalisatie, bescherming van persoonsgegeven en overige privacyrechten, beschermende maatregelen tegen mogelijke ongeoorloofde doorgifte van data naar en/of toegang daartoe van partijen buiten de EER, beveiliging, auditrechten, exit-strategieën en naleving van de wetgeving van Nederland en de Europese Unie. De clausules dienen ook de van toepassing zijnde risico's

[4] Tijdens een risicobeoordeling dient altijd gecontroleerd te worden of een land of instelling is opgenomen op de EU-sanctielijst. Daarnaast is het advies om bij deze beoordeling gebruik te maken van de ervaringen en controles die intern gehanteerd worden binnen het domein kennisveiligheid. Daarnaast dient te worden voldaan de doorgifte eisen van de AVG.

en beheersmaatregelen genoemd in uitgevoerde risico assessments (waaronder DPIA's) en due diligence te bevatten.

4.3. Technologische Onafhankelijkheid en Open Standaarden (Technologische soevereiniteit):

a) **Interoperabiliteit:** Voorkeur wordt gegeven aan oplossingen die gebaseerd zijn op open standaarden en die interoperabiliteit met andere (delen van de) ICT-voorzieningen bevorderen, om vendor lock-in te voorkomen.

b) **Het recht op audit:** De mogelijkheid om technologieën, inclusief de broncode van kritieke software te auditeren op kwetsbaarheden en ongewenste functionaliteiten, dient te worden gewaarborgd.

c) **Exit-strategieën:** Bij elke investering in een ICT-voorziening dient voor zover van toepassing een duidelijke exit-strategie te zijn, inclusief dataportabiliteit, procedures voor data-export en migratie naar alternatieve oplossingen/ICT-voorzieningen.

4.4. Risicomanagement en Compliance:

a) **Risicogebaseerde aanpak:** De implementatie van ICT-voorzieningen, dient gebaseerd te zijn op een risicoanalyse die de impact op digitale soevereiniteit beoordeelt. Indien bij of in verband met de voorgenomen implementatie van een ICT-voorziening - waaronder ook valt wijziging of aanpassing daarvan - persoonsgegevens (zullen) worden verwerkt, dient er een DPIA of ander risico assessment voor de verwerking van de persoonsgegevens te worden uitgevoerd, overeenkomstig het beleid van AUMC en de AVG, tenzij dat volgens het privacybeleid van AUMC niet nodig is.

b) **Wettelijke compliance:** Elke ICT-voorziening die AUMC gebruikt en de daarbij behorende processen en verwerking van persoonsgegevens, ongeacht of die zich intern of extern bevinden, moeten voldoen aan de toepasselijke wetgeving van Nederland en de Europese Unie en aan het beleid van [Naam UMC].

c) **Beveiliging:** robuuste informatiebeveiliging is een integraal onderdeel van digitale soevereiniteit. ICT-voorzieningen en data dienen adequaat beschermd te worden tegen ongeoorloofde toegang, diefstal, verlies, verminking of verstoring.

5. Verantwoordelijkheden

a) **Raad van Bestuur:** Eindverantwoordelijk voor de vaststelling, implementatie en naleving van deze richtlijn.

b) **CIO/CISO:** Verantwoordelijk voor de ontwikkeling, implementatie en het toezicht op deze richtlijn en bijbehorende procedures. Adviseert de Raad van Bestuur.

c) **Afdeling Inkoop:** Verantwoordelijk voor de integratie van digitale soevereiniteitsprincipes in het inkoopproces en bij de contractonderhandelingen.

d) **IT-afdeling:** Verantwoordelijk voor de technische implementatie, beheer en monitoring van IT-systemen, conform deze richtlijn.

e) **Afdeling Juridische Zaken:** Adviseert over wettelijke kaders en contractuele clausules.

f) **De Functionaris Gegevensbescherming** adviseert over de privacybescherming overeenkomstig de AVG en overige van toepassing zijnde sectorale privacyregelgeving en het privacybeleid van AUMC en houdt intern toezicht op de naleving van de AVG.

g) **Medewerkers (zowel in dienst als ingehuurd):** Verantwoordelijk voor het naleven van deze richtlijn bij het gebruik van IT-systemen en de verwerking van data in hun dagelijkse werkzaamheden.

h) CISO en Raad van Bestuur laten zich voor de ontwikkeling van deze richtlijn voor wat betreft de verwerking van persoonsgegevens, adviseren door de Functionaris Gegevensbescherming. Ook de overige vorengenoemde verantwoordelijken laten zich – indien nodig - voor wat betreft de verwerking van persoonsgegevens, adviseren door de Functionaris Gegevensbescherming in verband met de naleving van deze richtlijn.

i) **Non-compliance:** Het hoofd of de directeur van de afdeling of organisatieonderdeel van AUMC die intern verantwoordelijk is voor data of een betreffend ICT-voorziening, draagt er zorg voor dat bij non-compliance met deze richtlijnen, in het volgende wordt voorzien voorafgaand aan de aanvang van de verwerking van de betreffende data en/of implementatie de betreffende ICT-Infrastructuur:

- Dat er beheersmaatregelen worden geformuleerd en gedocumenteerd om de aan de non-compliance verbonden risico's te voorkomen en/of te mitigeren.

- Dat als een restrisico die niet met beheersmaatregelen kan worden voorkomen of gemitigeerd, wordt geaccepteerd, de noodzaak voor het accepteren van het restrisico's steekhoudend wordt onderbouwd en gedocumenteerd. Ingeval kritieke data daarbij is betrokken, informeert hij de Raad van Bestuur van AUMC schriftelijk hierover en zorgt hij dat hij goedkeuring verkrijgt van de Raad van Bestuur van [Naam UMC], als dat nodig is volgens het beleid van [Naam UMC].

6. Toepasbaarheid

Deze richtlijn is van toepassing op dienstverlening, data of producten die ingezet worden bij processen en ICT-voorzieningen die geclassificeerd zijn op Beschikbaarheid Hoog en/of Integriteit Hoog en/of Vertrouwelijkheid Hoog of Hoog + Medisch. Deze richtlijn doet geen afbreuk aan de eisen van de AVG of andere wet-of regelging of het beleid van AUMC van toepassing op dienstverlening, data of producten die ingezet worden bij processen en ICT-voorzieningen en waarop de classificatie van Beschikbaarheid Hoog en/of Integriteit Hoog en/of Vertrouwelijkheid Hoog of Hoog Medisch niet van toepassing is.

6. Uitwerking op Kerntaken en overige gebieden

6.1 Algemeen

a) Absolute prioriteit voor bescherming van persoons van patiënt, onderzoekdeelnemer, medewerker, student, stagiair, bezoeker etc. of bedrijfsvertrouwelijke gegevens (V – hoog)

b) Systemen of dienstverlening die geclassificeerd zijn op Beschikbaarheid en/of Integriteit en/of Vertrouwelijkheid Hoog of gebruikt worden in processen met deze classificatie dienen maximaal onder eigen beheer te staan of via leveranciers die aan de hoogste digitale soevereiniteits- en beveiligingsstandaarden voldoen.

c) Bijzondere persoonsgegevens dienen te worden verwerkt binnen de EER waarbij toegang tot de persoonsgegevens door partijen buiten de EER, waar de digitale soevereiniteit van AUMC mogelijk niet kan worden gewaarborgd,[5] zoveel mogelijk wordt uitgesloten.

d) Gegevensuitwisseling met externe partijen dient altijd via beveiligde, gecontroleerde kanalen plaats te vinden en te voldoen aan de EER-lokalisatievereiste of voorkeur, zoals aangegeven in deze richtlijn (waaronder ook valt geen toegang tot de data door partijen buiten de EER), tenzij expliciete uitzonderingen zijn vastgesteld en goedgekeurd door de interne verantwoordelijke van AUMC die daartoe bevoegde is.

6.2. Wetenschappelijk Onderzoek:

a) Erkenning van de noodzaak tot internationale samenwerking, maar met behoud van controle en zeggenschap over (gevoelige) onderzoekdata en intellectueel eigendom.

b) Data-soevereiniteit in onderzoekscontext betekent afspraken over controle en zeggenschap over data, toegangsrechten en de jurisdictie van dataopslag en -verwerking.

6.3. Academisch Onderwijs:

a) Keuze voor leermiddelen en platforms moeten voldoen aan de AVG en zoveel mogelijk de principes van digitale soevereiniteit ondersteunen.

b) Bewustwording creëren bij studenten en docenten over het belang van digitale soevereiniteit en databescherming.

6.4. Valorisatie:

a) Bescherming van intellectueel eigendom en commercieel gevoelige informatie die voortkomt uit onderzoek en innovatie.

b) Duidelijke afspraken over controle en zeggenschap over data en het gebruik van data bij spin-offs en samenwerkingsverbanden.

[5]Tijdens een risicobeoordeling dient altijd gecontroleerd te worden of een land of instelling is opgenomen op de EU-sanctielijst. Daarnaast is het advies om bij deze beoordeling gebruik te maken van de ervaringen en controles die intern gehanteerd worden binnen het domein kennisveiligheid. Daarnaast dient te worden voldaan de doorgifte eisen van de AVG.

c) Zorgen dat commerciële afspraken met externe partijen, de digitale soevereiniteit van het UMC niet ondermijnen.

6.5. Bedrijfsvoering

Digitale soevereiniteit is eveneens van toepassing op ondersteunende bedrijfsprocessen zoals financiën, HR, facilitaire zaken, inkoop en ICT. Hierbij gelden de volgende specifieke overwegingen:

a) **Technologische Onafhankelijkheid:** Streef naar technologische onafhankelijkheid door vendor lock-in te minimaliseren en exit-strategieën te waarborgen voor ICT-voorzieningen die in de bedrijfsvoering worden gebruikt.
b) **Compliance:** Zorg dat alle ICT-voorzieningen en diensten voor bedrijfsvoering voldoen aan van toepassing zijnde wetgeving van Nederland en van de Europese Unie.

6.6. Sturing en Verantwoording

De functie van sturing en verantwoording, waaronder governance, compliance, auditing en strategische besluitvorming, is fundamenteel en vereist specifieke aandacht voor digitale soevereiniteit:

a) **Data:** Informatie die ten grondslag ligt aan strategische beslissingen en governance dient maximaal te zijn beschermd tegen ongeoorloofde toegang en ongeoorloofde doorgifte of invloed van buitenlandse overheden.
b) **Onafhankelijkheid van Governance Processen:** ICT-voorzieningen voor governance en besluitvorming (bijv. managementinformatie, documentmanagement) moeten een hoge operationele soevereiniteit bezitten om onafhankelijke sturing te waarborgen.
c) **Audit- en Controlemogelijkheden:** De technische inrichting van ICT-voorzieningen voor sturing en verantwoording moet onafhankelijke audits mogelijk maken, met transparantie over gebruikte technologieën en toegang tot logs.
d) **Bescherming van Intellectueel Eigendom:** Systemen die gevoelige strategische plannen of intellectueel eigendom bevatten, dienen robuust beveiligd te zijn, waarbij technologische soevereiniteit een rol speelt in de autonomie over de hostingmiddelen.

7. Handhaving en Monitoren

a) Deze richtlijn zal periodiek worden geëvalueerd en bijgewerkt om te blijven voldoen aan nieuwe ontwikkelingen, wetgeving en technologische inzichten.
b) Er zal door de Raad van Bestuur een monitoringproces worden ingericht om de naleving van deze richtlijn te controleren, inclusief audits van IT-leveranciers en interne ICT-voorzieningen. Dit monitoringsproces wordt vastgelegd in beleid waarin tevens de handhavingsbevoegdheden en verantwoordelijkheden intern bij AUMC worden belegd. De instemming van de Ondernemingsraad zal moeten worden verkregen voor het monitoringsbeleid. Verder zal het monitoringsbeleid worden gecommuniceerd aan de medewerkers van AUMC.
c) Overtredingen kunnen leiden tot disciplinaire maatregelen en/of juridische stappen, conform het geldende beleid van AUMC.