GEGEVENSBESCHERMINGSBELEID

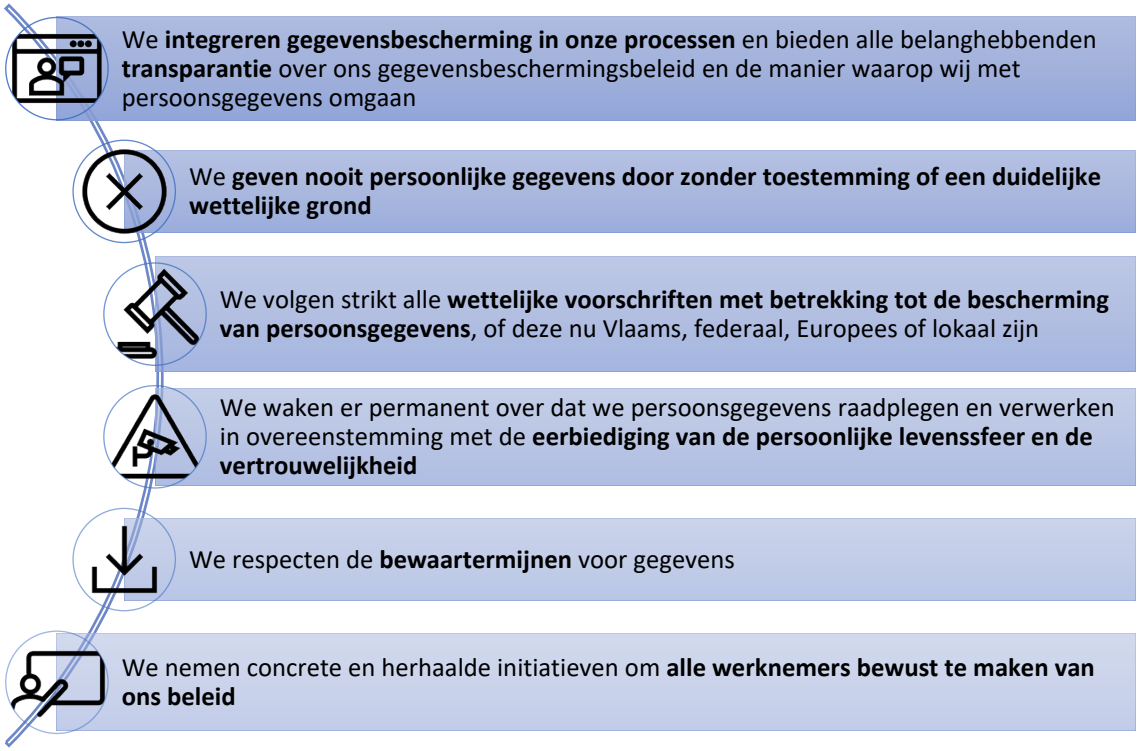
[NL] [EN]

1. Inleiding - Beleidsverklaring

Het ITG streeft naar wetenschappelijke vooruitgang in de tropische geneeskunde en de volksgezondheid door middel van wetenschappelijk onderzoek, gespecialiseerde opleidingen en door het verlenen van medische, wetenschappelijke en sociale diensten. Deze activiteiten vereisen dat het ITG in aanzienlijke mate persoonsgegevens verwerkt.

Gewetensvolle toepassing van de wet en strenge kwaliteitsnormen zijn enkele van de kernwaarden waarnaar wij leven. Het ITG gegevensbeschermingsbeleid maakt dan ook actief deel uit van deze kwaliteitsnormen en van de kwaliteitscultuur van het ITG. Het veilig, eerlijk, transparant en adequaat omgaan met patiënten informatie, deelnemers aan wetenschappelijk onderzoek, informatie over onze studenten en medewerkers, en andere relevante stakeholders is een voorwaarde voor het leveren van kwaliteitszorg in al onze activiteiten en voor het opbouwen en behouden van vertrouwen. Wij besteden de grootst mogelijke aandacht aan de bescherming van de privacy van alle betrokkenen en aan het bieden van veilige oplossingen voor de informatietechnologie (IT)-omgeving voor de verwerking van persoonsgegevens.

Wij houden ons aan de volgende beleidsdoelstellingen



De volledige beleidsverklaring gegevensbescherming kan [HIER] worden geraadpleegd.

Als ITG werken we allemaal samen om de beginselen van het gegevensbeschermingsbeleid toe te passen.

In dit beleid vertalen wij de bovengenoemde doelstellingen in beginselen, concrete termen en maatregelen voor de aanpak ervan op een aantal beleidsterreinen. Deze maatregelen zijn opgenomen in een gegevensbeschermings- en informatieveiligheidsplan, waarop wordt toegezien door de functionaris voor gegevensbescherming (DPO) en het IT diensthoofd, en dit onder de dagelijkse verantwoordelijkheid van de algemeen beheerder.

2. TOEPASSINGSGEBIED VAN HET BELEID

Dit beleid is van toepassing op alle persoonsgegevens zoals gedefinieerd door de AVG (of GDPR), met inbegrip van maar niet beperkt tot de persoonsgegevens van (ex-)werknemers, sollicitanten, consultants, stagiaires, leveranciers, bezoekers, zakelijke contacten, patiënten, deelnemers aan onderzoek in binnen- en buitenland, donoren van menselijke stalen die door het ITG worden verwerkt, docenten, studenten, (onderzoeks)partners, enz. Alle medewerkers en studenten van het ITG moeten dit beleid respecteren wanneer zij persoonsgegevens verwerken in het kader van hun professionele activiteiten voor het ITG. Dit geldt zowel voor de verwerking van persoonsgegevens via elektronische toepassingen als voor de verwerking van persoonsgegevens op papier.

Dit beleid is van toepassing op de verwerking van persoonsgegevens binnen en buiten de Europese Economische Ruimte (EER), waarvoor ITG optreedt als verwerkingsverantwoordelijke, gezamenlijk verwerkingsverantwoordelijke of als verwerker.

3. WETGEVING

Dit beleid is in overeenstemming met, en geeft uitvoering aan de Europese Algemene Verordening Gegevensbescherming 2016/679 (“AVG” of "GDPR"). Het heeft tot doel de "rechten en vrijheden" van natuurlijke personen te beschermen en er met name voor te zorgen dat persoonsgegevens niet onrechtmatig of zonder hun medeweten worden verwerkt, en, waar van toepassing, dat deze met hun toestemming worden verwerkt.

Dit gegevensbeschermingsbeleid is ook in overeenstemming met de Belgische wet gegevensbescherming van 30 juli 2018.

Wanneer gegevens buiten Europa worden verzameld, bv. voor onderzoek dat in het buitenland wordt uitgevoerd, moet erop worden toegezien dat aan alle wettelijke voorschriften in dat land wordt voldaan (bv. POPIA in Zuid-Afrika).

Bovendien, en relevant voor het specifieke domein, is het beleid in overeenstemming met de Belgische Wet Patiëntenrechten, de Kwaliteitswet, de Wet Klinische Proeven, relevante CAO's zoals CAO 81, de camerawet, sectorale normen, enz.

4. VERANTWOORDELIJKHEDEN

Dit beleid is van toepassing op:

- Alle werknemers van het ITG die persoonsgegevens verwerken;

- externe partijen zoals onderaannemers, verwerkers, consultants, adviseurs, extern onderwijzend personeel, onderzoekspartners, enz. die in naam van het ITG persoonsgegevens verwerken;
- Studenten voor zover zij persoonsgegevens verwerken onder de verantwoordelijkheid van, of in samenwerking met, het ITG.

De **Raad van Bestuur** keurt het gegevensbeschermingsbeleid goed.

De **directeur, de algemeen beheerder** en **de departementshoofden** bevorderen en stimuleren actief het gegevensbeschermingsbeleid. Zij formuleren antwoorden en nemen beslissingen met betrekking tot de adviezen van de DPO.

De diensthoofden en al wie een leidinggevende of toezichthoudende functie uitoefent, zijn verantwoordelijk voor het toezicht op de naleving van het gegevensbeschermingsbeleid.

In het bijzonder de **hoofdarts** en **de diensthoofden van de onderzoeksdiensten** zien toe op de adequate bescherming van gezondheidsgerelateerde of anderszins gevoelige gegevens die worden verwerkt voor medische zorg of wetenschappelijk onderzoek.

De **IT-dienst** en **het Project Management Office** (PMO) ontwikkelen of helpen bij de ontwikkeling van nieuwe ICT-oplossingen in het ITG. In die functie zien zij erop toe dat de beginselen inzake gegevensbescherming en Privacy-by-Design worden nageleefd. Vragen in verband met gegevensbescherming of informatiebeveiliging worden besproken met respectievelijk de DPO of het IT diensthoofd.

De **DPO** is verantwoordelijk voor het waarborgen van en toezien op de tenuitvoerlegging van de wetgeving inzake gegevensbescherming in het beleid en de procedures van het ITG. De DPO biedt hulp en advies bij de verwerking van persoonsgegevens. Hij of zij is ook het aanspreekpunt voor de Gegevensbeschermingsautoriteit.

Werknemers/personeelsleden zijn verantwoordelijk voor de naleving van de wetgeving inzake gegevensbescherming en het huidige gegevensbeschermingsbeleid voor hun specifieke functie en werktaken.

Niet-ITG-personeel of externen zoals contractanten, gasten, stagiairs, tijdelijke werknemers, enz. moeten op de hoogte worden gebracht van de vereisten inzake gegevensbescherming en vertrouwelijkheid die gelden voor hun taken en activiteiten die zij namens het ITG verrichten.

5. BEGINSELEN INZAKE GEGEVENSBESCHERMING EN DE TOEPASSING ERVAN BIJ HET ITG

Elke verwerking van persoonsgegevens moet worden uitgevoerd in overeenstemming met de gegevensbeschermingsbeginselen zoals beschreven in artikel 5 van de AVG. Alle beleidslijnen en procedures van het ITG zijn ontworpen om de naleving van de beginselen te waarborgen.

5.1 Rechtmatigheid, eerlijkheid en transparantie

Persoonsgegevens moeten op **transparante wijze** worden verwerkt met inachtneming van alle toepasselijke wetten, regelingen en voorschriften. Persoonsgegevens moeten **rechtmatig en eerlijk**

worden verwerkt en de betrokkenen moeten altijd worden **geïnformeerd** over welke persoonsgegevens van hen worden verwerkt en voor welke doeleinden. Dit staat los van de vraag of de persoonsgegevens direct of indirect bij de betrokkene worden bekomen (artikelen 13 & 14 van de AVG) en van deze verplichting kan alleen worden afgezien in specifieke, gemotiveerde en goedgekeurde omstandigheden (bv. wanneer er bij wet een geheimhoudingsplicht is of wanneer dit is toegestaan door een Gegevensbeschermingsautoriteit).

De volgende informatie moet aan de betrokkenen worden verstrekt:

- De identiteit van de verantwoordelijke voor de verwerking en de contactgegevens van de DPO;
- De welomschreven doeleinden van de verwerking van persoonsgegevens, met inbegrip van eventuele toekomstige doeleinden;
- De rechtmatige basis voor de verwerking (zie hieronder);
- De betrokken categorieën van persoonsgegevens;
- De ontvangers of categorieën van ontvangers van de persoonsgegevens, indien van toepassing;
- De bewaartermijnen (of de criteria die worden gebruikt om de bewaartermijn te bepalen);
- Het recht om te verzoeken om toegang, rectificatie, portabiliteit, verwijdering of om bezwaar te maken tegen de verwerking, of een uitleg over hoe en wanneer deze rechten niet kunnen uitgeoefend worden;
- In voorkomend geval, het voornemen om persoonsgegevens door te geven aan een ontvanger in een derde land en het door het betrokken land geboden beschermingsniveau;
- Alle verdere informatie die nodig is om een eerlijke verwerking te garanderen.

De wijze van informatieverstrekking aan de betrokkenen kan variëren en dient te worden afgestemd op de context van de gegevensverwerking, bv.:

- Door middel van een privacybeleid voor het gebruik van websites (zoals het privacybeleid van de ITG website) of specifieke toepassingen zoals een LIMS
- Door middel van contractuele overeenkomsten, zoals een arbeidsovereenkomst, een verwerkersovereenkomst, het examen- en onderwijsreglement voor studenten, enz.
- Door middel van een informatieblad/formulier voor geïnformeerde toestemming, privacyverklaringen en openbare registers voor wetenschappelijke studies
- Door middel van een centraal contactpunt voor de betrokkenen, d.w.z. voor ITG: informatieveiligheid@itg.be/

De privacyverklaring voor ITG werknemers, het GDPR-register en de arbeidsovereenkomst beschrijven hoe de persoonsgegevens van werknemers worden verwerkt en wat hun rechten zijn met betrekking tot die verwerkingen.

Verder moet elke verwerking van persoonsgegevens een **rechtmatige grondslag** of **een wettelijke basis** hebben voor de verwerking van de persoonsgegevens.

De rechtmatige grond voor elke verwerking van persoonsgegevens moet worden vermeld in de aan de betrokkenen verstrekte informatie en in het GDPR-register (zie “6. GDPR-register” onder).

De GDPR definieert 6 rechtmatige gronden voor de verwerking van persoonsgegevens:

I. Contractuele overeenkomst

Deze rechtmatige grond kan worden gebruikt voor de verwerking van persoonsgegevens van de contractpartijen en hun werknemers. Het is de voornaamste rechtsgrond voor de verwerking van persoonsgegevens van werknemers zoals geregeld in de arbeidsovereenkomst, bv. voor de salarisverwerking, het beheer van personeelsdossiers, het aanbieden van extralegale voordelen, interne werking, enz. Zij kan ook worden gebruikt voor de verwerking van persoonsgegevens van partners - zoals onderzoekers - in onderzoeksconsortia of studenten die deelnemen aan master- of postdoctorale opleidingen van het ITG.

II. Toestemming

Wanneer de gegevensverwerking gebaseerd is op toestemming van de betrokkene of, in het geval van minderjarigen of handelingsonbekwame personen, van de wettelijke vertegenwoordiger, moet uit een *vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting* blijken dat de betrokkene door middel van een verklaring of een duidelijk bevestigende handeling instemt met de verwerking van de hem betreffende persoonsgegevens. De verstrekte informatie moet adequaat zijn om de betrokkenen te informeren in een taal die voor hen begrijpelijk is. Toestemming houdt ook in dat deze te allen tijde kan worden ingetrokken. Toestemming moet uit vrije wil worden gegeven, hetgeen betekent dat onder dwang of op basis van misleidende informatie verkregen toestemming geen geldige grondslag voor verwerking zal vormen.
Wanneer het gaat om kwetsbare personen, zoals minderjarigen, of personen die niet in staat zijn een geïnformeerde toestemming te geven, moet een gevolmachtigde toestemming van de wettelijke vertegenwoordiger worden verkregen. Voorts worden de toestemmingsprocedure en -documenten voor wetenschappelijk onderzoek waarbij menselijke deelnemers, gegevens of lichaamsstalen betrokken zijn, door een ethisch comité (EC) en het Institutional Review Board (IRB) van het ITG getoetst, en kan niet met het onderzoek worden begonnen voordat goedkeuring is verkregen.
Om toestemming te kunnen aantonen, moet er sprake zijn van actieve communicatie tussen de betrokken partijen. Toestemming kan niet worden afgeleid uit het feit dat niet op een mededeling is gereageerd. Voor ***gevoelige gegevens moet uitdrukkelijke schriftelijke toestemming*** worden verkregen, tenzij er een alternatieve rechtmatige grondslag voor de verwerking bestaat. Toestemming is meestal verplicht voor de publicatie van foto's van personen, het versturen van nieuwsbrieven, het gebruik van gegevens voor niet-gerelateerde secundaire doeleinden, enz.
Voor wetenschappelijk onderzoek met menselijke deelnemers, gegevens en menselijke lichaamsstalen is toestemming niet altijd de meest geschikte rechtsgrond voor de verwerking van persoonsgegevens van deelnemers, ook al is een ethische toestemming (zoals goedgekeurd door de betrokken EC/IRB) vereist voor deelname aan onderzoek.

III. Wettelijke verplichting

ITG voert ook gegevensverwerkingsactiviteiten uit die moeten gebeuren uit wettelijke meldingsplicht, zoals de onmiddellijke of periodieke melding van bepaalde infectieziekten (zoals hiv, tuberculose, gonorroe), doorgifte van werknemersgegevens aan de Rijksdienst voor Sociale Zekerheid (RSZ), de Rijksdienst voor Arbeidsvoorziening (RVA), de collectieve verzekering, of de noodzaak om gegevens van onderzoekers door te geven aan het Vlaams departement Economie, Wetenschap en Innovatie (EWI). De melding van ernstige ongewenste voorvallen bij klinische proeven aan de nationale regelgevende instanties zal ook een wettelijke verplichting als rechtsgrond hebben.

IV. Publiek (of algemeen) belang

Deze wettelijke basis kan worden toegepast wanneer de gegevensverwerking gerechtvaardigd of noodzakelijk is in het belang van de samenleving, bijvoorbeeld wetenschappelijk onderzoek dat leidt tot een toename van kennis en begrip in de wetenschap.
Bijgevolg is dit een belangrijke rechtsgrond voor het ITG als instelling voor academisch onderzoek en onderwijs. Zij kan echter niet pro forma worden toegepast en verschillende criteria kunnen helpen bij het bepalen van het algemeen belang als geschikte grondslag, zoals:

- Het onderzoek levert een belangrijke bijdrage aan de (bio-)medische, klinische wetenschappen of de volksgezondheid, direct of indirect.
- Het onderzoek wordt gefinancierd met overheidsmiddelen (zoals van het FWO, BOF, HORIZON EUROPE, enz.)
- Onderzoeksresultaten worden openlijk toegankelijk gemaakt volgens de FAIR-beginselen.

De rechtsgrondslag voor gegevensverwerking kan niet het algemeen belang zijn indien de resultaten uitsluitend aan een andere partij worden overgedragen en de verworven kennis uitsluitend voor particuliere belangen is bestemd (bv. commerciële studies).

V. Vitaal belang

Dit betekent het vitale belang van de betrokkene of van een andere natuurlijke persoon, bijvoorbeeld in geval van noodsituaties.

VI. Gerechtvaardigd belang

ITG kan als organisatie een gerechtvaardigd belang hebben om persoonsgegevens te verwerken. Voorbeelden hiervan zijn de verwerking van elektronische gebruiksgegevens van werknemers om de IT- en netwerkbeveiliging te waarborgen, camera's voor beveiligingsdoeleinden, of de verwerking van patiënten- of studentengegevens om het beleid, de dienstverlening of de kwaliteit te verbeteren.
Wanneer deze wettelijke basis wordt gebruikt, moet zorgvuldig worden beoordeeld en gedocumenteerd dat de legitieme belangen van het ITG niet zwaarder wegen dan de rechten en vrijheden van de betrokkenen. De DPO helpt bij het uitvoeren van een dergelijke privacy risicoanalyse.

5.2 Specifieke, expliciete en legitieme doeleinden

Persoonsgegevens die voor een specifiek doel zijn verkregen, mogen niet worden gebruikt voor een doel dat verschilt van het hoofddoel en dat redelijkerwijs niet door de betrokkenen kan worden verwacht (beginsel van "finaliteit"). Vaak, maar niet altijd, moet toestemming van de betrokkene worden verkregen voor gegevensverwerkingen die geen deel uitmaken van het primair doel. Zo mogen studentenlijsten zonder hun toestemming niet voor marketingdoeleinden worden gebruikt.

Belangrijke leidinggevende functies in het ITG hebben een bijzondere verantwoordelijkheid om erop toe te zien dat de verwerking van persoonsgegevens in overeenstemming is met dit beginsel.

Wetenschappelijk onderzoek kan - in bepaalde omstandigheden - als een verenigbaar doel worden beschouwd wanneer het hoofddoel geen onderzoek is, d.w.z. dat het wordt uitgevoerd op basis van gegevens die oorspronkelijk zijn verkregen voor routinematige zorg voor patiënten of voor toezicht op besmettelijke ziekten. In dat geval moet het verdere gebruik van de gegevens voor wetenschappelijke studies op zijn minst een **redelijke verwachting** van de betrokkenen zijn. Overeenkomstig het transparantiebeginsel moeten de betrokkenen vooraf worden geïnformeerd over de mogelijkheid van een dergelijke verwerking. Andere factoren, zoals het nut voor de volksgezondheid, de aan de verwerkingsverantwoordelijke verleende bevoegdheid om wetenschappelijk onderzoek te verrichten, het specifieke onderzoeksgebied, de gevoeligheid van de gegevens of de kwetsbaarheid van de betrokkenen zijn belangrijke factoren bij de beoordeling van de verenigbaarheid en het verdere gebruik van gegevens voor wetenschappelijk onderzoek.

5.3 Adequate, relevante en beperkte gegevensverwerking

Er mogen niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is om het beoogde doel te bereiken (beginsel van "proportionaliteit" en "gegevensminimalisering"). Dit beginsel wordt ook toegepast in de "privacy-by-design"-methodologie voor software en systemen voor persoonsgegevens.

Voor onderzoeksdoeleinden moeten persoonsgegevens ofwel anoniem worden verzameld, ofwel bij de eerste gelegenheid worden geanonimiseerd of ten minste gepseudonimiseerd. De sleutel waarmee de gepseudonimiseerde gegevens aan de identificeerbare gegevens kunnen worden gekoppeld, moet overeenkomstig het informatiebeveiligingsbeleid op een afzonderlijke plaats worden bewaard.

Voorbeelden:

- Bij de registratie van bezoekers mogen geen overbodige persoonsgegevens worden verzameld, zoals bijvoorbeeld de geboortedatum of het huisadres van de betrokkene.
- Onderzoekers mogen in enquêtes geen vragen stellen die niet relevant zijn voor de onderzoeksvraag. Ze moeten de leeftijd verzamelen in plaats van geboortedatum waar mogelijk; enz.

5.4 Nauwkeurig, up-to-date en tijdige correctie en vernietiging

Persoonsgegevens die door het ITG worden opgeslagen, moeten regelmatig worden gecontroleerd en zo nodig bijgewerkt. Er worden geen persoonsgegevens bewaard tenzij redelijkerwijs kan worden aangenomen dat zij accuraat zijn (bv. gegevens van werknemers en studenten).

Het moet voor de betrokkenen duidelijk zijn hoe zij hun gegevens kunnen laten bijwerken. Bij voorkeur wordt hun de mogelijkheid geboden om hun gegevens zelf bij te werken in toepassingen waartoe zij toegang hebben, of is er een proces dat bijwerking mogelijk maakt, of wordt hun een contactpersoon meegedeeld waar zij hun persoonsgegevens kunnen laten bijwerken. In registratie- of aanvraagformulieren kan een verklaring worden opgenomen dat de verzamelde gegevens juist zijn op de datum van indiening en dat het in hun belang is dat de bewaarde gegevens up-to-date zijn.

5.5 De betrokkene kan slechts worden geïdentificeerd zolang als nodig

Persoonsgegevens worden niet langer bewaard dan nodig is voor de gegevensverwerking. Bewaartermijnen voor (persoons)gegevens zijn vastgelegd in retentieschema's, archiveringsprocedures, of het GDPR-register. Zodra de bewaartermijn is verstreken, moeten persoonsgegevens ofwel veilig worden vernietigd, ofwel, indien toegestaan, volledig worden geanonimiseerd of geaggregeerd (bv. voor verdere statistische, wetenschappelijke of beleidsdoeleinden).

Wanneer databanken of elektronische toepassingen worden ontworpen of aangeschaft, moet de (geautomatiseerde) verwijdering van gegevens na het verstrijken van de bewaartermijnen als een vereiste worden beschouwd.

5.6 Passende beveiliging

Persoonsgegevens worden verwerkt op een wijze die een passende beveiliging en vertrouwelijkheid waarborgt, en die voorkomt dat onbevoegden toegang krijgen tot persoonsgegevens. Bij het bepalen van passende technische en organisatorische maatregelen ter bescherming van de gegevens wordt rekening gehouden met de hoeveelheid, de gevoeligheid, de (reputatie)schade voor de betrokkenen en het ITG. De maatregelen moeten in overeenstemming zijn met het informatieveiligheidsbeleid van het ITG.

We passen volgende organisatorische maatregelen toe:

- Interne beleidslijnen en procedures zoals het gegevensbeschermingsbeleid, het informatieveiligheidsbeleid, het research data sharing beleid en het archiveringsbeleid bevatten de passende beschermingsmaatregelen.
- ITG heeft een DPO aangesteld.
- ITG-medewerkers worden bewust gemaakt van en regelmatig opgeleid in gegevensbescherming en cyberbeveiliging. Master- en doctoraatsstudenten krijgen opleiding en achtergrondinformatie over ethiek en gegevensbescherming.
- Alle werknemers, in het bijzonder die in leidinggevende functies, zijn zich bewust van hun rol en verantwoordelijkheden met betrekking tot gegevensbescherming.
- Extern personeel, contractanten, onderzoeks- en onderwijspartners zijn op de hoogte van of opgeleid in de omgang met persoonsgegevens.
- Interne organen zien toe op de vereisten rond gegevensbescherming en privacy, zoals het Institutional Review Board voor onderzoekstudies, het Data Access Comité voor toegang tot gegevens, de Doctoraatscommissie, de onderwijsdiensten, het Project Management Office voor de implementatie van nieuwe IT-oplossingen, enz.
- Onze overeenkomsten en contracten met derden bevatten passende clausules inzake vertrouwelijkheid en gegevensbescherming.
- We hebben een duidelijke procedure voor het melden van inbreuken op gegevens, voor het beperken van de gevolgen en voor escalatie, en wij documenteren de follow-up in geval van niet-naleving van de maatregelen.
- We evalueren periodiek onze gegevensverwerkingsactiviteiten door middel van interne en externe audits.
- We coördineren met externe regelgevende instanties zoals de Gegevensbeschermingsautoriteit, het IVC of externe adviesorganen zoals de VLIR AVG-werkgroep.

Technische maatregelen ter bescherming van gegevens en informatie omvatten standaard passende netwerk- en apparaatbeveiliging, fysieke toegangscontrole tot ruimten, lockers en apparaten, op rol gebaseerde toegang, multifactor authenticatie (MFA), wachtwoordbescherming of versleuteling van gevoelige gegevens in rust en transfer, beveiligde back-upopslag en beveiligde vernietiging van gegevens.

De toegang van gebruikers wordt zoveel mogelijk toegewezen op basis van het "need-to-know"-principe. De toegang tot databanken en toepassingen mag niet onevenredig permissief zijn en deze vereiste wordt dwingender naarmate de gevoeligheid van de gegevens toeneemt.

Wanneer gegevensverwerkers namens ITG persoonsgegevens verwerken, worden de minimale technische en organisatorische maatregelen die de verwerker in acht moet nemen, nader omschreven in een verwerkingsovereenkomst.

5.7 Verantwoordingsplicht

ITG garandeert en toont aan dat de gegevensbeschermingsvoorschriften worden nageleefd door middel van duidelijke en gedocumenteerde traceerbaarheid, bv. door registers bij te houden van gegevensverwerkingsactiviteiten, gegevensinbreuken, verwerkers, verzoeken om toegang tot gegevens, opleidingslogboeken, enz.

6 GDPR-REGISTER

In overeenstemming met de AVG legt het ITG een register aan van alle verwerkingsactiviteiten van persoonsgegevens waarvoor het de verwerkingsverantwoordelijke is, en houdt dit register actueel. Dit register dient meerdere doelen:

- Ondersteuning van de verantwoordingsverplichtingen tegenover toezichthoudende autoriteiten;
- Als interne inventaris van gegevensverwerkingsactiviteiten en documentatie/controle van de naleving van de wettelijke voorschriften, zoals het waarborgen van passende rechtsgronden voor gegevensverwerking en gegevensdoorgifte, overzichten van verwerkers en de noodzaak van gegevensverwerkingsovereenkomsten, de noodzaak van een gegevensbeschermingseffectbeoordeling, enz.

De DPO is verantwoordelijk voor de conformiteit van het register voor de verwerking van persoonsgegevens met de wettelijke voorschriften en voor het algemene beheer van het register zoals vastgelegd in de registerprocedure.

7 RECHTEN VAN BETROKKENEN

Betrokkenen hebben de volgende rechten met betrekking tot hun persoonsgegevens en de gegevens die over hen zijn verzameld:

Het recht op informatie

- Informatie over welke persoonsgegevens worden verwerkt en met welk(e) doel(en) dit gebeurt, wordt op duidelijke en transparante wijze verstrekt

Het recht op inzage

- De betrokkenen hebben het recht om toegang te vragen tot, of een kopie te ontvangen van de gegevens die wij over hen verwerken

Het recht op rectificatie

- Indien de gegevens niet correct of niet meer actueel zijn, kunnen de betrokkenen verzoeken om ze te verbeteren, aan te vullen of te wissen

Het recht op beperking van de verwerking

- Wanneer aan bepaalde criteria is voldaan, kunnen betrokkenen verzoeken om de verwerking van hun persoonsgegevens (tijdelijk) stop te zetten. Dit criterium kan ook de beperking van profilering of geautomatiseerde besluitvorming omvatten

Het recht op overdraagbaarheid

- Of het recht om hun gegevens over te dragen aan een andere verwerkingsverantwoordelijke van hun keuze (in machineleesbare vorm)

Het recht op verwijdering (het "recht om vergeten te worden")

- Bijvoorbeeld wanneer verwerking niet langer nodig is of de betrokkene zijn toestemming voor gegevensverwerking intrekt

Het is belangrijk erop te wijzen dat niet alle rechten altijd door de betrokkene kunnen worden uitgeoefend. De AVG vereist maximale bescherming en autonomie van de betrokkenen en zij moeten al die rechten kunnen uitoefenen waarvan niet kan worden afgeweken op specifieke gronden, zoals wettelijke verplichtingen om gegevens te verwerken of te bewaren, of zorgvuldig beoordeelde gerechtvaardigde redenen. De rechten en de uitzonderingen daarop moeten worden vastgesteld voordat met de gegevensverwerking wordt begonnen en moeten duidelijk zijn voor de betrokkenen.

Dit gebeurt bijvoorbeeld door middel van

- Privacyverklaringen voor patiënten, studenten en werknemers op onze website;
- Contractuele overeenkomsten met inbegrip van gegevensbeschermingsclausules;
- Informatiebladen en formulieren van geïnformeerde toestemming voor deelnemers aan onderzoek;
- Toepassingen voor privacy-by-design die subjecten controle bieden over hun eigen persoonsgegevens, de verwerking en het wissen ervan.

Met name wanneer de gegevensverwerking op de rechtmatige grond van toestemming berust, hebben de betrokkenen het recht die toestemming in te trekken, hetgeen betekent dat de persoonsgegevens niet verder mogen worden verwerkt of moeten worden gewist indien geen andere rechtmatige grond de bewaring van de persoonsgegevens rechtvaardigt.

Betrokkenen hebben het recht om vragen te stellen over, of een klacht in te dienen bij het ITG over de verwerking van hun persoonsgegevens. Deze procedure is laagdrempelig waarbij informatie en een contactpunt gemakkelijk vindbaar en beschikbaar zijn (zoals telefonisch of per e-mail bij de DPO (+32 3 247 07 43 of informatieveiligheid@itg.be), de algemene klachteninbox (klachten@itg.be), het IRB (irb@itg.be), of door rechtstreeks een klacht in te dienen bij ombudspersonen, secretariaten, onthaal of medewerkers rechtstreeks).
Voorts hebben betrokkenen het recht om klachten over de gegevensverwerking in te dienen bij de nationale Gegevensbeschermingsautoriteit, wat ook consequent wordt vermeld in privacyverklaringen, enz.

8 VERWERKING VAN BIJZONDERE CATEGORIEËN PERSOONSGEGEVENS

De verwerking van bijzondere categorieën van persoonsgegevens (ook wel "gevoelige gegevens" genoemd, zoals gezondheidsgegevens, etnische of raciale gegevens, justitiële of seksuele gegevens) is verboden, tenzij een aanvullende wettelijke basis kan worden gevonden als genoemd in artikel 9 van de AVG.

Belangrijke uitzonderingen op dit verbod zijn voor het ITG het verlenen van medische zorg aan patiënten en verwerking ten behoeve van statistisch, historisch en wetenschappelijk onderzoek.

Telkens wanneer het ITG gevoelige persoonsgegevens verwerkt, worden aanvullende maatregelen genomen, zoals:

- strengere veiligheidsmaatregelen (zoals strikte toegang op een "need-to-know"-basis, MFA, encryptie van gegevens, in overeenstemming met het informatieveiligheidsbeleid);
- De beschikbaarheid van bijgewerkte lijsten van personen die toegang hebben tot de persoonsgegevens;
- Patiëntgerelateerde gegevens en gegevens van klinische proeven worden verwerkt in gevalideerde en kwaliteitsgecontroleerde systemen, met inbegrip van audit trail en nominale privacy logging;
- Gezondheidsgegevens worden verwerkt onder de verantwoordelijkheid van een arts of een beoefenaar van de gezondheidszorgberoepen;
- Voor secundair gebruik van persoonlijke gezondheidsgegevens van Belgische betrokkenen kan een machtiging van het IVC nodig zijn.

9 GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Wanneer de verwerking van persoonsgegevens een waarschijnlijk groot risico inhoudt voor de rechten en vrijheden van natuurlijke personen, voert het ITG een gegevensbeschermingseffectbeoordeling (ofwel Data Processing Impact Assessment - DPIA) uit om de aard en de mogelijke impact van dergelijke risico's te beoordelen. Dit wordt beschreven in de DPIA-procedure.

Met de resultaten van de beoordeling wordt rekening gehouden bij het bepalen van passende beveiligings- en privacymaatregelen.

Wanneer een DPIA bevestigt dat de verwerking een hoog risico inhoudt dat niet op bevredigende wijze kan worden beperkt, moet de Gegevensbeschermingsautoriteit worden geconsulteerd voordat de verwerking aanvangt.

Alle onderzoeksprotocollen die ter beoordeling en goedkeuring bij het IRB worden ingediend, moeten een online privacytoets doorlopen, inclusief een voorlopige DPIA check.

Voor elk type gegevensverwerking dat door het ITG wordt uitgevoerd, adviseert de DPO of een DPIA noodzakelijk is.

10 GEGEVENSOVERDRACHTEN

10.1 Betrokkenheid van verwerkers

Wanneer een gegevensverwerker wordt ingeschakeld, moet in ieder geval voorafgaand aan de gegevensverwerking door de verwerker een verwerkersovereenkomst worden ondertekend. In de verwerkersovereenkomst wordt bepaald met welk doel en op welke wijze de gegevens precies kunnen worden verwerkt, welke beveiligingsmaatregelen minimaal moeten worden getroffen, wie toegang heeft tot de gegevens, hoe lang de gegevens mogen worden bewaard en onder welke voorwaarden gegevens door subverwerkers mogen worden verwerkt.

10.2 Gezamenlijke verwerkingsverantwoordelijken

Indien twee of meer voor de verwerking verantwoordelijken gezamenlijk beslissen over de middelen en het doel van de gegevensverwerking, treden zij op als gezamenlijk voor de verwerking verantwoordelijke. Dit is vaak het geval in consortia of partnerschappen voor wetenschappelijk onderzoek, maar kan ook voorkomen in elke vorm van transmurale samenwerking, zoals consortia van biobanken of gegevensopslagplaatsen, partnerschappen in het onderwijs, enz.

Wanneer het ITG mee optreedt als gezamenlijke verwerkingsverantwoordelijke zal het er door middel van een regeling voor zorgen dat de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijken duidelijk zijn vastgelegd, in het bijzonder wat betreft de transparantie ten aanzien van, en de uitoefening van de rechten van de betrokkenen.

10.3 Overdrachten buiten de EER

De AVG zorgt voor uniforme beschermingsregels die het vrije verkeer van persoonsgegevens binnen de Europese Economische Ruimte (EER) vergemakkelijken. Doorgifte van persoonsgegevens naar landen buiten de EER of internationale organisaties is alleen toegestaan als dat derde land of die internationale organisatie een "passend beschermingsniveau" voor de verwerking van persoonsgegevens kan garanderen. De Europese Commissie heeft voor een aantal landen reeds een adequaatheidsbesluit genomen waarin wordt bevestigd dat het land een passend beschermingsniveau biedt. De meest recente lijst van landen is hier te vinden.

Indien een land niet voorkomt op de lijst van besluiten waarbij een passend beschermingsniveau is vastgesteld, is de doorgifte van persoonsgegevens alleen mogelijk in een van de volgende gevallen:

- de opname van standaardclausules inzake gegevensbescherming, zoals de modelcontractbepalingen van de EU, in overeenkomsten die wij sluiten met organisaties uit derde landen.
- Er is een uitdrukkelijke toestemming van de betrokkenen voor de occasionele doorgifte van gegevens. De betrokkenen moeten ook worden geïnformeerd over de risico's die deze doorgifte voor hen kan inhouden.
- De doorgifte betreft een uitzonderlijke situatie, die in overeenstemming is met de bepalingen van artikel 49 van de AVG.

10.4 Overdrachten naar andere verwerkingsverantwoordelijken

Wanneer persoonsgegevens worden doorgegeven aan een derde die als verantwoordelijke voor de verwerking optreedt, is het van essentieel belang ervoor te zorgen dat er een passende wettelijke basis bestaat die deze doorgifte rechtvaardigt, aangezien de derde op zijn beurt volledig

verantwoordelijk zal worden voor het beheer van de persoonsgegevens. Vaak zal een dergelijke doorgifte gebaseerd zijn op een wettelijke verplichting (doorgifte aan agentschappen, volksgezondheidsinstellingen, ...), openbaar belang voor het delen van (geanonimiseerde) gegevens voor secundair wetenschappelijk onderzoek of toestemming van de deelnemer.

Dergelijke doorgiften moeten - samen met de secundaire doeleinden - bekend zijn bij de betrokkenen.

10.5 Delen van gegevens voor secundair onderzoek

ITG is vastberaden om te voldoen aan de FAIR principes van open access tot onderzoeksgegevens. Hierdoor kunnen resultaten door onafhankelijke onderzoekers worden geverifieerd en kan secundair onderzoek worden verricht ten behoeve van de volksgezondheid overal ter wereld.

Omdat de bescherming van de privacy van onderzoeksdeelnemers en patiënten van cruciaal belang is, kan het toegankelijk maken van onderzoeksgegevens die persoonsgegevens bevatten, enkel gebeuren binnen de grenzen van de Europese en Belgische wetgeving inzake gegevensbescherming. We houden ons dan ook aan de uitspraak "Zo open als mogelijk, zo gesloten als nodig".

De regels voor het beschikbaar stellen van gegevens voor secundair onderzoek en hoe dit op een privacy-verantwoorde manier kan gebeuren, zijn vastgelegd in het ITG data sharing beleid. Aanvragen voor toegang tot gegevens worden beoordeeld door het ITG Data Access Comité.

Bovendien is voor de doorgifte van Belgische (gepseudonimiseerde en niet-anonieme) gezondheidsgerelateerde persoonsgegevens voor secundair onderzoek a priori toestemming nodig van het IVC - en eventueel van de betrokken IRB/EC indien deze gegevens oorspronkelijk om andere redenen zijn verzameld en/of zonder toestemming van de proefpersoon voor toekomstig onderzoek.

11 BEHEER VAN INBREUKEN IN VERBAND MET PERSOONSGEGEVENS

Elke persoon die een mogelijk gegevenslek opmerkt, is verplicht dit onmiddellijk per e-mail (informatieveiligheid@itg.be) of telefoon aan de DPO te melden. In geval van twijfel is het aanbevolen het steeds te melden.

Inbreuken in verband met persoonsgegevens zijn gebeurtenissen met een potentiële of daadwerkelijke impact op de vertrouwelijkheid van persoonsgegevens. Dergelijke inbreuken kunnen onder meer bestaan uit accidentele of kwaadwillige ongeoorloofde toegang tot persoonsgegevens, intern of extern. Het ITG voorziet in een centrale en gestandaardiseerde meldingsprocedure voor haar personeel, partners en contractanten met betrekking tot de melding van datalekken. De noodzaak om datalekken onmiddellijk te melden en volgens welke procedure is opgenomen in alle verwerkingsovereenkomsten die wij sluiten en andere overeenkomsten voor zover relevant.

Wanneer het ITG optreedt als verwerkingsverantwoordelijke voor de gelekte gegevens, beoordeelt de DPO (samen met de informaticadienst en/of andere betrokken personeelsleden) de ernst, de context en de omstandigheden van de inbreuk, teneinde verdere mitigerende of preventieve maatregelen vast te stellen. Zij adviseren het management over de vraag of de inbreuk in verband

met persoonsgegevens aan de betrokkenen en/of de toezichthoudende autoriteit moet worden gemeld.

Indien het ITG optreedt als verwerker van de gelekte gegevens, stelt het de verwerkingsverantwoordelijke van de gegevens onverwijld in kennis van de inbreuk, samen met een voorlopige beschrijving (zoals hoeveelheid, identificeerbaarheid, context, omstandigheden, enz.).

VOORBEELDEN VAN DATALEKKEN
Gevoelige documenten op de printer laten liggen
E-mail adressen van ontvangers van een nieuwsbrief in CC zetten
Het verlies van persoonsgegevens aan cybercriminelen als gevolg van phishing of hacking
Verlies van een USB-drive, smartphone of laptop met vertrouwelijke gegevens (tenzij versleuteld)
Het opnemen van (indirect) identificeerbare gegevens in een open access gegevensbank
Het versturen van vertrouwelijke informatie naar een foutief e-mail adres
Het intentioneel gebruiken van studenten- of patiëntencontactgegevens voor niet-toegestane doeleinden

12 AFKORTINGEN

AVG	Algemene Verordening Gegevensbescherming (of General Data Protection Regulation)
BOF	Bijzondere Onderzoeksfinanciering
CAO	Collectieve Arbeidsovereenkomst
DAC	Data Access Comité
DPIA	Data Processing Impact Assessment (of Gegevensbeschermingseffectbeoordeling)
DPO	Functionaris voor gegevensbescherming (Data Protection Officer)
EC	Ethisch Comité
EER	Europese Economische Ruimte
FAIR	Vindbaar - Toegankelijk - Interoperabel – Herbruikbaar (Findable – Accessible – Interoperable – Reusable)
FWO	Fonds voor Wetenschappelijk Onderzoek
GDPR	General Data Protection Regulation (of Algemene Verordening Gegevensbescherming)
IRB	Institutional Review Board (van het ITG)
IVC	Informatieveiligheidscomité
MFA	Multifactor authenticatie
POPIA	Wet Bescherming Persoonsgegevens (Zuid-Afrika)
VLIR	Vlaamse Interuniversitaire Raad

13 DEFINITIES

Anonimisering - Anonimisering is een gegevensverwerking waarbij de persoonsgegevens niet langer in verband kunnen worden gebracht met een geïdentificeerde of identificeerbare natuurlijke persoon zonder gebruikmaking van middelen die redelijkerwijs niet te voorzien zijn (en dus redelijkerwijs onomkeerbaar zijn).

Verwerkingsverantwoordelijke - De natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of een ander orgaan die, alleen of samen met anderen, het doel van en de middelen voor de verwerking

van persoonsgegevens bepaalt. Indien twee of meer partijen samen verantwoordelijk zijn voor een gegevensverwerkingsactiviteit, worden zij gezamenlijke verwerkingsverantwoordelijken genoemd.

Betrokkene - De natuurlijke persoon van wie de persoonsgegevens worden verwerkt.

Persoonsgegevens - Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. 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.

Verwerking (van persoonsgegevens) - 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.

Verwerker - Een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander lichaam dat ten behoeve van de voor de verwerking verantwoordelijke persoonsgegevens verwerkt.

Pseudonimisering - Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Bijzondere categorieën persoonsgegevens (of gevoelige gegevens) - Alle persoonsgegevens met betrekking tot ras, etniciteit, gezondheid of medische toestand, seksueel leven/voorkeuren, politieke, filosofische of religieuze overtuigingen, lidmaatschap van vakbonden, genetische, biometrische, gerechtelijke of genetische gegevens.

Derde (partij) - Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

14 AUTEURSCHAP EN GOEDKEURING

Opgesteld door	Jef Verellen - Functionaris voor gegevensbescherming
Goedgekeurd door	ITG Raad van Bestuur tijdens haar vergadering van 23/05/2022

DATA PROTECTION POLICY

[NL] [EN]

1 INTRODUCTION – POLICY STATEMENT

ITM pursues scientific advances in tropical medicine and public health through scientific research, specialized training and by providing medical, scientific and social services. These activities require ITM to process personal data to a considerable extent.

Conscientious application of the law and stringent quality standards are some of the core values we live by. ITM's data protection policy therefore forms an active part of these quality standards and of ITM's quality culture. The secure, fair, transparent and adequate handling of patient information, scientific research participants, information on our students and staff, and other relevant stakeholders is a prerequisite for providing quality care in all our activities as well as building and retaining trust. We pay the utmost attention to protect the privacy of all concerned and to provide secure information technology (IT) environment solutions for processing personal data.

WE LIVE BY THE FOLLOWING POLICY OBJECTIVES

The full data protection policy statement can be read [HERE].

As ITM, we all work together to implement the principles of the data protection policy.

In this policy, we translate the above objectives into principles, concrete terms and measures on how to deal with them in a number of policy areas. These measures are incorporated into a data protection and information security plan, which are supervised by the Data Protection Officer (DPO) and the Head of IT respectively, under the daily responsibility of the general manager.

2 SCOPE OF THE POLICY

This policy applies to all personal data as defined by the EU GDPR, including but not limited to the personal data of (ex-) employees, applicants for employment, consultants, interns, suppliers, visitors, business contacts, patients, research participants in Belgium and abroad, donors of human biospecimens processed by ITM, lecturers, students, (research) partners, etc. All employees and students of ITM must respect this policy when they process personal data in the framework of their professional activities for ITM. This applies both to the processing of personal data via electronic applications as well as the processing of personal data on paper.

This policy applies to personal data processing within and outside of the European Economic Area (EEA), for which ITM acts either as data controller, joint controller or as processor.

3 LEGISLATION

This policy complies with, and implements the European General Data Protection Regulation 2016/679 (or 'GDPR'). Its purpose is to protect the 'rights and freedoms' of natural persons and, in particular, to ensure that personal data is not processed unlawfully or without their knowledge, and, wherever applicable, that it is processed with their consent.

This data protection policy also complies with the Belgian Law on Data Protection of 30 July 2018.

When data are collected outside of Europe, i.e. for research conducted overseas, care must be taken in complying with any legal requirements in the study country (for instance, POPIA in South Africa).

Furthermore and relevant to the specific domain, the policy complies with the Belgian Law on Patient Rights, the Quality Law, the Law on Clinical Trials, relevant CAO's such as CAO 81, the camera law, sectoral standards, etc.

4 RESPONSIBILITIES

This policy applies to:

- All ITM employees processing personal data;
- External parties such as subcontractors, processors, consultants, advisers, external teaching staff, research partners, etc. processing person data on behalf of ITM;
- Students insofar they process personal data under the responsibility of, or in partnership with ITM.

The **Board of Governors** approves the data protection policy.

The **Director, General Manager**, and **Department Heads**, actively promote and foster the data protection policy. They formulate answers and make decisions with regard to advices issued by the DPO.

Unit Heads and all those in managerial or supervisory roles are responsible for supervising adherence to the data protection policy.

In particular, the **Chief Physician** and **Research Unit Heads**, supervise the adequate protection of health-related or otherwise sensitive data processed for medical care or scientific research.

The **IT-unit** and **Project Management Office** (PMO) develop or assist in the development of new ICT solutions at ITM. In that function, they assure that the data protection and Privacy-by-Design principles are followed. Any questions with regard to data protection or information security are discussed with the DPO or IT Manager respectively.

The **Data Protection Officer** is responsible for assuring and overseeing data protection legislation implementation in ITM's policies and procedures. The DPO provides assistance and advice on the processing of personal data. He or she is also the point of contact for the Data Protection Authority.

Employees/staff are responsible for the compliance with data protection laws and the current data protection policy for their specific function and field of work.

Non-ITM staff or externals such as contractors, guests, trainees, temporary employees, etc. must be made aware of the data protection and confidentiality requirements as it applies for their duties and activities they perform on behalf of ITM.

5 DATA PROTECTION PRINCIPLES AND THEIR IMPLEMENTATION AT ITM

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. All ITM policies and procedures are designed to ensure compliance with the principles.

5.1 Lawfulness, fairness and transparency

Personal data must be processed in a **transparent manner** with respect for all applicable laws, regulations and rules. Personal data must be processed **honestly, fairly** and data subjects must always be **informed** of which personal data of them is processed and for which purposes. This is independent of whether the personal data is retrieved directly or indirectly from the subject (Articles 13 & 14 of the GDPR) and this requirement can only be omitted in specific, motivated and approved circumstances (e.g. when there are non-disclosure obligations by law or it is authorized by a Data Protection Authority).

The following information must be provided to data subjects:

- The identity of the controller and contact details of its Data Protection Officer;
- The well-defined purposes of the personal data processing, including any possible future purposes;
- The lawful ground for the processing (see below);
- The categories of personal data concerned;
- The recipients or categories of recipients of the personal data, where applicable;
- The retention periods (or criteria used to define the retention period);
- The rights to request access, rectification, portability, erasure or to object to the processing, or an explanation on how and when these rights cannot be exerted;
- Where applicable, the intention to transfer personal data to a recipient in a third country and the level of protection provided by the concerned country;

- Any further information necessary to guarantee fair processing.

The manner of providing information to subjects can vary and should be suitable for the context of the data processing, e.g. :

- By means of a privacy policy for use of websites (such as ITM's website privacy policy) or specific applications like a LIMS
- By means of contractual agreements, like an employment contract, data processing agreement, the students exam and education regulation, etc.
- By means of an Information Sheet/Informed Consent Form, privacy statements and public registries for scientific studies
- By means of a central point of contact for data subjects, i.e. for ITM: informatieveiligheid@itg.be/

Furthermore, all personal data processing must have a **lawful basis** or **lawful ground** for processing the personal data.

The lawful ground for any personal data processing should be mentioned in the information provided to subjects and in the GDPR registry (see "6. GDPR registry" below).

The privacy statement for ITM employees, the GDPR register and the employment contract describe how employees' personal data is processed and what their rights are in relation to such processing.

The GDPR defines 6 lawful grounds for the processing of personal data:

I. Contractual agreement

This lawful ground can be used for the processing of the personal data of the contractual parties and their employees. It is the main lawful ground for processing of employee personal data as arranged by the employment contract, e.g. for payroll processing, management of staff personnel files, offering extra-legal benefits, internal functioning, etc. It can also be used for processing of partners' - such as research Investigators' - personal data in research consortia or students attending ITM's Master or postgraduate courses.

II. Consent

Where data processing is based on consent by the subject or their legal representative for minors or those incapable to give consent, there needs to be a *free, specific, informed and unambiguous* indication of the data subject's wishes that, by statement or by a clear affirmative action, the subject signifies agreement to the processing of personal data relating to him or her. The information provided must be tailored to adequately inform subjects in a language that is understandable to them. Consent also implies that such consent can be withdrawn at any time. Consent needs to be freely given, meaning that obtained under duress, on the basis of misleading information it will not be a valid basis for processing. Whenever vulnerable subjects such as minors, or people incapable to provide informed consent are involved, a proxy consent from the legal representative must be obtained. Furthermore, Ethics Committees (ECs) and the ITM Institutional Review Board (IRB) review the consent procedure and documents for scientific research involving human participants, data or biospecimens, and research cannot be started before approval is obtained.

In order to be able to demonstrate consent, there must be some active communication between the parties concerned. Consent cannot be inferred from non-response to a communication. For ***sensitive data, explicit written consent*** must be obtained unless an alternative lawful basis for processing exists. Consent is usually mandatory for the publication of people's photographs, sending out newsletters, use of data for non-related secondary purposes, etc.
For scientific research involving human participants, data and human biospecimens, consent is not always the most suitable lawful ground for the processing of participant personal data, even though an ethics consent (as approved by the concerned EC/IRB) is required for participation in research.

III. Legal obligation

ITM also performs data processing activities which need to be done out of legal reporting obligation, such as the immediate or periodic reporting of certain infectious diseases (like hiv, tuberculosis, gonorrhea), transfers of employee data to the National Social Security Office (RSZ), the National Employment Service (RVA), the collective insurance, or the need to send researcher's data to the Flemish Department of Economy, Science and Innovation (EWI). The reporting of serious adverse events in clinical trials to National Regulatory Authorities will also have a legal obligation as lawful ground.

IV. Public interest

This lawful ground can be applied when the data processing is justified or necessary for the benefit of society, e.g. scientific research that leads to an increase in knowledge and understanding in science.
Consequently, this is an important lawful ground for ITM as an academic research and education institution. However, it cannot be applied pro forma and several criteria may assist in determining public interest as a suitable basis, such as:

- The research makes a notable contribution to the (bio-)medical, clinical sciences or public health, directly or indirectly.
- The research is funded with public means (such as from the FWO, BOF, HORIZON EUROPE, etc.)
- Research outputs are made openly accessible according to FAIR principles.

The legal basis for data processing cannot be public interest if results are transferred exclusively to another party and the knowledge acquired is intended solely for private interests (e.g. commercial studies).

V. Vital interest

This means the vital interest of the data subject or another natural person, e.g. in case of emergencies.

VI. Legitimate interest

ITM can have a legitimate interest as an organisation to process personal data. Examples can be the processing of employee electronic usage data to assure IT and network security, camera's for security purposes, or processing patient or student data for improving policies, service provision or quality.

When this lawful ground is used, it must be carefully assessed and documented that the legitimate interests of ITM do not outweigh the rights and freedoms of the data subjects. The DPO assists in performing such privacy risk analysis.

5.2 Specific, explicit and legitimate purposes

Personal data obtained for a specific purpose must not be used for a purpose that differs from the primary purpose and is not reasonably expected by subjects (principle of "finality"). Often, but not always, consent from the data subject needs to be obtained for data processing that is not part of the primary purpose. For instance, student listings cannot be used for marketing purposes without their consent.

Key management functions at ITM have a particular responsibility in overseeing that personal data processing complies with this principle.

Scientific research can – in certain circumstances – be considered a compatible purpose when the primary purpose is not research, i.e. it is carried out on data originally obtained for patient routine care or infectious disease routine surveillance. In such case, the further use of data for scientific studies should at least be a **reasonable expectation** of the subjects. In accordance with the transparency principle, data subjects should be informed upfront about the possibility of such processing. Other factors, like the benefit for the public (health), the authority vested in the controller to perform scientific research, the specific research study domain, the sensitivity of the data or vulnerability of the subjects may be important factors in assessing the compatibility and further use of data for scientific research.

5.3 Adequate, relevant and limited data processing

No more personal data should be processed than strictly necessary for achieving the intended purpose (principle of "proportionality" and "data minimisation"). This principle is also applied in the Privacy by Design methodology for personal data software and systems.

For research purposes, personal data should be either collected anonymously, or should be anonymised or at least pseudonymised at the earliest opportunity. The key linking the pseudonymised data to the identifiable data should be retained in a separate location, in accordance with the information security policy.

Examples:

- When registering visitors, no personal data should be collected that is superfluous, such as for example the date of birth or the person's home address.
- Researchers should not ask questions in surveys that are not relevant to the research question. They should collect age instead of date of birth if possible; etc.

5.4 Accurate and up to date, with every effort to erase or rectify without delay

Personal data stored by ITM must be regularly reviewed and updated as necessary. No personal data is kept unless it is reasonable to assume that it is accurate (e.g. employee and student data).

It must be clear to data subjects how they can have their data updated. Preferably, they are given the possibility to update their data themselves in applications they have access to, or there is a process that allows for updates, or they are provided with a contact to have their personal data updated. Registration or application forms can include a statement that the data collected is accurate at the date of submission and that it is in their best interest to have their retained data up-to-date.

5.5 Subject can be identified only as long as necessary for processing

Personal data is not retained longer than necessary for the data processing. (Personal) data retention periods are laid down in retention schedules, data retention procedures, or the GDPR registry. Once its retention date has passed, personal data must be either securely destroyed, or if allowed, fully anonymised or aggregated (e.g. for further statistical, scientific or policy uses).

When databases or electronic applications are designed or purchased, the (automated) deletion of data after the retention periods have expired should be considered as a requirement.

5.6 Appropriate security

Personal data is processed in a manner that ensures appropriate security and confidentiality, preventing unauthorised access to personal data. In determining appropriate technical and organisational measures for data protection, the amount, sensitivity, (reputational) damage to subjects and ITM is taken into account. The measures must be in line with ITM's information security policy.

We implement the following organisational measures:

- Internal policies and procedures such as the data protection policy, information security policy, research data sharing policy and archiving policy set out the appropriate protection measures.
- ITM has appointed a Data Protection Officer.
- ITM employees are made aware and regularly trained in data protection and cybersecurity. Master and PhD students are provided training and background information in ethics and data protection.
- All employees, and particularly those in executive functions, are aware of their role and responsibilities with regard to data protection.
- External staff, contractors, research and educational partners are aware or trained in how to deal with personal data.
- Internal bodies oversee data protection and privacy requirements, such as the ITM Institutional Review Board for research studies, the Data Access Committee for data access requests, the PhD Commission & Education Offices, the Project Management Office for implementation of new IT solutions, etc.
- Our agreements and contracts with third parties include appropriate confidentiality and data protection clauses.
- We have a clear data breach reporting, mitigation and escalation procedure and we document follow-up in case of non-compliance with any of the measures.
- We periodically review our data processing activities by means of internal and external audits.

- We coordinate with external regulatory authorities like the Data Protection Authority, IVC or external advisory bodies such as the VLIR GDPR working group.

By default, technical measures to protect data and information includes appropriate network and device security, physical access control to rooms, lockers and devices, role-based access, multifactor authentication (MFA), password protection or encryption of sensitive data in rest and transfer, secure back-up storage and secure destruction of data.

As much as possible, user access is assigned on a need-to-know basis. Access to databases and applications must not be disproportionately permissive and this requirement becomes more compelling as the sensitivity of the data increases.

Where data processors process personal data on behalf of ITM, the minimal technical and organisational measures to be adhered to by the processor are detailed in a data processing agreement.

5.7 Accountability

ITM assures and demonstrates compliance with the data protection requirements by means of clear and documented traceability, e.g. by keeping registries of data processing activities, data breaches, data processors, data access requests, training logs, etc.

6 GDPR Registry

In accordance with the GDPR, ITM establishes and keeps up-to-date a registry of all processing activities of personal data for which ITM is the data controller. This registry serves multiple purposes:

- Supporting accountability obligations towards supervisory authorities;
- As an internal inventory of data processing activities and documentation/review of legal compliance, such as assuring suitable lawful grounds for data processing and data transfers, providing overviews of processors and the need for data processing agreements, the need for Data Protection Impact Assessments, etc.

The DPO is responsible for the conformity of the personal data processing registry with the legal requirements and the overall governance of the registry as laid down in the registry procedure.

7 Subject rights

Data subjects retain the following rights with regard to their personal data and the data that is recorded about them:

The right to information

- Information about what personal data is processed, for what purpose(s) processing takes place, is provided in a clear and transparent manner

The right to access

- Subjects have the right to request access to, or receive a copy of the data we process about them

The right to rectification

- If the data are not correct or no longer up-to-date, the data subjects can ask to correct, supplement or erase them

The right to restriction of processing

- When certain criteria are met, data subjects can request to (temporarily) stop processing their personal data. This criterion may also include restriction of profiling or automated decision making

The right to data portability

- Or the right to transfer their data to another data controller of their choice (in machine-readable form)

The right to erasure (the "right to be forgotten")

- For instance when processing is no longer necessary or the subject withdraws consent for data processing

It is important to note that not all rights can always be exercised by the data subject. The GDPR requires maximum protection and autonomy of data subjects and they should be able to exert all those rights which cannot be derogated from on specific grounds, such a legal obligations to process or retain data, or carefully assessed legitimate reasons. The rights and derogations thereof should be established before the data processing is initiated and should be clear to data subjects. This is done through, e.g.

- Privacy statements for patients, students and employees on our website;
- Contractual agreements including data protection clauses;
- Information sheets and Informed Consent Forms for research participants;
- Privacy-by-design applications allowing subjects' control over their own personal data, its processing and erasure.

Especially where the data processing is based on the lawful ground of consent, subjects have the right to withdraw that consent, meaning that personal data cannot be further processed or should be erased in case no other lawful ground dictates the retention of the personal data.

Data subjects have the right to ask questions about, or make a complaint to ITM with regards to the processing of their personal data. ITM ensures a low threshold by making information and a point of contact easily findable and available (such as telephone or email to the DPO (+32 3 247 07 43 or informatieveiligheid@itg.be), the general complaints email (klachten@itg.be), the Institutional Review Board (irb@itg.be), or making a complaint to ombuds, secretariats, reception desks or staff directly).
Furthermore, data subjects have the right to make complaints about the data processing to the national Data Protection Authority, which is also consistently mentioned in privacy statements, consent information etc.

8 PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The processing of special categories of personal data (also referred to as 'sensitive data', such as health data, ethnicity or race, judicial or sexual data) is prohibited unless an additional lawful ground can be found as listed in Article 9 of the GDPR.

Important exceptions to this prohibition for ITM are providing medical care for patients and processing for the purpose of statistic, historic and scientific research.

Wherever ITM processes sensitive personal data, additional measures are implemented such as:

- Higher security measures (such as stringent access on a need-to-know basis, MFA, encryption of data, in accordance with the information security policy);
- The availability of up-to-date listings of persons with access to the personal data;
- Patient-related and clinical trial data are processed in validated and quality controlled systems, including audit trail and nominal privacy logging;
- Health data is processed under the responsibility of a doctor or health care practitioner;
- Secondary use of personal health data from Belgian subjects may require an authorisation from the IVC.

9 DATA PROTECTION IMPACT ASSESSMENTS

Where personal data processing is likely to present high risks to the rights and freedoms of natural persons, ITM conducts Data Processing Impact Assessments (DPIA) in order to evaluate the nature and potential impact of such risks. This is described in the DPIA procedure.

The results of the assessment is taken into account when appropriate security and privacy measures are established.

If a DPIA confirms that processing involves a high degree of risk which cannot be satisfactorily mitigated, a consultation of the Data Protection Authority should take place prior to the processing.

All research protocols submitted to the ITM IRB for review and approval are required to complete an online privacy check including a preliminary DPIA check.

For any type of data processing performed by ITM, the DPO advises whether a DPIA is necessary.

10 DATA TRANSFERS

10.1 Engagement of processors

In any event where data processors are engaged, a data processing agreement must be drawn up prior to the data processing by the processor. Such data processing agreement stipulates for what exact purpose and how the data can be processed, which security measures must minimally be in place, who can have access to the data, how long the data can be retained and under which conditions data can be processed by sub-processors.

10.2 Joint Controllers

If two or more Controllers jointly decide on the means and the purpose of data processing, they act as joint controller. This is often the case in scientific research consortia or partnerships, but can also exist in any kind of transmural collaboration such as biobank or data repository consortia, educational partnerships, etc.

Whenever ITM is engaged as joint-controller, it will assure by means of an arrangement that respective responsibilities of the controllers are clearly laid down, in particular as regards transparency towards, and exercising of the rights of data subjects.

10.3 Transfers outside of the EEA

The GDPR ensures uniformity of protection rules facilitating the free movement of personal data within the European Economic Area (EEA). Transfers of personal data to countries outside the EEA or international organisations are only allowed if such third country or international organisation can guarantee an "adequate level of protection" for the processing of personal data. The European Commission has already issued an adequacy decision for a number of countries confirming that the country has an adequate level of protection. The most recent list of countries can be found here.

If a country is not on the list of adequacy decisions, the transfer of personal data is only possible in one of the following cases:

- The inclusion of standard data protection clauses, such as the EU standard contractual clauses, in agreements we conclude with third country organisations.
- There is an explicit consent from the data subjects for the occasional transfer of data. The data subjects must also be informed of the risks that this transfer may entail for them.
- The transfer concerns an exceptional situation, which complies with the provisions of Article 49 of the GDPR.

10.4 Transfers to other Controllers

When personal data are transferred to a third party acting as Data Controller, it is essential to assure that an adequate lawful ground is present justifying such transfer, as the third party will in turn become fully responsible for the management of the personal data. Often, such transfer will be based on a legal obligation (transfers to agencies, public health institutes, …), public interest for the sharing of (anonymised) data for secondary scientific research or consent by the participant.

Such transfers – together with the secondary purposes – must be known to data subjects.

10.5 Data sharing for secondary research

ITM is committed to the FAIR principles of open access to research data, allowing verification of results by independent researchers and the performance of secondary research for public health reasons worldwide.

Because the privacy protection of research participants and patients is crucial, making research data that includes personal data, accessible can only be done within the boundaries of the European and Belgian data protection legislation. As such, we adhere to the statement "As open as possible, as closed as necessary".

The appropriate rules for making data available for secondary research and how to do this in a privacy responsible way, are laid down in ITMs Data Sharing Policy. Data Access Requests are evaluated by ITMs Data Access Committee.

Additionally, transfers of Belgian (pseudonymised and non-anonymous) health-related personal data for secondary research purposes need the a priori authorization of the IVC – and they may need approval of the concerned IRB/EC if they were originally collected for other reasons and/or without subject consent for future research.

11 PERSONAL DATA BREACH MANAGEMENT

Any person who notices a potential personal data breach is obliged to report it **immediately** by telephone or by email to the DPO (informatieveiligheid@itg.be). In case of doubt, it is recommended to always report.

Personal data breach incidents are occurrences with a potential or effective impact on the confidentiality of personal data. Such breaches could include, but are not limited to accidental or malicious unauthorised access to personal data, either internally or externally.

EXAMPLES OF DATA BREACHES
Leaving sensitive documents at a printer
Including e-mail addresses of recipients in CC of a newsletter
Loss of personal data to cybercriminals though phishing or hacking into systems
Loss of USB drive, smartphone or laptop containing confidential data (unless properly encrypted)
Putting (indirectly) identifiable data in an open access data repository
Mailing confidential information to an incorrect email address
Intentionally taking student/patient contact information and using it for prohibited purposes

ITM foresees a central and standardized notification procedure for its staff, partners and contractors with regard to data breach notification. The need to notify data breaches immediately and by which procedure is included in all processing agreements we conclude and other agreements as relevant.

Where ITM acts as controller for the breached data, the DPO (together with the IT-unit and/or other staff involved) will assess the severity, context and circumstances of the breach in order to define further mitigating or preventative actions. They advise the management on whether the data breach should be notified to the data subjects and/or the supervisory authority.

In the event that ITM acts as the processor of the breached data, it will notify the breach together with a preliminary description (such as amount, identifiability, context, circumstances, etc.) to the controller of the data without any delay.

12 ABBREVIATIONS

BOF	Bijzondere Onderzoeksfinanciering
CAO	Collectieve Arbeidsovereenkomst
DAC	Data Access Committee
DPIA	Data Protection Impact Assessment

DPO	Data Protection Officer
EC	Ethics Committee
EEA	European Economic Area
FAIR	Findable – Accessible – Interoperable - Reusable
FWO	Fonds voor Wetenschappelijk Onderzoek
GDPR	General Data Protection Regulation
IRB	Institutional Review Board
IVC	Information Security Committee (~ Informatieveiligheidscomité)
MFA	Multifactor Authentication
POPIA	Protection of Personal Information Act (South-Africa)
VLIR	Vlaamse Interuniversitaire Raad

13 DEFINITIONS

Anonymisation – Anonymization is data processing by which the data can no longer be associated with an identified or identifiable individual without the use of means that are not reasonably foreseeable (reasonably irreversible).

Controller – The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In the event that 2 or more controllers are responsible together for a data processing activity, they are referred to as joint-controllers.

(Data) Subject – The natural person of whom personal data is processed.

Personal data – Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing (of personal data) – Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor – A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Pseudonymisation – Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Special categories of personal data (or sensitive data) – Any personal data relating to the race, ethnicity, health or medical condition, sexual life/preferences, political, philosophical or religious beliefs, memberships of unions, genetic, biometrical, judicial, or genetic data.

Third party – A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

14 AUTHORSHIP AND APPROVAL

Authored by	Jef Verellen – Data Protection Officer
Approved by	ITM Board of Governors during its meeting of 23/05/2022