

UZ Gent – Datenschutzerklärung: Patient

Schutz personenbezogener Daten von Patienten

Der Hauptzweck dieser Datenschutzerklärung besteht darin, Sie als Patienten über die Art und Weise und die Gründe für die Verarbeitung Ihrer personenbezogenen Daten als Patient durch UZ Gent sowie über die Rechte, die Sie ausüben können, zu informieren.

Inhaltsverzeichnis

1	Wer ist der (Verarbeitungs-) Verantwortliche für die Verarbeitung Ihrer personenbezogenen Daten?	2
2	Datenschutzbeauftragter	2
3	Begriffe in dieser Datenschutzerklärung	2
4	Allgemeines	2
5	Welche personenbezogenen Daten verarbeitet UZ Gent?	3
6	Verarbeitungszwecke und rechtliche Gründe für diese Verarbeitung	3
6.1	Patientenversorgung	4
6.2	Patientenverwaltung	5
6.3	Elektronische Pflegekommunikation mit dem Patienten über das Patientenportal	7
6.4	Registrierung der Patienten	9
6.5	Materielle Sicherheit	11
6.6	Medizinische Kamera- und Tonaufzeichnungen	12
6.7	Wartung und Betrieb der Website	13
6.8	Nutzung des WLAN-Netzwerks des Krankenhauses	15
6.9	Kommunikation	16
6.10	Registrierung von Beschwerden beim Büro des Bürgerbeauftragten	16
6.11	Soziale Dienste	17
6.12	Wissenschaftliche Forschung	18
7	Übermittlung Ihrer Daten in ein Land außerhalb des EWR (Europäischer Wirtschaftsraum)	19
8	Ihre Rechte in Bezug auf die Verarbeitung Ihrer personenbezogenen Daten	19
8.1	Rechte in Bezug auf UZ Gent	19
8.2	Beschwerde über UZ Gent	22
8.3	Beschwerde bei der Datenschutzbehörde	22
9	Inkrafttreten und Änderungen der Datenschutzerklärung	22

10	Anhänge	23
10.1	ANHANG 1: Begriffe in dieser Datenschutzerklärung	23
10.2	ANHANG 2: Standardvertragsklauseln für die Übermittlung personenbezogener Daten in ein Land außerhalb des EWR	25

1 Wer ist der (Verarbeitungs-) Verantwortliche für die Verarbeitung Ihrer personenbezogenen Daten?

Das Universitair Ziekenhuis Gent, öffentliche Einrichtung mit Sitz in C. Heymanslaan 10, 9000 Gent und registriert in der „Kruispuntbank van Ondernemingen“ unter der Nummer 0232.987.862 (im Folgenden „UZ Gent“, „wir“ oder „uns“) ist verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten als Patient, wie in dieser Datenschutzerklärung beschrieben.

Das UZ Gent ist Teil der Universität Gent, einer öffentlichen Einrichtung mit Rechtspersönlichkeit gemäß dem Sonderdekret vom 26. Juni 1999, mit Verwaltungssitz in 9000 Gent, Sint-Pietersnieuwstraat 25, und eingetragen in der „Kruispuntbank van Ondernemingen“ unter der Nummer 0248.015.142.

2 Datenschutzbeauftragter

UZ Gent hat einen Datenschutzbeauftragten ernannt. Wenn Sie Fragen oder Anmerkungen zur Verarbeitung Ihrer personenbezogenen Daten haben, können Sie sich unter folgender Adresse an unseren Datenschutzbeauftragten wenden: Data Protection Officer UZ Gent, C. Heymanslaan 10, 9000 Gent, dpo@uzgent.be.

3 Begriffe in dieser Datenschutzerklärung

In dieser Datenschutzerklärung werden verschiedene Begriffe verwendet. Hierzu verweisen wir auf ANHANG 1.

4 Allgemeines

Diese Datenschutzerklärung wurde u.a. in Anwendung der folgenden Bestimmungen erstellt:

- Das Gesetz zum Schutz personenbezogener Daten gemäß der Verordnung (EU) 2016/679 vom 27. April 2016 und dem Gesetz vom 5. September 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten
- Das koordinierte Gesetz vom 10. Juli 2008 über Krankenhäuser und andere Pflegeeinrichtungen (im Folgenden das „Krankengesetz“) und Anhang A. III. Artikel 9 ff. des königlichen Erlasses vom 23. Oktober 1964 zur Festlegung der von den Krankenhäusern und ihren Diensten zu beachtenden Normen
- Das Gesetz vom 22. August 2002 über die Rechte der Patienten
- Das Gesetz über die Pflichtversicherung für medizinische Versorgung, abgestimmt am 14. Juli 1994
- Königlicher Erlass vom 03. Mai 1999 über die allgemeine Krankenakte
- Das Gesetz vom 1. Mai 2015 über die Ausübung von Gesundheitsberufen
- Das Gesetz über Krankenhäuser vom 7. August 1987, einschließlich der Patientenakten
- Das Gesetz vom 21. März 2007 zur Regelung der Aufstellung und Verwendung von Überwachungskameras

- Das Gesetz zur Qualitätspraxis im Gesundheitswesen vom 22. April 2019

5 Welche personenbezogenen Daten verarbeitet UZ Gent?

Kategorie der personenbezogenen Daten	Besondere personenbezogene Daten
Angaben zur Identifizierung	Name, Vorname, Geburtsort, Geburtsdatum, Staatsangehörigkeit, Passfoto
Nationale Nummer	Nationale Nummer (Beschluss Nr. 50/2008 des sektoralen Ausschusses der nationalen Nummer)
Kontaktangaben	Adresse, E-Mail-Adresse, Telefonnummer
Gesundheitsbezogene Daten	Alle Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen, einschließlich Daten über geleistete Gesundheitsdienste, die Auskunft über den Gesundheitszustand geben
Finanzielle Verwaltungsdaten	Kontonummer
Soziale Daten	Familiensituation, besondere Anforderungen
Daten zu Versicherungsverein auf Gegenseitigkeit und Versicherungsdaten	Name Versicherungsverein auf Gegenseitigkeit, Nummer Versicherungsverein auf Gegenseitigkeit
Daten zu einem Treuhänder/Familienmitgliedern	Mögliche Daten einer Vertrauensperson
Genetische Daten	Informationen aus einem DNA-Test
Biometrische Daten	Fingerabdruck, Gesichtsbild, Iris
Kameraaufnahmen	Gesichter, Formen, Autos, Nummernschilder
Medizinische Kamerabilder	Verhalten, Reaktionen, medizinisch relevantes Filmmaterial
Medizinische Tonaufnahmen	Menschliche Tonaufnahmen von medizinischer Relevanz
Cookies	Wesentlich, funktional, Präferenz, sozial

6 Verarbeitungszwecke und rechtliche Gründe für diese Verarbeitung

Es ist möglich, dass UZ Gent verschiedene Arten von personenbezogenen Daten für unterschiedliche Zwecke verarbeitet.

Im Folgenden erfahren Sie für jeden Zweck, welche personenbezogenen Daten UZ Gent verarbeitet, auf welcher Grundlage die Verarbeitung erfolgt, wie lange die Daten verarbeitet werden und an wen wir sie gegebenenfalls weitergeben.

Im Folgenden werden wir auf die folgenden Zwecke eingehen:

1. Patientenversorgung
2. Patientenverwaltung
3. Registrierung der Patienten
4. Materielle Sicherheit
5. Medizinische Kamera- und Tonaufzeichnungen
6. Wartung und Betrieb der Website
7. Nutzung des WLAN-Netzwerks des Krankenhauses
8. Kommunikation
9. Registrierung von Beschwerden beim Büro des Bürgerbeauftragten
10. Soziale Dienste
11. Wissenschaftliche Forschung

6.1 Patientenversorgung

Unter dem Zweck der Patientenversorgung ist Folgendes zu verstehen:

- Vorbeugende Maßnahmen (und medizinische Diagnosen); und/oder
- Erbringung von Pflegeleistungen (einschließlich Behandlung des Patienten).

Kategorie der personenbezogenen Daten	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Angaben zur Identifizierung	Vorbeugende Maßnahmen	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	Interne Mitarbeiter, die in einer Betreuungsbeziehung zu der betroffenen Person stehen, der Hausarzt des Patienten, Betreuer, gesetzliche Vertreter. Wenn wir aufgrund von Vorschriften oder Rechtsprechung dazu verpflichtet sind, auch gegenüber der Regierung oder dem Versicherungsverein auf Gegenseitigkeit.
	Bereitstellung von Pflege	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen		
Kontaktangaben	Vorbeugende Maßnahmen	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	
	Bereitstellung von Pflege	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen		
Gesundheitsbezogene Daten	Vorbeugende Maßnahmen	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	
	Bereitstellung von Pflege	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen		
Soziale Daten	Bereitstellung von Pflege	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	
Finanzielle Verwaltungsdaten	Vorbeugende Maßnahmen	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	Mitarbeiter

6.1.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, Ihre personenbezogenen Daten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

Die gesetzliche Verpflichtung, auf deren Grundlage UZ Gent die personenbezogenen Daten für die oben genannten Zwecke verarbeitet, ist: das koordinierte Gesetz vom 10. Juli 2008 über Krankenhäuser und andere Pflegeeinrichtungen (im Folgenden das Krankenhausgesetz) und Anhang A.III Artikel 9 ff. des königlichen Erlasses vom 23. Oktober 1964 zur Festlegung der von Krankenhäusern und ihren Diensten einzuhaltenden Normen.

6.1.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die UZ Gent im Rahmen der Patientenbetreuung verarbeitet, wurden direkt vom Patienten erhalten, es sei denn, der Patient war nicht in der Lage, die personenbezogenen Daten mitzuteilen.

6.1.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen über Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

6.2 Patientenverwaltung

Unter Patientenverwaltung verstehen wir:

- Die Verwaltung und Nachverfolgung von Gesundheitsdienstleistungen auf der Grundlage der Identifizierung und Nachverfolgung von Patienten („Verwaltung und Identifizierung“) und/oder
- Verarbeitung in Bezug auf die Nachverfolgung des Aufenthalts und der Behandlung von Patienten im Hinblick auf die Rechnungsstellung („Nachverfolgung und Rechnungsstellung“).

Kategorie der personenbezogenen Daten	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Angaben zur Identifizierung	Verwaltung und Identifizierung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	7 Jahre	Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung
	Nachverfolgung und Rechnungsstellung	Notwendig für die Ausführung der Vereinbarung mit UZ Gent		Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung, Rechtsanwalt, Gerichtsvollzieher, Callcenter Drittanbieter von Diensten

Kontaktangaben	Verwaltung und Identifizierung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	7 Jahre	Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung
	Nachverfolgung und Rechnungsstellung	Notwendig für die Ausführung der Vereinbarung mit UZ Gent		Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung, Rechtsanwalt, Gerichtsvollzieher, Callcenter Drittanbieter von Diensten
Gesundheitsbezogene Daten	Verwaltung und Identifizierung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	7 Jahre	Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung
	Nachverfolgung und Rechnungsstellung	Notwendig für die Ausführung der Vereinbarung mit UZ Gent		Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung, Rechtsanwalt, Gerichtsvollzieher, Callcenter
Finanzielle Verwaltungsdaten	Verwaltung und Identifizierung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	7 Jahre	Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung
Soziale Daten	Verwaltung und Identifizierung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	7 Jahre	Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung
	Nachverfolgung und Rechnungsstellung	Notwendig für die Ausführung der Vereinbarung mit UZ Gent		Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung, Rechtsanwalt, Gerichtsvollzieher, Callcenter
Angaben zum vorläufigen Verwalter /Familie	Verwaltung und Identifizierung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	7 Jahre	Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung
Daten zu Versicherungsverein auf Gegenseitigkeit und Versicherungsdaten	Verwaltung und Identifizierung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	7 Jahre	Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung
	Nachverfolgung und Rechnungsstellung	Notwendig für die Ausführung der Vereinbarung mit UZ Gent		Sozialversicherungsträger, Versicherungsverein auf Gegenseitigkeit, Krankenhausversicherung, Rechtsanwalt,

				Gerichtsvollzieher, Callcenter
--	--	--	--	-----------------------------------

6.2.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, die personenbezogenen Daten des Patienten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

Die gesetzliche Verpflichtung, auf deren Grundlage UZ Gent die personenbezogenen Daten für die oben genannten Zwecke verarbeitet, ist: das koordinierte Gesetz vom 10. Juli 2008 über Krankenhäuser und andere Pflegeeinrichtungen (im Folgenden das Krankenhausgesetz) und Anhang A.III Artikel 9 ff. des königlichen Erlasses vom 23. Oktober 1964 zur Festlegung der von Krankenhäusern und ihren Diensten einzuhaltenden Normen.

Wenn UZ Gent die oben genannten personenbezogenen Daten für die genannten Zwecke verarbeitet, weil dies für die Ausführung der Vereinbarung, die der Patient mit UZ Gent geschlossen hat, erforderlich ist, kann UZ Gent diese Dienstleistungen für diese Zwecke nicht erbringen, ohne diese personenbezogenen Daten zu verarbeiten.

6.2.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die UZ Gent im Rahmen der Patientenverwaltung verarbeitet, wurden direkt vom Patienten erhalten, es sei denn, der Patient war nicht in der Lage, die personenbezogenen Daten mitzuteilen.

Personenbezogene Gesundheitsdaten werden beim Patienten selbst erhoben, es sei denn, der Zweck der Verarbeitung erfordert eine andere Erhebungsmethode oder der Patient selbst ist nicht in der Lage, die Daten zur Verfügung zu stellen.

Die medizinischen Daten erhält UZ Gent unter anderem von (internen oder externen) Gesundheitsdienstleistern.

6.2.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen über Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

6.3 Elektronische Pflegekommunikation mit dem Patienten über das Patientenportal

Das Patientenportal versucht, dem Patienten mehr Kontrolle über seine Pflege zu geben, indem es elektronische Fragebögen und Versorgungsinformationen bereitstellt.

Kategorie der personenbezogenen Daten	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrung sfrist	Kategorie des Empfängers
Angaben zur Identifizierung	Elektronische Pflegekommunikation	Einwilligung	Mindestens 30 Jahre und maximal 50 Jahre nach dem letzten Patientenkontakt	Interne Mitarbeiter, die in einer Betreuungsbeziehung zu der betroffenen Person stehen, der Hausarzt des Patienten, Betreuer,

Kontaktangaben	Elektronische Pflegekommunikation	Einwilligung	Mindestens 30 Jahre und maximal 50 Jahre nach dem letzten Patientenkontakt	gesetzliche Vertreter. Wenn wir aufgrund von Vorschriften oder Rechtsprechung dazu verpflichtet sind, auch gegenüber der Regierung oder dem
Gesundheitsbezogene Daten	Elektronische Pflegekommunikation	Einwilligung	Mindestens 30 Jahre und maximal 50 Jahre nach dem letzten Patientenkontakt	Versicherungsverein auf Gegenseitigkeit.
Soziale Daten	Elektronische Pflegekommunikation	Einwilligung	Mindestens 30 Jahre und maximal 50 Jahre nach dem letzten Patientenkontakt	
Finanzielle Verwaltungsdaten	Elektronische Pflegekommunikation	Einwilligung	Mindestens 30 Jahre und maximal 50 Jahre nach dem letzten Patientenkontakt	Mitarbeiter

6.3.1 Rechtsgrundlage

Wenn das UZ Gent beabsichtigt, Ihre personenbezogenen Daten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten, werden wir Sie im voraus darüber informieren.

Für bestimmte Zwecke (siehe oben) gibt der Patient seine Einwilligung, indem er einer bestimmten Verarbeitung ausdrücklich zustimmt (z. B. über die Nutzung des Patientenportals). Der Patient hat das Recht, seine Einwilligung jederzeit zu widerrufen. Der Widerruf einer solchen Einwilligung berührt nicht die Rechtmäßigkeit der vor dem Widerruf aufgrund der Einwilligung erfolgten Verarbeitung

6.3.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die das UZ Gent im Rahmen der elektronischen Pflegekommunikation mit dem Patienten verarbeitet, hat das Krankenhaus direkt vom Patienten erhalten, es sei denn, der Patient war nicht in der Lage, die personenbezogenen Daten zu übermitteln.

6.3.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen über Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

6.4 Registrierung der Patienten

Unter Registrierung der Patienten verstehen wir:

- Aufzeichnung von Gesundheits- und Unterbringungsdaten für verwaltungstechnische Zwecke wie: Bettenbelegung, Bestandsverwaltung, Personalplanung („verwaltungstechnische Aufzeichnung“)
- Aufzeichnung von Gesundheits- und Unterkunftsdaten für staatliche Zwecke wie die Seuchenbekämpfung („vorgeschriebene Aufzeichnung“)
- Aufzeichnung von Gesundheitsdaten für wissenschaftliche Zwecke. Wissenschaftliche Forschung ist eine der Kernaufgaben eines Universitätsklinikums. Ziel der wissenschaftlichen Forschung ist es, das Wissen über Krankheit und Gesundheit zu verbessern und neue Erkenntnisse zu gewinnen, die zu neuen oder besseren Therapien für Patienten führen. („wissenschaftliche Aufzeichnung“)

Kategorie der personenbezogenen Daten	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Angaben zur Identifizierung	Verwaltungstechnische Aufzeichnung	Notwendig für die Ausführung der Vereinbarung mit UZ Gent	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	Keine externen Empfänger
	Vorgeschriebene Aufzeichnung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	Sozialversicherungsträger, staatliche Dienste
	Wissenschaftliche Aufzeichnung	Notwendig zur Erfüllung des öffentlichen Interesses	25 Jahre nach Abschluss der Studie	Ärzte, Forscher, ihre Teams, Studiensponsor erhalten pseudonymisierte Form der personenbezogenen Daten
Kontaktangaben	Verwaltungstechnische Aufzeichnung	Notwendig für die Ausführung der Vereinbarung mit UZ Gent	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	Keine externen Empfänger
	Vorgeschriebene Aufzeichnung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	Sozialversicherungsträger, staatliche Dienste
	Wissenschaftliche Aufzeichnung	Notwendig zur Erfüllung des öffentlichen Interesses	25 Jahre nach Abschluss der Studie	Ärzte, Forscher, ihre Teams, Studiensponsor erhalten pseudonymisierte Form der personenbezogenen Daten
Gesundheits-bezogene Daten	Verwaltungstechnische Aufzeichnung	Für die Erbringung von Gesundheitsleistungen nach Artikel 9.2h) DSGVO	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	Keine externen Empfänger
	Vorgeschriebene Aufzeichnung	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	Sozialversicherungsträger, staatliche Dienste

	Wissenschaftliche Aufzeichnung	Notwendig zur Erfüllung einer Aufgabe des öffentlichen Interesses	25 Jahre nach Abschluss der Studie	Ärzte, Forscher, ihre Teams, Studiensponsor erhalten pseudonymisierte Form der personenbezogenen Daten
Genetische Daten	Wissenschaftliche Aufzeichnung	Notwendig zur Erfüllung des öffentlichen Interesses	25 Jahre nach Abschluss der Studie	Ärzte, Forscher, ihre Teams, Studiensponsor erhalten pseudonymisierte Form der personenbezogenen Daten
Biometrische Daten	Wissenschaftliche Aufzeichnung	Notwendig zur Erfüllung des öffentlichen Interesses	25 Jahre nach Abschluss der Studie	Ärzte, Forscher, ihre Teams, Studiensponsor erhalten pseudonymisierte Form der personenbezogenen Daten

6.4.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, die personenbezogenen Daten des Patienten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

Die gesetzliche Verpflichtung, auf deren Grundlage UZ Gent die personenbezogenen Daten für die oben genannten Zwecke verarbeitet, ist: das koordinierte Gesetz vom 10. Juli 2008 über Krankenhäuser und andere Pflegeeinrichtungen (im Folgenden das Krankenhausgesetz) und Anhang A.III Artikel 9 ff. des königlichen Erlasses vom 23. Oktober 1964 zur Festlegung der von Krankenhäusern und ihren Diensten einzuhaltenden Normen. Die gesetzliche Verpflichtung kann auch auf staatlich angeordneten Registrierungen beruhen, wie z. B. im Rahmen der Covid-19-Überwachung.

Wenn UZ Gent die oben genannten personenbezogenen Daten für die genannten Zwecke verarbeitet, weil dies für die Ausführung der Vereinbarung, die der Patient mit UZ Gent geschlossen hat, erforderlich ist, kann UZ Gent diese Dienstleistungen für diese Zwecke nicht erbringen, ohne diese personenbezogenen Daten zu verarbeiten.

Wenn UZ Gent die oben genannten personenbezogenen Daten für die oben genannten Zwecke aus Gründen des öffentlichen Interesses verarbeitet, besteht das öffentliche Interesse darin, das Wissen über Krankheit und Gesundheit zu verbessern und neue Erkenntnisse zu bieten, die zu neuen oder besseren Therapien für den Patienten führen.

6.4.2 Wie haben wir diese personenbezogenen Daten erhalten?

Personenbezogene Gesundheitsdaten werden beim Patienten selbst erhoben, es sei denn, der Zweck der Verarbeitung erfordert eine andere Erhebungsmethode oder der Patient selbst ist nicht in der Lage, die Daten zur Verfügung zu stellen.

- *Für die verwaltungstechnische und vorgeschriebene Aufzeichnung:*

Die personenbezogenen Daten, die UZ Gent im Rahmen der verwaltungstechnischen und vorgeschriebenen Aufzeichnung verarbeitet, wurden direkt vom Patienten erhalten, es sei denn, der Patient war nicht in der Lage, die personenbezogenen Daten mitzuteilen.

Die Gesundheitsdaten wurden vom UZ Gent über interne oder externe Gesundheitsdienstleister eingeholt.

- *Für die wissenschaftliche Aufzeichnung:*

Angaben zur Identifizierung, die UZ Gent im Rahmen der wissenschaftlichen Aufzeichnung verarbeitet, wurden direkt vom Patienten erhalten, es sei denn, der Patient war nicht in der Lage, die personenbezogenen Daten mitzuteilen.

Die gesundheitlichen, genetischen und biometrischen Daten wurden von UZ Gent über die Patientenakte empfangen.

6.4.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen über Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

Im Rahmen der wissenschaftlichen Registrierung ist es möglich, dass Sie die in dieser Datenschutzerklärung näher erläuterten Rechte nicht haben bzw. nur eingeschränkt wahrnehmen können, da diese Rechte die Erreichung bestimmter Zwecke unmöglich machen oder ernsthaft behindern könnten und solche Abweichungen zur Erreichung der Zwecke erforderlich sind (z. B. darf ein Patient nicht wissen, ob ihm in klinischen Prüfungen ein Medikament mit oder ohne Wirkstoffe („Placebo“) verabreicht wurde).

6.5 Materielle Sicherheit

Kategorie der personenbezogenen Daten	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Kameraaufnahmen	Zum Schutz des Geländes, der Gebäude und der Güter, die UZ Gent zur Verfügung stehen, durch die Verhinderung oder Aufdeckung von Vandalismus, Beschädigung und Diebstahl;	Berechtigtes Interesse	30 Tage	Polizei- und Justizbehörden im Falle von Straftaten gemäß den geltenden Rechtsvorschriften (Artikel 9 des Kameragesetzes).
	Zum Schutz der Sicherheit und Gesundheit der Mitarbeiter durch Vermeidung von Konfrontationen mit Personen, die Diebstähle, Vandalismus, Gewalt und Belästigungen begehen, sowie zur Wahrung der öffentlichen Ordnung und Moral und zur Vermeidung von Belästigungen;	Berechtigtes Interesse	30 Tage	
	Identifizierung von Verhaltensweisen, die nach belgischem Recht strafbar sind, und Weitergabe von Informationen darüber an die Ermittlungs-, Polizei- und Justizbehörden zum Zwecke der Aufdeckung.	Berechtigtes Interesse	30 Tage	

6.5.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, die personenbezogenen Daten des Patienten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

Wenn UZ Gent die oben genannten personenbezogenen Daten für die oben genannten Zwecke auf der Rechtsgrundlage des berechtigten Interesses verarbeitet, sind der Schutz der Güter, die Sicherheit des Personals und die Kontrolle der Produktionsprozesse (z. B. Cyclotron) die berechtigten Interessen von UZ Gent. Die oben erwähnte Verarbeitung personenbezogener Daten durch UZ Gent im Zusammenhang mit der Kameraüberwachung ist keine Verarbeitung, die UZ Gent als staatliche Einrichtung in Erfüllung ihrer Aufgaben vornimmt. Folglich kann UZ Gent als öffentliche Einrichtung das berechnete Interesse geltend machen. Nach sorgfältiger Abwägung der verschiedenen Interessen ist UZ Gent der Ansicht, dass sein Interesse das des Patienten aus den oben genannten Gründen überwiegt. Zu diesem Zweck kann UZ Gent nachweisen, dass:

1. die Interessen, die mit der Verarbeitung verfolgt werden, als rechtmäßig anerkannt werden können („**Zweckprüfung**“);
2. die beabsichtigte Verarbeitung für die Verwirklichung dieser Interessen erforderlich ist („**Erforderlichkeitsprüfung**“); und
Die Abwägung dieser Interessen mit den Interessen, grundlegenden Freiheiten und Rechten der betroffenen Personen zugunsten des für die Verarbeitung Verantwortlichen ausfällt („**Abwägungsprüfung**“).

6.5.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die UZ Gent im Rahmen der Kameraüberwachung verarbeitet, wurden direkt von der betroffenen Person eingeholt.

6.5.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen über Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

6.6 Medizinische Kamera- und Tonaufzeichnungen

Wir verarbeiten diese Daten im Rahmen der wissenschaftlichen Forschung, bei thorax- und gefäßchirurgischen Eingriffen und bei der EEG-Überwachung (Registrierung der Hirnaktivität), in der Schlafklinik, auf der Schlaganfallstation, der (neonatologischen) Intensivstation. Filmaufnahmen können auch zur Qualitätssicherung notwendig sein, z. B. während einer Operation oder zur Überwachung bestimmter Erkrankungen (z. B. Bewegungsstörungen).

Kategorie der personenbezogenen Daten	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Medizinische Kamerabilder	Wissenschaftliche Forschung <ul style="list-style-type: none"> • Thorax- und gefäßchirurgischen Eingriffe • EEG-Überwachung • In der Schlafklinik • Auf der Schlaganfallstation 	Einwilligung	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	Die von UZ Gent zu diesem Zweck verarbeiteten personenbezogenen Daten werden von UZ Gent nicht an Dritte weitergegeben.

	<ul style="list-style-type: none"> • Neonatologische Intensivstation • Überwachung bestimmter Störungen <p>Intensivmedizin</p> <p>Medizinische Ausbildung</p>	<p>Erforderlich für Zwecke der Präventivmedizin oder der medizinischen Diagnose</p> <p>Allgemeines Interesse</p>		
Medizinische Tonaufnahmen	<ul style="list-style-type: none"> • Wissenschaftliche Forschung • Thorax- und gefäßchirurgischen Eingriffe • EEG-Überwachung 	Einwilligung	Mindestens 30 Jahre und bis zu 50 Jahre nach dem letzten Patientenkontakt	

6.6.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, die personenbezogenen Daten des Patienten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

Für bestimmte Zwecke, wie oben erwähnt, gibt der Patient seine Einwilligung, indem er einer bestimmten Verarbeitung ausdrücklich zustimmt (z. B. durch Ankreuzen eines Kästchens auf einem Informationsformular vor Beginn der Untersuchung). Der Patient hat das Recht, seine Einwilligung jederzeit zu widerrufen. Der Widerruf einer solchen Einwilligung berührt nicht die Rechtmäßigkeit der aufgrund der Einwilligung vor dem Widerruf erfolgten Verarbeitung.

6.6.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die UZ Gent zum Zwecke der wissenschaftlichen Forschung verarbeitet, wurden direkt bei der betroffenen Person erhoben, es sei denn, diese war dazu nicht in der Lage.

Personenbezogene Gesundheitsdaten werden beim Patienten selbst erhoben, es sei denn, der Zweck der Verarbeitung erfordert eine andere Erhebungsmethode oder der Patient selbst ist nicht in der Lage, die Daten zur Verfügung zu stellen.

6.6.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen über Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

6.7 Wartung und Betrieb der Website

Um die Website und das Patientenportal von UZ Gent zu unterhalten und zu betreiben, verwendet UZ Gent verschiedene Cookies auf ihrer Website. Weitere Informationen finden Sie in unserer [Cookie-Erklärung](#).

Art der Cookies	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Wesentliche und funktionale Cookies	Ordnungsgemäßes Funktionieren und Sicherheit der Website	Berechtigtes Interesse	<u>Siehe Cookie-Erklärung</u>	Keine externe Kommunikation
Cookies für Präferenzen, Statistiken und soziale Medien	Verbesserung des Browsing-Erlebnisses	Einwilligung	<u>Siehe Cookie-Erklärung</u>	<u>Siehe Cookie-Erklärung</u>

6.7.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, die personenbezogenen Daten des Patienten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

Wenn UZ Gent die oben genannten personenbezogenen Daten für die oben genannten Zwecke auf der Rechtsgrundlage eines berechtigten Interesses verarbeitet, ist das ordnungsgemäße Funktionieren und die Sicherheit der Website das berechtigte Interesse von UZ Gent. Die oben genannten Verarbeitungen personenbezogener Daten, die die Verarbeitung personenbezogener Daten mittels Cookies betreffen, sind keine Verarbeitungstätigkeiten, die UZ Gent als staatliche Einrichtung in Erfüllung ihrer Aufgaben durchführt. Nach sorgfältiger Abwägung der verschiedenen Interessen ist UZ Gent der Ansicht, dass sein Interesse das des Patienten aus den oben genannten Gründen überwiegt. Zu diesem Zweck kann UZ Gent nachweisen, dass:

1. die Interessen, die mit der Verarbeitung verfolgt werden, als rechtmäßig anerkannt werden können („**Zweckprüfung**“);
2. die beabsichtigte Verarbeitung für die Verwirklichung dieser Interessen erforderlich ist („**Erforderlichkeitsprüfung**“); und
3. Die Abwägung dieser Interessen mit den Interessen, grundlegenden Freiheiten und Rechten der betroffenen Personen zugunsten des für die Verarbeitung Verantwortlichen ausfällt („**Abwägungsprüfung**“).

Für bestimmte Zwecke, wie oben erwähnt, gibt der Patient seine Einwilligung, indem er einer bestimmten Verarbeitung ausdrücklich zustimmt (z. B. durch Ankreuzen des Kästchens seiner Wahl). Der Patient hat das Recht, seine Einwilligung jederzeit zu widerrufen. Der Widerruf einer solchen Einwilligung berührt nicht die Rechtmäßigkeit der aufgrund der Einwilligung vor dem Widerruf erfolgten Verarbeitung.

6.7.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die UZ Gent im Rahmen von Cookies verarbeitet, werden direkt vom Nutzer der Website erhoben, wenn dieser die Website besucht und/oder wenn der Nutzer diesen Cookies zustimmt.

6.7.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen über Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

6.8 Nutzung des WLAN-Netzwerks des Krankenhauses

Daten der Kategorie	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Identifikationsnummer des Geräts	Verhinderung des Missbrauchs des Netzwerks	Berechtigtes Interesse	1 Jahr	Keine externe Kommunikation, es sei denn, das Netz wird illegal genutzt, dann können die Daten an Justizbehörden weitergegeben werden.
Surfverhalten durch Protokollierung	Verhinderung des Missbrauchs des Netzwerks	Berechtigtes Interesse	1 Jahr	Keine externe Kommunikation, es sei denn, das Netz wird illegal genutzt, dann können die Daten an Justizbehörden weitergegeben werden.

6.8.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, die personenbezogenen Daten des Patienten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

Wenn UZ Gent die oben genannten personenbezogenen Daten für die oben genannten Zwecke auf der Rechtsgrundlage eines berechtigten Interesses verarbeitet, ist die Verhinderung des Missbrauchs des Netzwerks das berechtigte Interesse von UZ Gent. Die oben genannten Verarbeitungen personenbezogener Daten, die die Verarbeitung personenbezogener Daten mittels Protokollierung betreffen, sind keine Verarbeitungstätigkeiten, die UZ Gent als staatliche Einrichtung in Erfüllung ihrer Aufgaben durchführt. Nach sorgfältiger Abwägung der verschiedenen Interessen ist UZ Gent der Ansicht, dass sein Interesse das des Patienten aus den oben genannten Gründen überwiegt. Zu diesem Zweck kann UZ Gent nachweisen, dass:

1. die Interessen, die mit der Verarbeitung verfolgt werden, als rechtmäßig anerkannt werden können („**Zweckprüfung**“)
2. die beabsichtigte Verarbeitung für die Verwirklichung dieser Interessen erforderlich ist („**Erforderlichkeitsprüfung**“) und
3. die Abwägung dieser Interessen mit den Interessen, grundlegenden Freiheiten und Rechten der betroffenen Personen zugunsten des für die Verarbeitung Verantwortlichen ausfällt („**Abwägungsprüfung**“).

6.8.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die UZ Gent im Rahmen der Protokollierung verarbeitet, werden direkt vom Benutzer erhoben, wenn dieser das WLAN-Netzwerk des Krankenhauses nutzt.

6.8.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Meer informatie over de rechten t.a.v. deze verwerking van persoonsgegevens kunt u hier vinden.

6.9 Kommunikation

Daten der Kategorie	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Identität des Anrufers	Sicherheit der Patienten und/oder des Personals	Allgemeines Interesse	1 Jahr	Keine externe Kommunikation, es sei denn, dies ist im Rahmen eines Strafverfahrens gesetzlich vorgeschrieben.

6.9.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, die personenbezogenen Daten des Patienten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

6.9.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die UZ Gent im Rahmen der Sicherheit des Patienten bzw. des Mitarbeiters verarbeitet, wurden direkt von der betroffenen Person eingeholt.

6.9.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen zu den Rechten in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

6.10 Registrierung von Beschwerden beim Büro des Bürgerbeauftragten

Jeder Patient des Krankenhauses hat das Recht, beim Bürgerbeauftragten des Krankenhauses eine Beschwerde über die Dienstleistungen von UZ Gent einzureichen (z. B. Beschwerden über die Pflege, den Aufenthalt und die Betreuung).

Im Rahmen dieses Zwecks verarbeiten wir die folgenden personenbezogenen Daten:

Kategorie der personenbezogenen Daten	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Angaben zur Identifizierung	Weiterverfolgung und Bearbeitung von Beschwerden	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	1 Jahr nach Schließen des Vorgangs	Leistungserbringer, über den die Beschwerde eingereicht wird, der Chefarzt des Krankenhauses, die Rechtsabteilung des Krankenhauses,
Gesundheitsbezogene Daten	Weiterverfolgung und Bearbeitung der Beschwerde	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	1 Jahr nach Schließen des Vorgangs	professionelle Berater (z. B. Rechtsanwälte von UZ Gent), Versicherungsträger, bei spezifischen Fragen zur Verarbeitung von

Kontaktdaten	Weiterverfolgung und Bearbeitung von Beschwerden	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	1 Jahr nach Schließen des Vorgangs	personenbezogenen Daten: der Datenschutzbeauftragte von UZ Gent.
Finanzverwaltungsdaten	Weiterverfolgung und Bearbeitung von Beschwerden	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	1 Jahr nach Schließen des Vorgangs	
Angaben zum vorläufigen Verwalter/Familienmitgliedern	Weiterverfolgung und Bearbeitung von Beschwerden	Notwendig, um einer gesetzlichen Verpflichtung nachzukommen	1 Jahr nach Schließen des Vorgangs	

6.10.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, die personenbezogenen Daten des Patienten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

Die gesetzliche Verpflichtung, auf deren Grundlage UZ Gent die personenbezogenen Daten für die oben genannten Zwecke verarbeitet, ist: das koordinierte Gesetz vom 10. Juli 2008 über Krankenhäuser und andere Pflegeeinrichtungen (im Folgenden das Krankenhausgesetz) und Anhang A.III . Artikel 9 ff. des königlichen Erlasses vom 23. Oktober 1964 zur Festlegung der von Krankenhäusern und ihren Diensten einzuhaltenden Normen.

6.10.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die UZ Gent im Zusammenhang mit der Registrierung von Beschwerden im Rahmen des Bürgerbeauftragtendienstes verarbeitet, wurden direkt bei der betroffenen Person eingeholt, es sei denn, diese war dazu nicht in der Lage.

6.10.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen über Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

6.11 Soziale Dienste

Der „soziale Dienst“ des Krankenhauses bedeutet zum Beispiel die Betreuung von Patienten, näher bestimmt als:

- Entlassung aus dem Krankenhaus,
- Unterstützung bei der Beantragung von häuslichen Pflegediensten,
- Aufnahme in ein Pflege- oder Rehabilitationszentrum; und/oder
- finanzielle und verwaltungstechnische Angelegenheiten.

Auch psychosoziale Unterstützung kann angeboten werden.

Kategorie der personenbezogenen Daten	Zweckbestimmung(en) der Verarbeitung	Rechtsgrundlage	Aufbewahrungsfrist	Kategorie des Empfängers
Angaben zur Identifizierung	Soziale Dienste	Einwilligung	Solange soziale Dienstleistungen erbracht werden	Externe Pflegekräfte, informelle Pflegekräfte, staatliche Stellen und Versicherungsvereine auf Gegenseitigkeit.
Kontaktdaten	Soziale Dienste	Einwilligung	Solange soziale Dienstleistungen erbracht werden	
Gesundheitsbezogene Daten	Soziale Dienste	Einwilligung	Solange soziale Dienstleistungen erbracht werden	

6.11.1 Rechtsgrundlage

Wir werden Sie im Voraus informieren, wenn UZ Gent beabsichtigt, die personenbezogenen Daten des Patienten für andere als die in dieser Datenschutzerklärung genannten Zwecke zu verarbeiten.

Für bestimmte Zwecke, wie oben erwähnt, gibt der Patient seine Einwilligung, indem er einer bestimmten Verarbeitung ausdrücklich zustimmt. Der Patient hat das Recht, seine Einwilligung jederzeit zu widerrufen. Der Widerruf einer solchen Einwilligung berührt nicht die Rechtmäßigkeit der aufgrund der Einwilligung vor dem Widerruf erfolgten Verarbeitung.

6.11.2 Wie haben wir diese personenbezogenen Daten erhalten?

Die personenbezogenen Daten, die UZ Gent zum Zwecke der sozialen Dienstleistung verarbeitet, wurden direkt bei der betroffenen Person erhoben, es sei denn, diese war dazu nicht in der Lage.

Personenbezogene Gesundheitsdaten werden beim Patienten selbst erhoben, es sei denn, der Zweck der Verarbeitung erfordert eine andere Erhebungsmethode oder der Patient selbst ist nicht in der Lage, die Daten zur Verfügung zu stellen.

6.11.3 Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten

Weitere Informationen über Ihre Rechte in Bezug auf diese Verarbeitung personenbezogener Daten finden Sie [hier](#).

6.12 Wissenschaftliche Forschung

Die wissenschaftliche Forschung ist eine der Kernaufgaben des Universitair Ziekenhuis Gent.

Die Zwecke sind zum einen die Erfassung von Gesundheitsdaten für wissenschaftliche Zwecke, für die UZ Gent Auftraggeber ist, und zum anderen die Verarbeitung von Daten, die im Rahmen der Sicherheitsberichterstattung durch UZ Gent erforderlich sind.

Die Datenschutzbestimmungen „Wissenschaftliche Forschung UZ Gent“ finden Sie [hier](#).

7 Übermittlung Ihrer Daten in ein Land außerhalb des EWR (Europäischer Wirtschaftsraum)

UZ Gent übermittelt grundsätzlich keine personenbezogenen Daten von Patienten in Länder außerhalb des EWR. Wenn UZ Gent dies dennoch tut, wird sie den Patienten vorher konsultieren und sich vergewissern, ob das Bestimmungsland ein angemessenes Schutzniveau bietet. Wenn das Land, in das UZ Gent Daten übermitteln möchte, keine angemessenen Garantien bietet, wird UZ Gent selbst angemessene Garantien durchsetzen, und zwar mit Hilfe von Musterverträgen (Anlage 2), die von der Europäischen Kommission zur Verfügung gestellt werden, oder anderen akzeptierten Maßnahmen.

8 Ihre Rechte in Bezug auf die Verarbeitung Ihrer personenbezogenen Daten

8.1 Rechte in Bezug auf UZ Gent

Der Klarheit halber werden im Folgenden Ihre Rechte in Bezug auf Ihre personenbezogenen Daten erläutert. Wenn Sie eines dieser Rechte geltend machen möchten, senden Sie bitte eine E-Mail an dpo@uzgent.be.

8.1.1 Recht auf Einsicht und Kopie

Sie haben das Recht, eine Bestätigung darüber zu erhalten, ob personenbezogene Daten, die Sie betreffen, verarbeitet werden, und wenn dies der Fall ist, Zugang zu diesen Daten zu erhalten und die folgenden Informationen zu bekommen:

- Die Zwecke der Verarbeitung;
- Die betroffenen Kategorien von personenbezogenen Daten;
- Die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben wurden oder werden, insbesondere Empfänger in Drittländern oder internationale Organisationen;
- Wenn möglich, den Zeitraum, für den die personenbezogenen Daten voraussichtlich gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieses Zeitraums;
- Sie haben das Recht, von UZ Gent die Berichtigung oder Löschung personenbezogener Daten zu verlangen oder die Verarbeitung der Sie betreffenden personenbezogenen Daten einzuschränken, sowie das Recht, einer solchen Verarbeitung zu widersprechen;
- Sie haben das Recht, eine Beschwerde bei einer Datenschutzbehörde einzureichen;
- Falls die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, alle verfügbaren Informationen über die Quelle dieser Daten;
- Das Vorhandensein einer automatisierten Entscheidungsfindung, einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4, und – zumindest in diesen Fällen – nützliche Informationen.

Sie haben auch das Recht, eine kostenlose Kopie dieser Informationen von UZ Gent zu erhalten, indem Sie eine E-Mail an dpo@uzgent.be senden.

Im Rahmen Ihres Rechts auf Einsichtnahme und Vervielfältigung behält sich UZ Gent das Recht vor, bestimmte personenbezogene Daten oder Informationen in den angeforderten Dokumenten unleserlich zu machen oder zu verbergen (z. B. durch Schwärzung), um die Rechte anderer zu schützen.

8.1.2 Recht auf Berichtigung und Ergänzung

Wenn Sie der Meinung sind, dass UZ Gent unvollständige oder falsche Daten über Sie speichert, haben Sie das Recht, UZ Gent aufzufordern, diese Daten kostenlos zu korrigieren oder zu ergänzen.

Wenn die Daten unrichtig oder unvollständig sind, kann auf einfachen Antrag eine Ergänzung gewährt werden. Hinsichtlich der Gesundheitsdaten kann eine Verbesserung nur nach Zustimmung des behandelnden Arztes oder des Chefarztes zugelassen werden.

Wird eine Korrektur eines medizinisch subjektiven Gutachtens oder von Daten beantragt, kann auf Antrag eine Ergänzung, nicht aber eine Korrektur gewährt werden.

8.1.3 Recht auf Löschung

Unter bestimmten Umständen können Sie UZ Gent auffordern, Ihre personenbezogenen Daten zu löschen. Dies ist in den folgenden Fällen möglich:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder anderweitig verarbeitet wurden, nicht mehr erforderlich;
- Sie widerrufen Ihre Einwilligung, auf der die Verarbeitung beruhte, und es gibt keinen anderen Rechtsgrund für die Verarbeitung;
- Sie legen Widerspruch gegen die Verarbeitung Ihrer personenbezogenen Daten ein und es liegen keine vorrangigen berechtigten Gründe für die Aufbewahrung Ihrer Daten vor;
- UZ Gent verarbeitet Ihre personenbezogenen Daten unrechtmäßig;
- Die personenbezogenen Daten müssen gelöscht werden, um bestimmte gesetzliche Bestimmungen zu erfüllen, die bei UZ Gent liegen.

Aus verschiedenen Gründen kann es sein, dass UZ Gent Ihren Antrag auf Löschung ablehnen muss. Dies trifft zum Beispiel in diesen Fällen zu:

- Zur Erfüllung einer gesetzlichen Verarbeitungsverpflichtung, die UZ Gent nach europäischem oder mitgliedstaatlichem Recht obliegt;
- Zur Erfüllung einer Aufgabe von allgemeinem Interesse oder zur Ausübung öffentlicher Gewalt, die UZ Gent übertragen wurde;
- Aus Gründen des allgemeinen Interesses im Bereich der öffentlichen Gesundheit;
- Wenn die Daten Teil eines Archivs sind, das zum Zweck der wissenschaftlichen Forschung aufbewahrt wird, und die Entfernung Ihrer Daten die weitere Forschung unmöglich zu machen droht;
- wenn die Daten für die Begründung, Ausübung oder Begründetheit eines Rechtsanspruchs erforderlich sind.

8.1.4 Recht auf Einschränkung der Verarbeitung

In einer begrenzten Anzahl von Fällen können Sie beantragen, dass Ihre personenbezogenen Daten aufbewahrt, aber nicht verarbeitet werden (*Aussetzen* der Verarbeitung):

- Die Richtigkeit der personenbezogenen Daten wird von Ihnen bestritten, und zwar während eines Zeitraums, der es UZ Gent ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen;
- Die Verarbeitung ist unrechtmäßig und Sie widersprechen der Löschung der personenbezogenen Daten und beantragen stattdessen die Einschränkung ihrer Verwendung;

- UZ Gent benötigt die personenbezogenen Daten nicht mehr für die oben genannten Verarbeitungszwecke, aber Sie benötigen sie für die Begründung, Ausübung oder Begründetheit eines Rechtsanspruchs;
- Sie haben gegen die Verarbeitung personenbezogener Daten durch UZ Gent Widerspruch eingelegt, solange die Antwort auf die Frage aussteht, ob die berechtigten Gründe von UZ Gent Ihre eigenen überwiegen.

8.1.5 Recht auf Übertragbarkeit von Daten

Wenn UZ Gent Daten auf der Grundlage Ihrer ausdrücklichen Einwilligung oder auf der Grundlage einer mit UZ Gent getroffenen Vereinbarung verarbeitet, haben Sie als Patient auch das Recht, eine elektronische Kopie Ihrer personenbezogenen Daten an sich selbst oder direkt an eine andere Einrichtung oder Person Ihrer Wahl zu übermitteln.

Diese Übertragung muss in einem strukturierten, gemeinsamen und maschinenlesbaren Format erfolgen.

8.1.6 Recht auf Einspruch

Wenn die Verarbeitung Ihrer Daten nur (i) auf dem Rechtsgrund beruht, dass dies für UZ Gent zur Erfüllung einer Aufgabe von allgemeinem Interesse notwendig ist, oder (ii) auf den berechtigten Interessen von UZ Gent, können Sie einen begründeten Widerspruch einlegen.

UZ Gent wird den begründeten Widerspruch respektieren, es sei denn, es liegen zwingende berechnete Gründe vor, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Daten stehen im Zusammenhang mit der Geltendmachung, Ausübung oder Begründetheit eines Rechtsanspruchs.

Die betroffene Person kann sich niemals der Verarbeitung personenbezogener Daten widersetzen, die UZ Gent für die Erfüllung einer Vereinbarung oder als Folge gesetzlicher Verpflichtungen benötigt.

Werden personenbezogene Daten von UZ Gent zum Zwecke der wissenschaftlichen Forschung verarbeitet, so haben Sie das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, gegen die Verarbeitung Sie betreffender personenbezogener Daten Widerspruch einzulegen, es sei denn, die Verarbeitung ist für die Erfüllung einer Aufgabe von allgemeinem Interesse erforderlich.

8.1.7 Recht, seine/ihre Einwilligung jederzeit zu widerrufen

Beruht die Verarbeitung personenbezogener Daten auf Ihrer vorherigen Einwilligung, können Sie diese Einwilligung jederzeit kostenlos widerrufen.

Der Widerruf der Einwilligung hat zur Folge, dass UZ Gent die betreffenden Daten nicht mehr verarbeiten darf. Der Widerruf der Einwilligung hat keinen Einfluss auf die Gültigkeit der Verarbeitung.

8.1.8 Recht auf Widerspruch gegen automatisierte Unterstützung

UZ Gent macht keinen Gebrauch von automatisierten Entscheidungsprozessen.

8.2 Beschwerde über UZ Gent

Haben Sie Beschwerden oder Fragen bezüglich der Verarbeitung Ihrer personenbezogenen Daten durch UZ Gent?

Dann können Sie sich jederzeit an unseren Datenschutzbeauftragten unter der folgenden Adresse wenden: Data Protection Officer UZ Gent, C. Heymanslaan 10, 9000 Gent oder per E-Mail: dpo@uzgent.be.

8.3 Beschwerde bei der Datenschutzbehörde

Wenn Sie der Meinung sind, dass Sie eine Beschwerde in Bezug auf den Schutz der Privatsphäre haben, können Sie sich auch an die belgische Datenschutzbehörde wenden (www.gegevensbeschermingsautoriteit.be) in 1000 Brüssel, Drukpersstraat 35; oder +32(0)2 274 48 00; oder contact@apd-gba.be.

9 Inkrafttreten und Änderungen der Datenschutzerklärung

Diese Datenschutzerklärung ist am 30. Mai 2022 in Kraft getreten.

UZ Gent behält sich das Recht vor, diese Datenschutzbestimmungen jederzeit zu ändern. Änderungen werden vom Verwaltungsausschuss von UZ Gent und, soweit es sich um Gesundheitsdaten handelt, auf Anraten der Ärztekammer vorgenommen.

Das Datum der letzten Änderung dieser Datenschutzerklärung finden Sie oben rechts auf dieser Seite.

Die Änderungen werden auf der Website von UZ Gent bekanntgegeben. Dort wird auf die entsprechenden Artikel verwiesen, in denen die Änderungen vorgenommen werden.

10 Anhänge

10.1 ANHANG 1: Begriffe in dieser Datenschutzerklärung

- **Anonyme Daten:** Alle Daten, die nicht (oder nicht mehr) mit einer identifizierten oder identifizierbaren Person in Verbindung gebracht werden können und die daher keine personenbezogenen Daten (mehr) sind.
- **Biometrische Daten:** Personenbezogene Daten, die sich aus einer spezifischen technischen Verarbeitung ergeben, die sich auf die physischen, physiologischen oder verhaltensbezogenen Merkmale einer natürlichen Person beziehen und die eine eindeutige Identifizierung dieser natürlichen Person ermöglichen oder zu ihr beitragen (z. B. Gesichtsbilder oder Fingerabdruckdaten).
- **Genetische Daten:** Personenbezogene Daten über die ererbten oder erworbenen genetischen Merkmale einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe dieser natürlichen Person stammen.
- **Pseudonymisierte personenbezogene Daten:** Personenbezogene Daten, die so verarbeitet werden, dass sie ohne Hinzuziehung zusätzlicher Daten nicht mit bestimmten natürlichen Personen in Verbindung gebracht werden können, sofern diese zusätzlichen Daten gesondert aufbewahrt werden und technische und organisatorische Maßnahmen getroffen werden, die gewährleisten, dass die personenbezogenen Daten nicht mit einer identifizierten oder identifizierbaren natürlichen Person in Verbindung gebracht werden. Es handelt sich also nicht um anonyme Daten, da die natürliche Person nach der Pseudonymisierung identifizierbar ist.
- **Mitarbeiter:** Arbeitnehmer und/oder andere Angestellte von UZ Gent und/oder Freiberufler innerhalb von UZ Gent.
- **Patient (oder „Sie“):** Die natürliche Person, die im Krankenhaus aufgenommen oder behandelt wird und deren personenbezogene Daten verarbeitet werden (auch als „**betroffene Person**“ bezeichnet).
- **Daten über die Gesundheit (oder „Gesundheitsdaten“):** Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen, einschließlich Daten über erbrachte Gesundheitsdienstleistungen, mit denen Informationen über ihren Gesundheitszustand gegeben werden.
- **Personenbezogene Daten:** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, z. B. einen Patienten, beziehen. Eine identifizierbare Person ist eine natürliche Person, die direkt oder indirekt identifiziert werden kann, insbesondere mithilfe eines Identifikators wie einem Namen, einer Kennnummer (z. B. der nationalen Registernummer), einem Geburtsdatum, Standortdaten, einer Online-Kennung (z. B. einer E-Mail-Adresse oder einer IP-Adresse) oder mithilfe eines oder mehrerer Faktoren, die Ausdruck seiner/ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.
- **Einwilligung:** Jede ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und auf eindeutige Weise abgegebene Willensbekundung, mit der der Patient oder sein gesetzlicher Vertreter durch eine Erklärung oder eine eindeutige aktive Handlung zustimmt, dass personenbezogene Daten des Patienten verarbeitet werden dürfen.
- **Verarbeiter:** Natürliche oder juristische Person, Behörde, Dienst oder andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet, ohne dem für die Verarbeitung Verantwortlichen unmittelbar unterstellt zu sein.

- **Verarbeitung:** jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie Erheben, Erfassen, Ordnen, Strukturieren, Speichern, Verändern, Auslesen, Abfragen, Verwenden, Bekanntgeben durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, Abgleich, Verknüpfung, Sperrung, Löschung oder Vernichtung personenbezogener Daten.
- **Für die Verarbeitung Verantwortlicher:** Natürliche oder juristische Person, Behörde, Dienststelle oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.
- **Rechtsvorschriften über personenbezogene Daten:** (i) die Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG ab dem 25. Mai 2018, (ii) das belgische Gesetz vom 30. Juli 2018 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und (iii) alle sonstigen geltenden oder künftigen Rechtsvorschriften, die sich auf den Schutz der Privatsphäre und die Verarbeitung personenbezogener Daten beziehen oder auswirken.

10.2 ANHANG 2: Standardvertragsklauseln für die Übermittlung personenbezogener Daten in ein Land außerhalb des EWR

COMMISSION IMPLEMENTING DECISION (EU) 2021/914

of 4 June 2021

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

(Text with EEA relevance)

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ⁽¹⁾ for the transfer of personal data to a third country.
- (b) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)
- have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8: Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12: Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16 (e);
 - (viii) Clause 18: Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business

secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ⁽⁴⁾ (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ⁽⁸⁾ The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ⁽¹⁾ at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ⁽¹²⁾;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16 (d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14 (e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14 (e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of _____ (*specify Member State*).
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

⁽⁴⁾ Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are

aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

- (²) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.
- (³) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.
- (⁴) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.
- (⁵) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.
- (⁶) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.
- (⁷) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.
- (⁸) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
- (⁹) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
- (¹⁰) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.
- (¹¹) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.
- (¹²) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: University Hospital Ghent

Address: C. Heymanslaan 10 – 9000 Ghent

Contact person's name, position and contact details: Katya Van Driessche – Data Protection Officer – dpo@uzgent.be

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): controller

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

...

Categories of personal data transferred

...

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

...

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

...

Nature of the processing

...

Purpose(s) of the data transfer and further processing

...

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

...

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

...

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

...

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2.

...
