

UZ Gent - Déclaration de confidentialité : Patient

Protection des données personnelles des patients

L'objectif principal de cette déclaration de confidentialité est de vous informer, en tant que patient, sur la manière et les raisons pour lesquelles l'UZ Gent traite vos données personnelles en tant que patient et sur les droits que vous pouvez exercer.

Table des matières

1	Qui est le responsable du traitement de vos données personnelles ?	2
2	Délégué à la protection des données	2
3	Notions reprises dans la présente déclaration de confidentialité	2
4	Généralités	2
5	Quelles sont les données personnelles traitées par l'UZ Gent ?	3
6	Finalités du traitement et fondements juridiques de ce traitement	3
6.1	Soins aux patients	4
6.2	Administration des patients	5
6.3	Communication électronique en matière de soins avec le patient via le portail patient	6
6.4	Enregistrement des patients	8
6.5	Sécurité physique	10
6.6	Enregistrement par caméra de surveillance médicale et enregistrement audio	11
6.7	Maintenance et exploitation du site Web	12
6.8	Utilisation du réseau wifi de l'hôpital	13
6.9	Communication	14
6.10	Enregistrement des réclamations auprès du Bureau du Médiateur	14
6.11	Services sociaux	15
6.12	Recherche scientifique	16
7	Transfert de vos données vers un pays situé en dehors de l'EEE (Espace Économique Européen)	16
8	Vos droits concernant le traitement de vos données personnelles	17
8.1	Droits vis-à-vis de l'UZ Gent	17
8.2	Plainte à l'encontre de l'UZ Gent	19
8.3	Plainte auprès de l'Autorité chargée de la protection des données	19
9	Entrée en vigueur et modifications de la déclaration de confidentialité	19

10 ANNEXE	21
10.1 Annexe 1 : Notions reprises dans la présente déclaration de confidentialité	21
10.2 Annexe 1 : Clauses contractuelles types pour les transferts de données personnelles vers un pays hors EEE	23

1 Qui est le responsable du traitement de vos données personnelles ?

L'Universitair Ziekenhuis Gent, institution publique ayant son siège social à C. Heymanslaan 10, 9000 Gent et inscrite à la Banque-Carrefour des Entreprises sous le numéro 0232.987.862 (ci-après "UZ Gent", ou "nous") est responsable du traitement de vos données personnelles en tant que donateur tel que décrit dans cette déclaration de confidentialité.

L'UZ Gent fait partie de l'Université de Gand, établissement public doté de la personnalité juridique en vertu du décret spécial du 26 juin 1999, dont le siège administratif est situé à 9000 Gent, Sint-Pietersnieuwstraat 25, et qui est inscrit à la Banque-Carrefour des Entreprises sous le numéro 0248.015.142

2 Délégué à la protection des données

L'UZ Gent a nommé un délégué à la protection des données. Si vous avez des questions ou des commentaires sur le traitement de vos données personnelles, veuillez contacter notre délégué à la protection des données à l'adresse suivante Délégué à la protection des données UZ Gent, C. Heymanslaan 10, 9000 Gent, dpo@uzgent.be.

3 Notions reprises dans la présente déclaration de confidentialité

Plusieurs notions sont utilisées dans la présente déclaration de confidentialité. Veuillez vous référer à l'ANNEXE 1.

4 Généralités

La présente déclaration de confidentialité a été préparée en application, entre autres, des dispositions suivantes :

- La législation portant sur les Données personnelles en application du Règlement UE 2016/679 du 27 avril 2016 et de la loi du 5 septembre 2018 relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
- La loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins (ci-après « loi hospitalière ») et l'Annexe A. III. L'Article 9 quater de l'Arrêté royal du 23 octobre 1964 portant fixation des normes auxquelles les hôpitaux et leurs services doivent répondre
- La loi du 22 août 2002 relative aux droits du patient
- La loi relative à l'assurance obligatoire soins de santé coordonnée le 14 juillet 1994
- L'AR du 3 mai 1999 relatif au dossier médical général
- La loi du 1er mai 2015 relative à l'exercice des professions des soins de santé
- La loi sur les hôpitaux du 7 août 1987, y compris le dossier des patients
- La loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance
- La loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé

5 Quelles sont les données personnelles traitées par l'UZ Gent ?

Catégorie de données à caractère personnel	Données personnelles spécifiques
Données d'identification	Nom, prénom, lieu de naissance, date de naissance, nationalité, photo d'identité
Numéro de registre national	Numéro de registre national (délibération n° 50/2008 du Comité sectoriel du numéro de registre national)
Coordonnées	Adresse, adresse électronique, numéro de téléphone
Données relatives à la santé	Toutes les données relatives à la santé physique ou mentale d'une personne physique, y compris les données concernant les services de santé qui fournissent des informations sur l'état de santé de la personne concernée
Données comptables	Numéro de compte
Données sociales	Situation familiale, besoins spécifiques
Données relatives aux mutuelles et aux assurances	Nom de la mutuelle, numéro de la mutuelle
Données relatives à un administrateur/des membres de la famille	Coordonnées d'une personne de confiance, le cas échéant
Données génétiques	Informations résultant d'un test ADN
Données biométriques	Empreintes digitales, image faciale, iris
Images d'une caméra de surveillance	Visages, statures, voitures, plaques d'immatriculation
Images de caméras de surveillance médicale	Comportements, réactions, images médicalement pertinentes
Enregistrements audio à caractère médical	Enregistrements audio humains à caractère médical
Cookies	Essentiels, fonctionnels, préférentiels, sociaux

6 Finalités du traitement et fondements juridiques de ce traitement

Il est possible que l'UZ Gent traite différents types de données personnelles à des fins différentes. Vous trouverez ci-dessous, pour chaque finalité, quelles sont les données personnelles traitées par l'UZ Gent, sur quelle base le traitement est effectué, pendant combien de temps les données sont traitées et avec qui nous pouvons les partager.

Dans ce qui suit, nous développons les objectifs suivants :

1. Soins aux patients ;
2. Administration des patients ;
3. Enregistrement des patients ;
4. Sécurité physique ;
5. Enregistrement par caméra de surveillance médicale et enregistrement audio ;
6. Maintenance et exploitation du site Web ;
7. Utilisation du réseau wifi de l'hôpital ;
8. Communication
9. Enregistrement des réclamations auprès du Bureau du Médiateur ;
10. Services sociaux.
11. Recherche scientifique

6.1 Soins aux patients

L'objectif des soins dispensés aux patients doit être compris comme suit :

- Soins préventifs (et diagnostic médical) ; et/ou
- Prestation de soins (y compris le traitement du patient).

Catégorie de données à caractère personnel	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de destinataires
Données d'identification	Soins préventifs	Nécessaire pour remplir une obligation légale	Au moins 30 ans et jusqu'à 50 ans après le dernier contact avec le patient	Les membres du personnel interne ayant une relation de soins avec la personne concernée, le médecin traitant du patient, les prestataires de soins, le représentant légal. Si nous sommes obligés de le faire en vertu de la réglementation ou de la jurisprudence, également vis-à-vis des autorités ou de la mutuelle.
	Prestation de soins	Nécessaire pour remplir une obligation légale		
Coordonnées	Soins préventifs	Nécessaire pour remplir une obligation légale	Au moins 30 ans et jusqu'à 50 ans après le dernier contact avec le patient	
	Prestation de soins	Nécessaire pour remplir une obligation légale		
Données relatives à la santé	Soins préventifs	Nécessaire pour remplir une obligation légale	Au moins 30 ans et jusqu'à 50 ans après le dernier contact avec le patient	
	Prestation de soins	Nécessaire pour remplir une obligation légale		
Données sociales	Prestation de soins	Nécessaire pour remplir une obligation légale	Au moins 30 ans et jusqu'à 50 ans après le dernier contact avec le patient	
Données comptables	Soins préventifs	Nécessaire pour remplir une obligation légale	Au moins 30 ans et jusqu'à 50 ans après le dernier contact avec le patient	Collaborateurs

6.1.1 Fondements juridiques

Nous vous informerons au préalable si l'UZ Gent a l'intention de traiter vos données personnelles à des fins autres que celles mentionnées dans la présente déclaration de confidentialité.

L'obligation légale sur la base de laquelle l'UZ Gent traite les données à caractère personnel aux fins susmentionnées est : la loi coordonnée du 10 juillet 2008 relative aux hôpitaux et autres établissements de soins (ci-après Loi hospitalière) et l'annexe A.III article 9quater de l'Arrêté Royal du 23 octobre 1964 déterminant les normes à respecter par les hôpitaux et leurs services.

6.1.2 Comment avons-nous obtenu ces données personnelles ?

Les données personnelles que l'UZ Gent traite dans le cadre des soins aux patients ont été reçues directement du patient, à moins que celui-ci n'ait pas été en mesure de les communiquer.

6.1.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données personnelles [ici](#).

6.2 Administration des patients

Par administration des patients, nous entendons ce qui suit :

- Gestion et suivi des services de santé par l'identification et le suivi des patients ("gestion et identification") ; et/ou
- Traitement du suivi du séjour et du traitement des patients à des fins de facturation ("suivi et facturation").

Catégorie de données à caractère personnel	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de destinataires
Données d'identification	Gestion et identification	Nécessaire pour remplir une obligation légale	7 ans	Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière
	Suivi et facturation	Nécessaire à l'exécution de l'accord conclu avec l'UZ Gent		Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière, avocat, huissier, centre d'appel Prestataires de services tiers
Coordonnées	Gestion et identification	Nécessaire pour remplir une obligation légale	7 ans	Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière
	Suivi et facturation	Nécessaire à l'exécution de l'accord conclu avec l'UZ Gent		Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière, avocat, huissier, centre d'appel Prestataires de services tiers
Données relatives à la santé	Gestion et identification	Nécessaire pour remplir une obligation légale	7 ans	Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière
	Suivi et facturation	Nécessaire à l'exécution de l'accord conclu avec l'UZ Gent		Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière, avocat, huissier, centre d'appel
Données comptables	Gestion et identification	Nécessaire pour remplir une obligation légale	7 ans	Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière
Données sociales	Gestion et identification	Nécessaire pour remplir une obligation légale	7 ans	Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière
	Suivi et facturation	Nécessaire à l'exécution de l'accord conclu avec l'UZ Gent		Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière, avocat, huissier, centre d'appel
Données relatives à l'administrateur provisoire/à la famille	Gestion et identification	Nécessaire pour remplir une obligation légale	7 ans	Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière

Données relatives à la mutuelle et à l'assurance	Gestion et identification	Nécessaire pour remplir une obligation légale	7 ans	Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière
	Suivi et facturation	Nécessaire à l'exécution de l'accord conclu avec l'UZ Gent		Institutions de sécurité sociale, mutuelle, compagnie d'assurances hospitalière, avocat, huissier, centre d'appel

6.2.1 Fondements juridiques

Nous vous informerons à l'avance si l'UZ Gent a l'intention de traiter les données personnelles du patient à des fins autres que celles indiquées dans la présente déclaration de confidentialité.

L'obligation légale sur la base de laquelle l'UZ Gent traite les données à caractère personnel aux fins susmentionnées est : la loi coordonnée du 10 juillet 2008 relative aux hôpitaux et autres établissements de soins (ci-après Loi hospitalière) et l'annexe A.III article 9quater de l'Arrêté Royal du 23 octobre 1964 déterminant les normes à respecter par les hôpitaux et leurs services.

Si l'UZ Gent traite les données personnelles susmentionnées aux fins susmentionnées, parce que cela est nécessaire pour l'exécution de l'accord que le patient a conclu avec l'UZ Gent, l'UZ Gent ne pourra pas prester ces services à ces fins sans traiter ces données personnelles.

6.2.2 Comment avons-nous obtenu ces données personnelles ?

Les données personnelles que l'UZ Gent traite dans le cadre des soins aux patients ont été reçues directement du patient, à moins que celui-ci n'ait pas été en mesure de les communiquer.

Les données personnelles concernant la santé sont collectées auprès du patient lui-même, sauf si un autre mode de collecte est requis en fonction des finalités du traitement, ou si le patient lui-même n'est pas en mesure de fournir ces données.

Les données médicales ont été obtenues par l'UZ Gent par le biais des prestataires de soins de santé (internes ou externes).

6.2.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données personnelles [ici](#).

6.3 Communication électronique en matière de soins avec le patient via le portail patient

Le portail patient tente de donner aux patients plus de contrôle sur leurs soins en leur fournissant des questionnaires électroniques et des informations sur les soins.

Catégorie de données à caractère personnel	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de destinataires
--	---------------------------	----------------	-------------------------	----------------------------

Données d'identification	Communication électronique en matière de soins	Consentement	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	Les membres du personnel interne ayant une relation de soins avec la personne concernée, le médecin traitant du patient, les prestataires de soins, le représentant légal. Si nous sommes obligés de le faire en vertu de la réglementation ou de la jurisprudence, également vis-à-vis des autorités ou de la mutuelle.
Coordonnées	Communication électronique en matière de soins	Consentement	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	
Données relatives à la santé	Communication électronique en matière de soins	Consentement	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	
Données sociales	Communication électronique en matière de soins	Consentement	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	
Données comptables	Communication électronique en matière de soins	Consentement	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	

6.3.1 Bases juridiques

Nous vous informerons au préalable si l'UZ Gent a l'intention de traiter vos données à caractère personnel à des fins autres que celles mentionnées dans la présente déclaration de confidentialité.

Pour certaines finalités, comme mentionné ci-dessus, le patient donne son consentement en acceptant explicitement un certain traitement (par ex. en utilisant le portail patient). Le patient a le droit de retirer son consentement à tout moment. Le retrait de ce consentement ne porte pas atteinte à la légitimité du traitement fondé sur le consentement avant son retrait.

6.3.2 Comment avons-nous obtenu ces données à caractère personnel ?

Les données à caractère personnel que l'UZ Gent traite dans le cadre de la communication électronique en matière de soins avec le patient ont été reçues directement du patient, à moins que celui-ci n'ait pas été en mesure de les communiquer.

6.3.3 Vos droits vis-à-vis de ce traitement de données à caractère personnel

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement de données à caractère personnelles [ici](#).

6.4 Enregistrement des patients

Par enregistrement des patients, nous entendons ce qui suit :

- Enregistrement des données relatives à la santé et au séjour à des fins stratégiques telles que : occupation des lits, gestion des stocks, planification du personnel ("enregistrement stratégique")
- Enregistrement des données relatives à la santé et au séjour à des fins mandatées par le gouvernement, par exemple dans le cadre du contrôle des épidémies ("enregistrement imposé")
- Enregistrement de données de santé à des fins scientifiques. La recherche scientifique constitue l'une des tâches essentielles d'un hôpital universitaire. L'objectif de la recherche scientifique est d'améliorer les connaissances sur les maladies et la santé et de fournir de nouvelles perspectives menant à des thérapies nouvelles ou plus performantes pour le patient ("enregistrement scientifique")

Catégorie de données à caractère personnel	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de destinataires
Données d'identification	Enregistrement stratégique	Nécessaire à l'exécution de l'accord conclu avec l'UZ Gent	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	Pas de destinataires externes
	Enregistrement imposé	Nécessaire pour remplir une obligation légale	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	Services de sécurité sociale, services publics
	Enregistrement scientifique	Nécessaire à la défense de l'intérêt général	25 ans après la fin de l'étude	Les médecins, les chercheurs, leur équipe, le commanditaire de l'étude reçoivent une forme pseudonymisée des données personnelles
Coordonnées	Enregistrement stratégique	Nécessaire à l'exécution de l'accord conclu avec l'UZ Gent	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	Pas de destinataires externes
	Enregistrement imposé	Nécessaire pour remplir une obligation légale	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	Services de sécurité sociale, services publics
	Enregistrement scientifique	Nécessaire à la défense de l'intérêt général	25 ans après la fin de l'étude	Les médecins, les chercheurs, leur équipe, le commanditaire de l'étude reçoivent une forme pseudonymisée des données personnelles
Données relatives à la santé	Enregistrement stratégique	Pour la prestation de soins de santé comme stipulé à l'article 9.2h) du RGPD	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	Pas de destinataires externes
	Enregistrement imposé	Nécessaire pour remplir une obligation légale	Minimum 30 ans et maximum 50 ans après le dernier contact avec le patient	Services de sécurité sociale, services publics
	Enregistrement scientifique	Nécessaire à l'accomplissement d'une mission d'intérêt public	25 ans après la fin de l'étude	Les médecins, les chercheurs, leur équipe, le commanditaire de l'étude reçoivent une forme pseudonymisée des données personnelles

Données génétiques	Enregistrement scientifique	Nécessaire à la réalisation d'une tâche d'intérêt public	25 ans après la fin de l'étude	Les médecins, les chercheurs, leur équipe, le commanditaire de l'étude reçoivent une forme pseudonymisée des données personnelles
Données biométriques	Enregistrement scientifique	Nécessaire à la réalisation d'une tâche d'intérêt public	25 ans après la fin de l'étude	Les médecins, les chercheurs, leur équipe, le commanditaire de l'étude reçoivent une forme pseudonymisée des données personnelles

6.4.1 Fondements juridiques

Nous vous informerons à l'avance si l'UZ Gent a l'intention de traiter les données personnelles du patient à des fins autres que celles indiquées dans la présente déclaration de confidentialité.

L'obligation légale sur la base de laquelle l'UZ Gent traite les données à caractère personnel aux fins susmentionnées est : la loi coordonnée du 10 juillet 2008 relative aux hôpitaux et autres établissements de soins (ci-après Loi hospitalière) et l'annexe A.III article 9quater de l'Arrêté Royal du 23 octobre 1964 déterminant les normes à respecter par les hôpitaux et leurs services. L'obligation légale peut également se fonder sur des enregistrements imposés par les pouvoirs publics, comme dans le cadre de la surveillance du Covid-19.

Si l'UZ Gent traite les données personnelles susmentionnées aux fins susmentionnées, parce que cela est nécessaire pour l'exécution de l'accord que le patient a conclu avec l'UZ Gent, l'UZ Gent ne pourra pas prester ces services à ces fins sans traiter ces données personnelles.

Lorsque l'UZ Gent traite les données personnelles susmentionnées aux fins susmentionnées pour des raisons d'intérêt public, l'intérêt public consiste à améliorer les connaissances sur les maladies et la santé et à offrir de nouvelles perspectives qui mènent à de nouvelles ou de meilleures thérapies pour le patient.

6.4.2 Comment avons-nous obtenu ces données personnelles ?

Les données personnelles concernant la santé sont collectées auprès du patient lui-même, sauf si un autre mode de collecte est requis en fonction des finalités du traitement, ou si le patient lui-même n'est pas en mesure de fournir ces données.

- *Pour l'enregistrement stratégique et imposé :*

Les données personnelles que l'UZ Gent traite dans le cadre des soins aux patients ont été reçues directement du patient, à moins que celui-ci n'ait pas été en mesure de les communiquer.

Les données de santé ont été obtenues par l'UZ Gent par le biais des prestataires de soins de santé internes ou externes.

- *Pour l'enregistrement scientifique :*

Les données d'identification que l'UZ Gent traite dans le cadre de l'enregistrement scientifique ont été reçues directement du patient, sauf si le patient n'était pas en mesure de communiquer ces données personnelles.

Les données de santé, génétiques et biométriques ont été reçues par l'UZ Gent par le biais du dossier du patient.

6.4.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données personnelles [ici](#).

Dans le cadre d'un enregistrement scientifique, vous pouvez ne pas avoir les droits ou avoir des droits plus restreints que ceux repris plus loin dans la présente déclaration de confidentialité, dans la mesure où ces droits risquent de rendre impossible ou d'entraver gravement la réalisation de certains objectifs et que certaines dérogations sont nécessaires pour atteindre les objectifs visés (un patient ne peut par exemple pas savoir si un médicament avec ou sans principe actif ("placebo") lui a été administré lors d'essais cliniques).

6.5 Sécurité physique

Catégorie de données à caractère personnel	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de destinataires
Images d'une caméra de surveillance	Afin de protéger les terrains, les bâtiments et les biens qui sont à la disposition de l'UZ Gent, en prévenant ou en constatant les destructions, les dommages et les vols ;	Intérêt légitime	30 jours	Les services de police et judiciaires en cas d'infractions pénales conformément à la législation en vigueur (article 9 de la loi sur les caméras de surveillance).
	de préserver la sécurité et la santé des membres du personnel en évitant la confrontation avec les auteurs de vols, de destructions, de violences et de harcèlement, en préservant l'ordre public et les bonnes moeurs et en prévenant les nuisances ;	Intérêt légitime	30 jours	
	L'identification des comportements punissables en vertu du droit belge et la mise à disposition d'informations à ce sujet aux services d'enquête et de police ou aux autorités judiciaires à des fins d'enquête.	Intérêt légitime	30 jours	

6.5.1 Fondements juridiques

Nous vous informerons à l'avance si l'UZ Gent a l'intention de traiter les données personnelles du patient à des fins autres que celles indiquées dans la présente déclaration de confidentialité.

Lorsque l'UZ Gent traite les données personnelles susmentionnées aux fins susmentionnées sur la base juridique de l'intérêt légitime, la protection des biens, la sécurité du personnel et le contrôle des processus de production (par exemple, Cyclotron) relèvent de l'intérêt légitime de l'UZ Gent. Le traitement des données personnelles par l'UZ Gent, tel que mentionné ci-dessus, en ce qui concerne les caméras de sécurité, ne constitue pas un traitement effectué par l'UZ Gent en tant qu'organisme public dans l'exercice de ses fonctions. Par conséquent, l'UZ Gent, en tant qu'organisme public, peut valablement invoquer l'intérêt légitime. Après avoir soigneusement pesé les différents intérêts, l'UZ Gent est d'avis que son intérêt l'emporte sur celui du patient aux fins susmentionnées. L'UZ Gent peut dans cette optique démontrer que :

1. les intérêts qu'elle défend avec ce traitement peuvent être considérés comme légitimes ("**test de finalité**") ;
2. le traitement prévu est nécessaire à la réalisation de ces intérêts ("**test de nécessité**") ; et

la pondération de ces intérêts par rapport aux intérêts, aux libertés fondamentales et aux droits des personnes concernées pèse en faveur du responsable du traitement ("**test de pondération**").

6.5.2 Comment avons-nous obtenu ces données personnelles ?

Les données personnelles que l'UZ Gent traite dans le cadre de la sécurité des caméras ont été obtenues directement auprès de la personne concernée.

6.5.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données personnelles [ici](#).

6.6 Enregistrement par caméra de surveillance médicale et enregistrement audio

Nous traitons ces données dans le cadre de la recherche scientifique, lors d'interventions chirurgicales thoraciques et vasculaires et lors du monitoring par électro-encéphalogramme (enregistrement de l'activité cérébrale), dans le cadre de la clinique du sommeil, dans l'unité des accidents vasculaires cérébraux, dans l'unité de soins intensifs (néonataux). Il peut également être nécessaire de filmer à des fins d'assurance qualité, par exemple pendant une opération ou pour surveiller certains troubles (par exemple les troubles du mouvement).

Catégorie de données à caractère personnel	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de récepteurs
Images de caméras de surveillance médicale	<ul style="list-style-type: none"> Recherche scientifique chirurgie thoracique et vasculaire Monitoring de l'électro-encéphalogramme Dans la clinique du sommeil Stroke unit Soins intensifs néonataux Suivi de certains troubles 	Consentement	Au moins 30 ans et jusqu'à 50 ans après le dernier contact avec le patient	Les données personnelles traitées par l'UZ Gent à cette fin ne sont pas transmises par celle-ci à des tiers.
	Soins intensifs	Nécessaire à des fins de médecine préventive ou de diagnostic médical		
	Enseignement médical	Intérêt général		
Enregistrements audio à caractère médical	<ul style="list-style-type: none"> Recherche scientifique chirurgie thoracique et vasculaire Monitoring de l'électro-encéphalogramme 	Consentement	Au moins 30 ans et jusqu'à 50 ans après le dernier contact avec le patient	

6.6.1 Fondements juridiques

Nous vous informerons à l'avance si l'UZ Gent a l'intention de traiter les données personnelles du patient à des fins autres que celles indiquées dans la présente déclaration de confidentialité.

À certaines fins, comme mentionné ci-dessus, le patient donne son consentement en acceptant explicitement un certain traitement (par exemple en cochant une case sur un formulaire d'information avant le début de l'examen). Le patient a le droit de retirer son consentement à tout moment. Le retrait de ce consentement n'affecte pas la légitimité du traitement fondé sur le consentement avant son retrait.

6.6.2 Comment avons-nous obtenu ces données personnelles ?

Les données à caractère personnel que l'UZ Gent traite à des fins de recherche scientifique ont été obtenues directement auprès de la personne concernée, sauf si celle-ci n'était pas en mesure de le faire.

Les données personnelles concernant la santé sont collectées auprès du patient lui-même, sauf si un autre mode de collecte est requis en fonction des finalités du traitement, ou si le patient lui-même n'est pas en mesure de fournir ces données.

6.6.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données personnelles [ici](#).

6.7 Maintenance et exploitation du site Web

Afin d'assurer la maintenance et l'exploitation du site Web et du portail patient de l'UZ Gent, celui-ci utilise divers cookies sur son site Web. Vous trouverez de plus amples informations à ce sujet dans notre [déclaration relative aux cookies](#).

Type de cookies	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de récepteurs
Cookies essentiels et fonctionnels	Bon fonctionnement et sécurité du site Web	Intérêt légitime	Voir la déclaration relative aux cookies	Pas de communication externe
Cookies préférentiels, statistiques et médias sociaux	Amélioration de l'expérience de navigation	Consentement	Voir la déclaration relative aux cookies	Voir la déclaration relative aux cookies

6.7.1 Fondements juridiques

Nous vous informerons à l'avance si l'UZ Gent a l'intention de traiter les données personnelles du patient à des fins autres que celles indiquées dans la présente déclaration de confidentialité.

Lorsque l'UZ Gent traite les données personnelles susmentionnées aux fins susmentionnées sur la base juridique de l'intérêt légitime, le bon fonctionnement et la sécurité du site Web relèvent de l'intérêt légitime de l'UZ Gent. Le traitement des données personnelles par l'UZ Gent, tel que mentionné ci-dessus, en ce qui concerne les caméras de sécurité, ne constitue pas un traitement effectué par l'UZ Gent en tant qu'organisme public dans l'exercice de ses fonctions. Après avoir soigneusement pesé les différents intérêts, l'UZ Gent est d'avis que son intérêt l'emporte sur celui du patient aux fins susmentionnées. L'UZ Gent peut dans cette optique démontrer que:

1. les intérêts qu'elle défend avec ce traitement peuvent être considérés comme légitimes ("**test de finalité**") ;
2. le traitement prévu est nécessaire à la réalisation de ces intérêts ("**test de nécessité**") ; et
3. la pondération de ces intérêts par rapport aux intérêts, aux libertés fondamentales et aux droits des personnes concernées pèse en faveur du responsable du traitement ("**test de pondération**").

Pour certaines finalités, comme mentionné ci-dessus, le patient donne son consentement en acceptant explicitement un certain traitement (par exemple en cochant la case de votre choix). Le patient a le droit de retirer son consentement à tout moment. Le retrait de ce consentement n'affecte pas la légitimité du traitement fondé sur le consentement avant son retrait.

6.7.2 Comment avons-nous obtenu ces données personnelles ?

Les données à caractère personnel que l'UZ Gent traite dans le cadre des cookies sont obtenues directement auprès de l'utilisateur du site Web, lorsque cet utilisateur visite le site Web et/ou lorsqu'il accepte ces cookies.

6.7.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données à caractère personnel [ici](#) .

6.8 Utilisation du réseau wifi de l'hôpital

Catégorie de données	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de destinataires
Numéro d'identification de l'appareil	Prévention de toute utilisation abusive du réseau	Intérêt légitime	1 an	Pas de communication externe, sauf en cas d'utilisation illégale du réseau, les données peuvent dans ce cas être transmises aux autorités judiciaires.
Le comportement de navigation via enregistrement	Prévention de toute utilisation abusive du réseau	Intérêt légitime	1 an	Pas de communication externe, sauf en cas d'utilisation illégale du réseau, les données peuvent dans ce cas être transmises aux autorités judiciaires.

6.8.1 Bases juridiques

Nous vous informerons préalablement si l'UZ Gent a l'intention de traiter les données personnelles du patient à des fins autres que celles indiquées dans la présente déclaration de confidentialité.

Lorsque l'UZ Gent traite les données personnelles susmentionnées aux fins susmentionnées sur la base juridique de l'intérêt légitime, la prévention de toute utilisation abusive du réseau relève de l'intérêt légitime de l'UZ Gent. Le traitement des données personnelles par l'UZ Gent, comme mentionné ci-dessus, en ce qui concerne le traitement des données personnelles par enregistrement ne constitue pas un traitement effectué par l'UZ Gent en tant qu'organisme public dans l'exercice de ses fonctions. Après avoir soigneusement pesé les différents intérêts, l'UZ Gent est d'avis que son intérêt l'emporte sur celui du patient aux fins susmentionnées. L'UZ Gent peut dans cette optique démontrer que :

1. les intérêts qu'elle défend avec ce traitement peuvent être considérés comme légitimes (« **test de finalité** »)
2. le traitement prévu est nécessaire à la réalisation de ces intérêts (« **test de nécessité** ») et

3. la pondération de ces intérêts par rapport aux intérêts, aux libertés fondamentales et aux droits des personnes concernées pèse en faveur du responsable du traitement (« **test de pondération** »)

6.8.2 Comment avons-nous obtenu ces données personnelles ?

Les données à caractère personnel que l'UZ Gent traite dans le cadre de l'enregistrement ont été obtenues directement auprès de l'utilisateur, lorsque cet utilisateur utilise le réseau wifi de l'hôpital.

6.8.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données à caractère personnel [ici](#).

6.9 Communication

Catégorie de données	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de destinataires
Identité de l'appelant	Sécurité du patient et/ou du collaborateur	Intérêt général	1 an	Pas de communication externe, sauf si cela est légalement exigé dans le cadre d'une procédure pénale

6.9.1 Bases juridiques

Nous vous informerons préalablement si l'UZ Gent a l'intention de traiter les données personnelles du patient à des fins autres que celles indiquées dans la présente déclaration de confidentialité.

6.9.2 Comment avons-nous obtenu ces données personnelles ?

Les données personnelles que l'UZ Gent traite dans le cadre de la sécurité du patient et/ou du collaborateur ont été obtenues directement auprès de la personne concernée.

6.9.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données à caractère personnel [ici](#).

6.10 Enregistrement des réclamations auprès du Bureau du Médiateur

Tout patient de l'hôpital a le droit de déposer plainte auprès du service de médiation de l'hôpital concernant les services de l'UZ Gent (par exemple, plaintes concernant les soins, le séjour et l'accueil).

Dans le cadre de cette finalité, nous traitons les données personnelles suivantes :

Catégorie de données à caractère personnel	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de récepteurs
Détails d'identification	Suivi et traitement de la plainte	Nécessaire à l'exécution d'une obligation légale	1 an après le traitement du dossier	Le prestataire de soins faisant l'objet de la plainte, le médecin-chef de l'hôpital, le service juridique de

				l'hôpital, les conseillers professionnels (par exemple, les avocats de l'UZ Gent), l'assureur, en cas de questions spécifiques concernant le traitement des données à caractère personnel : le délégué à la protection des données de l'UZ Gent.
Données relatives à la santé	Suivi et traitement de la plainte	Nécessaire à l'exécution d'une obligation légale	1 an après le traitement du dossier	
Coordonnées	Suivi et traitement de la plainte	Nécessaire à l'exécution d'une obligation légale	1 an après le traitement du dossier	
Données sur l'administration financière	Suivi et traitement de la plainte	Nécessaire à l'exécution d'une obligation légale	1 an après le traitement du dossier	
Données relatives à l'administrateur provisoire/à la famille	Suivi et traitement de la plainte	Nécessaire à l'exécution d'une obligation légale	1 an après le traitement du dossier	

6.10.1 Fondements juridiques

Nous vous informerons à l'avance si l'UZ Gent a l'intention de traiter les données personnelles du patient à des fins autres que celles indiquées dans la présente déclaration de confidentialité.

L'obligation légale sur la base de laquelle l'UZ Gent traite les données à caractère personnel aux fins susmentionnées est : la loi coordonnée du 10 juillet 2008 relative aux hôpitaux et autres établissements de soins (ci-après Loi hospitalière) et l'annexe A.III article 9quater de l'Arrêté Royal du 23 octobre 1964 déterminant les normes à respecter par les hôpitaux et leurs services.

6.10.2 Comment avons-nous obtenu ces données personnelles ?

Les données à caractère personnel que l'UZ Gent traite en vue de l'enregistrement des plaintes dans le cadre du service de médiation ont été obtenues directement auprès de la personne concernée, sauf si celle-ci n'était pas en mesure de le faire.

6.10.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données personnelles [ici](#).

6.11 Services sociaux

Le "service social" de l'hôpital signifie l'accompagnement des patients, et plus spécifiquement :

- La sortie de l'hôpital,
- L'aide à la demande de services de soins à domicile,
- L'admission dans un centre de soins résidentiels ou de rééducation ; et /ou
- Les questions financières et administratives.

Un soutien psychosocial peut également être fourni.

Catégorie de données à caractère personnel	Finalité(s) du traitement	Base juridique	Période de conservation	Catégorie de récepteurs
--	---------------------------	----------------	-------------------------	-------------------------

Détails d'identification	Services sociaux	Consentement	Tant que des services sociaux sont prestés	Les aidants et prestataires de soins externes, les aidants informels, les services publics et la mutuelle.
Coordonnées	Services sociaux	Consentement	Tant que des services sociaux sont prestés	
Données relatives à la santé	Services sociaux	Consentement	Tant que des services sociaux sont prestés	

6.11.1 Fondements juridiques

Nous vous informerons à l'avance si l'UZ Gent a l'intention de traiter les données personnelles du patient à des fins autres que celles indiquées dans la présente déclaration de confidentialité.

Pour certaines finalités, comme mentionné ci-dessus, le patient donne son consentement en acceptant explicitement un certain traitement. Le patient a le droit de retirer son consentement à tout moment. Le retrait de ce consentement n'affecte pas la légitimité du traitement fondé sur le consentement avant son retrait.

6.11.2 Comment avons-nous obtenu ces données personnelles ?

Les données à caractère personnel que l'UZ Gent traite à des fins de recherche scientifique ont été obtenues directement auprès de la personne concernée, sauf si celle-ci n'était pas en mesure de le faire.

Les données personnelles concernant la santé sont collectées auprès du patient lui-même, sauf si un autre mode de collecte est requis en fonction des finalités du traitement, ou si le patient lui-même n'est pas en mesure de fournir ces données.

6.11.3 Vos droits par rapport à ce traitement de données personnelles

Vous trouverez de plus amples informations sur les droits relatifs à ce traitement des données personnelles [ici](#).

6.12 Recherche scientifique

La recherche scientifique est l'une des tâches essentielles de l'UZ Gent.

Les finalités sont, d'une part, l'enregistrement des données relatives à la santé à des fins scientifiques dont l'UZ Gent est le client et, d'autre part, le traitement des données nécessaires dans le cadre des rapports de sécurité par l'UZ Gent.

Le règlement relatif à la protection de la vie privée "Recherche scientifique UZ Gent" peut être consulté [ici](#).

7 Transfert de vos données vers un pays situé en dehors de l'EEE (Espace Économique Européen)

En principe, l'UZ Gent ne transmet pas les données personnelles des patients à des pays situés en dehors de l'EEE. Si cela est malgré tout le cas, l'UZ Gent vérifiera si le pays de destination offre un niveau de protection adéquat. Si le pays vers lequel l'UZ Gent souhaite transférer des données n'offre pas de garanties suffisantes, l'UZ Gent doit, par le biais d'accords types (annexe 2) mis à disposition par la Commission européenne, ou par le biais d'autres mesures acceptées, imposer lui-même des garanties suffisantes.

8 Vos droits concernant le traitement de vos données personnelles

8.1 Droits vis-à-vis de l'UZ Gent

Par souci de clarté, nous précisons ci-dessous vos droits concernant vos données personnelles : Si vous souhaitez invoquer l'un de ces droits, veuillez envoyer un courrier électronique à l'adresse suivante dpo@uzgent.be.

8.1.1 Droit de regard et de copie

Vous avez le droit d'obtenir la confirmation que des données à caractère personnel vous concernant sont ou ne sont pas traitées et, le cas échéant, d'accéder à ces données à caractère personnel et de recevoir les informations suivantes :

- Les finalités du traitement ;
- Les catégories de données personnelles concernées ;
- Les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront divulguées, notamment les destinataires dans les pays tiers ou les organisations internationales ;
- Si possible, la période pendant laquelle les données à caractère personnel sont censées être conservées ou, dans le cas contraire, les critères permettant de déterminer cette période ;
- Que vous avez le droit de demander à l'UZ Gent de rectifier ou d'effacer les données personnelles, ou de limiter le traitement des données personnelles vous concernant, ainsi que le droit de vous opposer à un tel traitement ;
- Que vous avez le droit de déposer plainte auprès d'une Autorité chargée de la protection des données ;
- Lorsque les données personnelles ne sont pas collectées auprès de la personne concernée, toutes les informations disponibles sur la source de ces données ;
- L'existence d'une prise de décision automatisée, y compris le profilage visé à l'article 22, paragraphes 1 et 4, et, au moins dans ces cas, des informations utiles.

Vous avez également le droit de recevoir gratuitement une copie de ces informations de la part de l'UZ Gent en envoyant un e-mail à dpo@uzgent.be.

Dans le cadre de votre droit de regard et de copie, l'UZ Gent se réserve le droit de rendre illisibles ou de masquer (par exemple en les noircissant) certaines données personnelles ou informations contenues dans les documents demandés afin de sauvegarder les droits d'autrui.

8.1.2 Droit de rectification et d'achèvement

Si vous pensez que l'UZ Gent conserve des données incomplètes ou incorrectes vous concernant, vous avez le droit de demander à l'UZ Gent de les rectifier ou compléter gratuitement.

Dans le cas où les données sont incorrectes ou incomplètes, un ajout peut être accordé sur simple demande. En ce qui concerne les données relatives à la santé, une correction ne peut être autorisée qu'après approbation du médecin traitant ou du médecin-chef.

Si l'on demande la correction d'un avis ou d'une donnée médical(e) subjectif(ve), un ajout peut être accordé sur demande, mais pas une correction.

8.1.3 Droit à l'effacement

Dans certaines circonstances, vous pouvez demander à l'UZ Gent de supprimer vos données personnelles. C'est possible dans les cas suivants :

- Les données à caractère personnel ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées ou traitées ;
- Vous retirez votre consentement, sur lequel reposait le traitement, et il n'existe aucune autre base juridique pour le traitement ;
- Vous vous êtes opposé au traitement de vos données personnelles et il n'existe pas de motifs légitimes prépondérants pour conserver vos données ;
- L'UZ Gent traite vos données personnelles de manière illégale ;
- Les données personnelles doivent être supprimées afin de respecter certaines dispositions légales qui s'appliquent à l'UZ Gent.

L'UZ Gent peut être amené à refuser votre demande d'effacement pour diverses raisons. C'est le cas, par exemple :

- Afin de respecter une obligation légale de traitement qui incombe à l'UZ Gent en vertu du droit de l'Union ou du droit des États membres ;
- Pour l'accomplissement d'une mission d'intérêt général ou l'exercice d'un pouvoir public accordé à l'UZ Gent ;
- Pour des raisons d'intérêt public dans le domaine de la santé publique ;
- Si les données font partie d'archives conservées à des fins de recherche scientifique et que la suppression de vos données risque de rendre impossible toute recherche ultérieure ;
- Si les données sont nécessaires pour la constatation, l'exercice ou la justification d'une action en justice.

8.1.4 Droit à la limitation du traitement

Dans un nombre limité de cas, vous pouvez demander que vos données personnelles soient conservées mais non traitées ("*mise en attente*" du traitement) :

- L'exactitude des données à caractère personnel est contestée par vous-même, pendant une période permettant à l'UZ Gent de vérifier l'exactitude des données à caractère personnel ;
- Le traitement est illégal et vous vous opposez à l'effacement des données personnelles et demandez plutôt la restriction de leur utilisation ;
- L'UZ Gent n'a plus besoin des données à caractère personnel aux fins de traitement susmentionnées, mais vous en avez besoin pour l'introduction, l'exercice ou la justification d'un droit légal ;
- Vous vous êtes opposé au traitement des données à caractère personnel par l'UZ Gent, en attendant de savoir si les motifs avancés par l'UZ Gent l'emportent sur les vôtres.

8.1.5 Droit à la portabilité des données

Si l'UZ Gent traite des données sur la base de votre autorisation explicite, ou sur la base d'un accord conclu avec l'UZ Gent, vous avez également le droit, en tant que patient, de vous faire transférer une copie électronique de vos données personnelles ou de les faire transmettre directement à une autre institution ou personne de votre choix.

Ce transfert doit être effectué dans un format structuré, couramment utilisé et lisible par machine.

8.1.6 Droit d'opposition

Si le traitement de vos données n'est fondé que sur (i) le motif juridique selon lequel il est nécessaire pour l'UZ Gent d'exécuter une tâche d'intérêt général ou (ii) par les intérêts justifiés d'UZ Gent, vous pouvez introduire un recours motivé.

L'UZ Gent respectera l'objection motivée, à moins qu'il n'ait des motifs légitimes impérieux qui l'emportent sur vos intérêts, vos droits et vos libertés ou que les données soient liées à la constitution, l'exercice ou la justification d'un droit légal.

La personne concernée ne peut jamais s'opposer au traitement des données personnelles dont l'UZ Gent a besoin pour l'exécution d'un contrat ou en vertu d'obligations légales.

Lorsque des données personnelles sont traitées par l'UZ Gent à des fins de recherche scientifique, vous avez le droit, pour des raisons tenant à votre situation particulière, de vous opposer au traitement des données personnelles vous concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt général.

8.1.7 Droit de retrait de votre consentement à tout moment

Si le traitement des données personnelles est basé sur un consentement préalable, vous pouvez retirer ce consentement à tout moment.

Le retrait de ce consentement implique que l'UZ Gent n'est plus autorisé à traiter les données concernées. Le retrait de ce consentement n'affecte pas la légitimité du traitement fondé sur le consentement avant son retrait.

8.1.8 Droit d'opposition à l'assistance automatisée

L'UZ Gent n'a pas recours à la prise de décision automatisée.

8.2 Plainte à l'encontre de l'UZ Gent

Vous avez des réclamations ou des questions concernant le traitement de vos données personnelles par l'UZ Gent ?

Veuillez contacter notre délégué à la protection des données à l'adresse suivante : Délégué à la protection des données UZ Gent, C. Heymanslaan 10, 9000 Gent ou par e-mail dpo@uzgent.be.

8.3 Plainte auprès de l'Autorité chargée de la protection des données

Si vous pensez pouvoir déposer plainte concernant la protection de votre vie privée, vous pouvez aussi contacter directement l'Autorité belge de protection des données (www.autoriteprotectiondonnees.be) à 1000 Bruxelles, rue du Mail 35 ; ou +32(0)2 274 48 00; ou contact@apd-gba.be.

9 Entrée en vigueur et modifications de la déclaration de confidentialité

La présente déclaration de confidentialité entre en vigueur le 30 mai 2022.

L'UZ Gent se réserve le droit de modifier le présent règlement de confidentialité à tout moment. Les modifications seront effectuées par le Comité directeur de l'UZ Gent.

Vous trouverez la dernière date d'adaptation de la présente déclaration de confidentialité en haut, à droite.

Les modifications seront communiquées sur le site Web de l'UZ Gent. On y fera référence aux articles concernés par ces modifications.

10 ANNEXE

10.1 Annexe 1 : Notions reprises dans la présente déclaration de confidentialité

- **Données anonymes** : toutes les données qui ne peuvent pas (ou plus) être reliées à une personne identifiée ou identifiable et qui ne constituent donc pas (ou plus) des données personnelles.
- **Données biométriques** : données à caractère personnel résultant d'un traitement technique spécifique lié aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment l'identification sans équivoque de cette personne physique (telles que les images faciales ou les données relatives aux empreintes digitales).
- **Données génétiques** : données à caractère personnel relatives aux caractéristiques génétiques héritées ou acquises d'une personne physique qui fournissent des informations uniques sur la physiologie ou la santé de cette personne physique et qui découlent, notamment, d'une analyse d'un échantillon biologique de cette personne physique.
- **Données à caractère personnel pseudonymisées** : données à caractère personnel traitées de telle sorte qu'elles ne peuvent être liées à des personnes physiques spécifiques sans l'utilisation de données supplémentaires, à condition que ces données supplémentaires soient stockées séparément et que des mesures techniques et organisationnelles soient prises pour garantir que les données à caractère personnel ne soient pas liées à une personne physique identifiée ou identifiable. Il ne s'agit donc pas de données anonymes, puisque la personne physique est identifiable après pseudonymisation.
- **Collaborateur(s)** : salariés et/ou autres personnes nommées par l'UZ Gent et/ou professionnels indépendants travaillant au sein de l'UZ Gent.
- **Patient (ou "vous", "tu")** : la personne physique, admise ou traitée à l'hôpital et dont les données personnelles sont traitées (également appelée "**personne concernée**").
- **Données concernant la santé (ou "données relatives à la santé")** : données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris les données concernant les prestations de santé fournies qui donnent des informations sur l'état de santé de cette personne.
- **Données à caractère personnel** : toute forme d'information concernant une personne physique identifiée ou identifiable, par exemple un patient. Une personne identifiable est une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification (par exemple, le numéro de registre national), au nom et à la date de naissance, à des données de localisation, à un identifiant en ligne (par exemple, une adresse électronique ou une adresse IP) ou à un ou plusieurs facteurs spécifiques à son identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale.
- **Consentement**: toute manifestation de volonté librement consentie, spécifique, informée et non équivoque par laquelle le patient ou son représentant légal, par une déclaration ou une démarche active non équivoque, accepte que des données à caractère personnel le concernant soient traitées.
- **Sous-traitant** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement, sans être sous l'autorité directe de ce dernier.
- **Traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, comme la collecte, l'enregistrement, l'organisation, la structuration, la conservation, la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le

rapprochement ou la combinaison, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel.

- **Responsable du traitement** : une personne physique ou morale, une autorité publique, un service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens liés au traitement des données à caractère personnel.
- **Législation relative aux données personnelles** : désigne(i) le Règlement(Eu) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des Données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE à compter du 25 mai 2018,(ii) la loi belge du 30 juillet 2018 relative à la protection de la personne physique à l'égard du traitement des Données à caractère personnel (iii) toute autre législation applicable actuelle ou future se rapportant à la vie privée et au traitement des Données à caractère personnel ou ayant un impact sur ceux-ci.

10.2 Annexe 1 : Clauses contractuelles types pour les transferts de données personnelles vers un pays hors EEE

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.

(¹) 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. ...
