**DATA PROCESSING AGREEMENT**

This data processing agreement, including any annexes hereto, (together the "Data Processing Agreement") is an integrated part of the Agreement.

All defined terms within the Agreement shall have the same meaning when used in this Data Processing Agreement, unless explicitly defined otherwise in this Data Processing Agreement.

1. **Scope of the data processing Agreement**
	1. The Institution acts as a data processor as defined under article 4, 8) of the Regulation (EU) 2016/679 (“Data Processor”) for the Sponsor who acts as data controller as defined under article 4, 7) of the Regulation (EU) 2016/679 (“Data Controller”), as the Institution processes Personal Data for the Sponsor as set out in Annex 1.
	2. Further, the Parties acknowledge that Institution is the Data Controller in relation to the personal data processed for healthcare purposes.
	3. “Applicable Law” means any applicable data protection or privacy laws, including

(a) the European Data Protection Directive (95/46/EC) and upon its entry into force the Regulation (EU) 2016/679 also referred as the General Data Protection Regulation ("GDPR"),

(b) other applicable laws that are similar or equivalent to or that are intended to or implement the laws that are identified in (a) of this definition,

1. **Processing of Personal Data**
	1. Instructions: The Data Processor is instructed to process the Personal Data for the term of this Data Processing Agreement and only for the purposes of providing the data processing tasks set out in Annex 1. As part of the Study, Data Processor may not process or use Personal Data in another way than provided in the instructions, including with regard to transfers of personal data to a third country or an international organization, unless the Data Processor is required to do so according to Union or Member State law. In that case, the Data Processor shall inform the Data Controller in writing of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
	2. Data Processor shall at all times maintain a record of processing of Personal Data in accordance with Applicable Law and if the Data Processor considers an instruction from the Data Controller to be in violation of the Applicable Law, the Data Processor shall promptly inform the Data Controller in writing about this.
2. **The Data Processor's obligations**
	1. The Data Processor must ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
	2. The Data Processor shall implement appropriate technical and organizational measures to prevent that the Personal Data processed is:

accidentally or unlawfully destroyed, lost or altered,

disclosed or made available without authorization, or

otherwise processed in violation of Applicable Law.

* 1. The Data Processor must also comply with the special data security requirements of Annex 2.
	2. The appropriate technical and organizational security measures must be determined with due regard for:

the current state of the art,

the cost of their implementation, and

the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

* 1. The Data Processor shall upon request provide the Data Controller with sufficient information to enable the Data Controller to ensure that the Data Processor's obligations under this Data Processing Agreement are complied with, including ensuring that the appropriate technical and organizational security measures have been implemented.
	2. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller, by means of appropriate technical and organizational measures, insofar as this is possible, in fulfilling its obligation to respond to requests from data subjects pursuant to laws and regulations in the area of privacy and data protection (such as, the right of access, the right to rectification, the right to erasure, the right to restrict the processing, the right to data portability and the right to object).

* 1. The Data Controller is entitled to appoint at its own cost an independent expert, reasonably acceptable to Data Processor, who shall have access to the Data Processor's data processing facilities and receive the necessary information for the sole purpose of auditing whether the Data Processor has implemented and maintained said technical and organizational security measures. The expert shall upon the Data Processor's request sign a non-disclosure agreement provided by the Data Processor, and treat all information obtained or received from the Data Processor confidentially, and may only pass on, after conferral with Data Processor, the findings as described under article 3.9, (ii) below to the Data Controller.
	2. The Data Processor must give authorities who by Union or Member State law have a right to enter the Data Controller's or the Data Controller's processors’ facilities, or representatives of the authorities, access to the Data Processor's physical facilities against proper proof of identity and mandate, during normal business hours and upon reasonable prior written notice.
	3. The Data Processor must within 24 hours in writing notify the Data Controller about:

any request for disclosure of Personal Data processed under the Agreement by authorities, unless expressly prohibited under Union or Member State law,

any finding of (a) breach of security that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by the Data Processor under the Agreement, or (b) other failure to comply with the Data Processor's obligations under Clause 3, or

any request for access to the Personal Data (with the exception of medical records for which the Data Processor is considered data controller) received directly from the data subjects or from third parties.

* 1. Such a notification from the Data Processor to the Data Controller with regard to a breach of security as meant in Clause 3.9 (ii)(a) will contain at least the following information:

The nature of the Personal Data breach, stating the categories and (by approximation) the number of Data Subjects concerned, and stating the categories and (by approximation) the number of the personal data registers affected (datasets);

The likely consequences of the Personal Data breach;

A proposal for measures to be taken to address the Personal Data breach, including (where appropriate) measures to mitigate any possible adverse effects of such breach.

The Data Processor shall document (and shall keep such documentation available for the Data Controller) any Personal Data breaches, including the facts related to the Personal Data breach, its effects and the corrective measures taken. After consulting with the Data Controller, the Data Processor shall take any measures needed to limit the (possible) adverse effects of Personal Data breaches (unless such consultation cannot be awaited due to the nature of the Personal Data breach).

* 1. The Data Processor must promptly and reasonably assist the Data Controller (with the handling of (a) responses to any breach of security as described in 3.9 (ii) above and (b) any requests from Data Subjects under Chapter III of the GDPR (upon its entry into force), including requests for access, rectification, blocking or deletion. The Data Processor must also reasonably assist the Data Controller by implementing appropriate technical and organizational measures for the fulfilment of the Data Controller's obligation to respond to such requests. Any reasonable documented costs and expenses pre-approved in writing by the Data Controller related to the above will be reimbursed by the Data Controller to the extent such costs and expenses are not related to any requirements according to Applicable Law imposed on the Data Processor or due to any breach data protection rules or the Agreement by Data Processor.
	2. The Data Processor must reasonably assist the Data Controller with meeting the other obligations that may be incumbent on the Data Controller according to Union or Member State law where the assistance of the Data Processor is implied, and where the assistance of the Data Processor is necessary for the Data Controller to comply with its obligations. This includes, but is not limited to, at the request to provide the Data Controller with all necessary information about an incident under Clause 3.9 (ii), and all necessary information for an impact assessment in accordance with Article 35 and Article 36 of the GDPR. Any reasonable documented costs and expenses pre-approved in writing by the Data Controller related to the above will be reimbursed by the Data Controller to the extent such expenses are not related to any requirements according to Applicable Law imposed on the Data Processor or due to breach of data protection rules or the Agreement by Data Processor.
1. **DATA CONTROLLER’S OBLIGATIONS**

1. The Sponsor is responsible for supplying the Investigator and Study staff with sufficient information regarding the collection of their personal data on how this may be and will be handled by Sponsor as well as their rights before providing their personal data to the Sponsor. Upon Sponsor’s request, the Institution through the Investigator will assist the Sponsor in providing the necessary information.

2. The Data Controller shall take all necessary measures to ensure data protection in accordance with the General Data Protection Regulation (GDPR), including but not limited to providing adequate agreements with its subcontractors and obtaining data subject’s consent.

1. **SubProcessors**

The Data Processor may only engage a subprocessor, with prior specific or general written consent from the Data Controller. The Data Processor undertakes to inform the Data Controller of any intended changes concerning the addition or replacement of a subprocessor by providing a reasonable prior written notice to the Data Controller. The Data Controller may reasonably and in a duly substantiated manner object to the use of a subprocessor. The Data Processor must inform the Data Controller in writing of the discontinued use of a subprocessor.

Prior to the engagement of a subprocessor, the Data Processor shall conclude a written agreement with the subprocessor, in which at least the same data protection obligations as set out in this Data Processing Agreement shall be imposed on the subprocessor, including obligations to implement appropriate technical and organizational measures and to ensure that the transfer of Personal Data is done in such a manner that the processing will meet the requirements of the Applicable Law.

The Data Controller has the right to receive a copy of the relevant provisions of Data Processor's agreement with the subprocessor related to data protection obligations. The Data Processor shall remain fully liable to the Data Controller for the performance of the subprocessor obligations under this Data Processing Agreement. The fact that the Data Controller has given consent to the Data Processor's use of a subprocessor is without prejudice for the Data Processor's duty to comply with this Data Processing Agreement.

1. **Confidentiality**
2. The Data Processor shall keep Personal Data confidential.
3. The Data Processor shall not disclose the Personal Data to third parties or take copies of Personal Data unless strictly necessary for the performance of the Data Processor's obligations towards the Data Controller according to this Data Processing Agreement, and on condition that whoever Personal Data is disclosed to is under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies. Notwithstanding the foregoing, the Institution shall remain Data Controller for its own processing in relation to the personal data processed for healthcare purposes.
4. The Data Processor shall ensure that its employees comply with this Data Processing Agreement.
5. The Data Processor shall limit the access to Personal Data to employees for whom access to said data is necessary to fulfil the Data Processor's obligations towards the Data Controller.
6. The obligations of the Data Processor under Clause 5 shall continue until such time as provided by Applicable Law and regardless of whether the cooperation of the parties has been terminated.
7. **Term and termination of the Data Processing Agreement**
8. Regardless of the expiry or termination, for whatever reason, of the Agreement, this Data Processing Agreement remains in force and applicable as long as the Data Processor processes the Personal Data for the Data Controller under the Agreement.
9. In case of termination of the Agreement, the Data Processor must provide the necessary transition services to the Data Controller. The Data Processor is obliged to reasonably assist Data Controller at Data Controller’s expense.

Data Processor shall have appropriate procedures in place for the archiving of the Personal Data after the end of the Study in accordance with Data Controller Instruction, Applicable Law and at the end of the legally mandated archiving period ensure the destruction of the Personal Data and promptly inform Data Controller of this same, without prejudice to its own legal retention obligation.

**Annexes:**

Annex 1: Instructions

Annex 2: Security measures**Annex 1 – Instructions**

This Annex 1 constitutes the Data Controller's instruction to the Data Processor in connection with the Data Processor's Personal Data processing for the Data Controller, and is an integrated part of the Data Processing Agreement.

Contact details of the Data Controller (including its Data Protection Officer, if applicable):\_\_\_\_\_\_\_\_\_\_\_

Contact details of the Data Processor (including its Data Protection Officer, if applicable): rgpd-saintluc@uclouvain.be

a) **Purpose and nature of the processing operations**

Performance of Clinical Study services under the Agreement and for the purpose of mandatory safety monitoring– as specifically described in the Protocol.

I. Transfer of Personal Data to a third country: YES/NO

II. If YES to I., transfer outside the EU: YES/NO

b) **Categories of Data Subjects**

I. Former, current or future persons and/or patients who voluntarily enrolled in the Study, and/or their relatives, and/or

II. Investigator and staff members

III. […]

c) **Categories of Personal Data**

Re b) I: *To specify : for example:*  *age, personal identification number assigned to Data Subjects participating in the Study, description of characteristics of physical features of the body*

Re b) II: Contact information, CV, details on the involvement in the Study

Re b) III: […].

d) **Special categories of Personal Data**

Re b) I: *Health information including past medical history and medical test information (such as blood samples results from scans and biopsies), data revealing racial or ethnic origin, genetic data*

e) Insert address, city and country of all locations where the processing will be performed : Cliniques Universitaires Saint-Luc, Avenue Hippocrate 10, 1200 Brussels

f) **Specific security requirements**

The following requirements reflect the minimum data processing requirements expected of the Data Processor. It is a condition that other agreed documents, legislation or industry standards laying down requirements of the processing of Personal Data in connection with Study/ /mandatory safety monitoring are complied with as well.

1. The collection, registration and other processing of Personal Data must be legally authorized under Applicable Law, or applicable policies issued of the supervisory authorities.

2. Any person who takes part in the processing of Personal Data must be familiar with these requirements.

3. Premises used for the storage and other processing of Personal Data must be arranged in such a way as to prevent unauthorized access.

4. Appropriate security measures must be implemented to protect data against accidental or unlawful destruction, loss or impairment. Furthermore, it must be ensured that no incorrect or misleading Personal Data is processed. Incorrect or misleading data, or data processed in contravention of the above Applicable Law, policy of the supervisory authority or these requirements, shall be rectified or erased. Data Processor will provide a security annex describing the security level of its IT infrastructure and access management.

6. Personal Data may not be stored in a way that makes it possible to identify the Data Subjects for longer than is necessary for the achievement of the Study and/or mandatory safety monitoring.

7. The publication of results from clinical studies must take place in such a way that it is impossible to identify individual persons.

8. It is a condition that other legislation laying down requirements of the processing of Personal Data in connection with Study and/or mandatory safety monitoring is complied with.

**Electronic data**

9. Identification data must be encrypted or replaced by a code number or similar. Alternatively, all data stored can be encrypted. Encryption keys, code keys, etc. must be stored securely and separately from the Personal Data. This also applies to Personal Data that is stored on portable devices such as laptop PCs, tablets, etc.

10. Data may only be accessed by using a unique user name and a confidential password. The password must be renewed at least once a year and when otherwise necessary in order to ensure the secure processing of the data.

11. On the transfer of Personal Data via the internet or other external networks, the necessary security measures must be taken to ensure that the Personal Data does not come to the knowledge of any unauthorized persons. This includes that encryption is required if sensitive Personal Data is transferred via the internet (or other open networks), and security of authenticity (identities of transmitter and recipient) and integrity (the authenticity of the transmitted Personal Data) must be appropriately ensured by the use of suitable security measures. On using internal networks, it must be ensured that no unauthorized persons can gain access to the data.

12. Removable storage media, safety copies of Personal Data, etc. must be stored securely and under lock and key, so that unauthorized access is prevented.

**Manual ("paper") data**

13. Manual material, including print-outs, error and control lists, etc. with Personal Data, must be stored securely under lock and key, and in such a way as to prevent unauthorized access.

**Biobank and biological material**

14. Samples with biological material and biological material in biobanks must be stored securely under lock and key so as to prevent unauthorized access, and in such a way as to ensure that the material is not lost, impaired, or accidentally or illegally destroyed.

15. Biological material collected for the purpose of the Study and marked with a civil registration number or name must be stored subject to special safety requirements.

16. Internal guidelines must be laid down within the Data Processor’s organization regarding the project for the storage of biological material.

**Information to be given to the clinical Study participant/Data Subject**

17. Where the Personal Data is obtained from the clinical Study participant/Data Subject (via interviews, questionnaires, clinical or para-clinical examination, treatment, observation, etc.), more detailed information concerning the clinical Study/testing/safety monitoring shall be distributed/forwarded to the Data Subject in accordance with Article 13 of the GDPR. The clinical Study participant must, via the informed consent form as drafted by the Data Controller and as approved by the relevant ethics committee and /or relevant authorities, be informed of the name of the Data Controller, the purpose of the trial/testing/safety monitoring, the fact that it is voluntary to participate in the trial/testing, the identity of any recipients of Personal Data, and the purpose of the disclosure of Personal Data, as well as any further information which is necessary for the clinical Study participant / Data Subject to be able to safeguard his/her interests. The Data Subject has been informed about the right of access to the Personal data that is processed concerning the person in question.

When collecting data from Study participant/Data Subject through their own devices, the Data Controller cannot handle identifying metadata such as cookie, phone number, IP address or e-mail address. If the Data Controller resorts to subcontractors (i.e.: web host, cloud solution, online survey provider, intermediary organism in charge of de-identify data…), the Data Controller have to, according to data protection rules, assure that those respect Data Protection rules through a Data Processor Agreement or a Joint Controller Agreement.

**Disclosure**

18. Disclosure/issue of Personal Data to other parties may take place to the extent that this is legally authorized under Applicable Law.

**On the conclusion of the project**

19. At the latest on the conclusion of the trial/testing/safety monitoring the Personal Data (including biological material) shall be erased, made anonymous, or destroyed, unless Union or Member State law requires continued storage of the Personal Data. In accordance with Belgian Law as defined in the Agreement the Data Processor is required to store the medical records for 30 years. It must not subsequently be possible to identify individuals participating in the clinical Study/testing/safety monitoring. The deletion of Personal Data must be properly documented.

20. Alternatively, the Personal Data may be transferred for further storage in archives according to the Data Controller’s instructions. Any costs related to such transfer and further storage of Personal Data shall be borne by the Data Controller.

21. Erasure of Personal Data from electronic media shall take place in such a manner that it is impossible to recover the Personal Data and such erasure must be properly documented.

**Annex 2: Security Measures**

*Preamble:*

*To comply with its obligations about security of information and data confidentiality, the Cliniques universitaires Saint-Luc have implemented an information security framework and data security management. The information security management system is based on certification ISO 27001. No external audit has been done. The process is internal.*

*Our Information and System Department (DIS) apply strong binding rules to ensure confidentiality, integrity, availability and auditability of information.*

*Those binding rules are applied to all personal data that we collect, store or process as data controller or as data processor for a partner or contractor of the Cliniques universitaires Saint-Luc.*

**Central ICT infrastructure in two internal data centers**

All important component of the central ICT infrastructure are installed in two data centres. This professional organisation of data centre aims to guaranty an optimum physical security, consistent power supply, fire protection (only DC4) and natural disaster.

An ultra fast direct connection between the two data centres gives additional opportunities for continuous disponibility and disaster recovery.

**Network and advanced infrastructure**

Server’s infrastructure, storage and network have been developed in a way that guarantees a maximal availability and to prevent data loss or data destruction. This infrastructure is regularly revisited.

* Redundant connexions and high quality switching guaranty fast communication between sites and to data centres.
* The majority of the servers has been virtualized to permit fast recovery in a disturbed environment.
* Critical servers have been doubled and, when necessary, set in cluster.
* Data is stored locally as well as on the other site trough regular snapshots, in accordance with back-up policy.

Following technologies have been set to prevent external threats and protect the environment of those threats:

* Firewall
* Malware analysis
* Web filtering
* Subdivision of the network into virtual local networks (VLAN),
* Remote access only trough VPN SSL
* Data exchange trough SFTP, trough health network or Lan-2-Lan

Permissions to access data, apps and devices are subject of strict rules, on basis of a permission matrices controlled by the directorate. The access is related to the user function and is limited to the data needed to perform the tasks. Accounts with special rights are scrupulously controlled and followed.

Any modification of the permission, critical data movement and data system manger activities are recorded in a logbook and supervised.

**Physical security**

Both data centres and production sites are electronically secured. The entrances are secured with electronic badge system. The premises of the Hospital are split in different areas depending on the security risks. Accesses to sensitive areas are subject to additional rules.

**Staff behaviour**

Staff members are tested on hiring on both technical skills and attitude (sense of respect of procedure, sense of responsibility, data confidentiality worries). At hiring, each member staff signs a confidentiality clause. Those responsibilities are clearly indicated in the employment contract and work regulations. There are clear work instructions about data confidentiality and protection and correct use of ICT devices, Internet and mobile data communication. Sensitization campaigns are planned.

If some missions are trusted to external partners, confidentiality clauses are always concluded and the partner’s staff members must respect all security instructions applicable in the Cliniques.

**ICT work**

Introduction of a new infrastructure or new software systems and development of new user apps or new apps and platform are subject an intern certification principle (including defined level of data protection) and works procedure (separation of production environment from non-production environment; formal approval of modifications trough change request procedure).

**Compliance**

The board of directors and the directorate of the Cliniques follow those policies and their respect. The various responsibilities are clearly described and concretely. The Cliniques have elected a data protection officer. The information security and data confidentiality policy has been formalized instructions and workflows.

Those are rewritten in the institutional quality assurance system. Respect of those policies is subject to internal and external audits.

**Back-up and destruction of personal data.**

1. Back-up and mirroring of virtualized central server.

The Cliniques universitaires Saint-Luc have adopted storage and saving policy depending on the sensitivity of information.

The virtualized servers of central platform are saved. The frequency depends of the server’s criticality (every 15 minutes, every hour, every 4 hours or every 24 hours).

Both the servers and the data disk are saved following this method. The snapshots are compressed and saved on storage device, but on another autonomous part, in a way that the original and the save cannot be impacted in case of defective disk or controller. Those snapshots are moreover exchanged between the two data centres.

We dispose in this way, with a light delay, the needed data on another site to restore a server, on the same site, on other hardware or on another site, in case of unavailability.

Only some versions of those snapshots and files are stored, the purpose being recovery of the most recent data. Thus, those disappear automatically as they are replaced by more recent versions.

The recovery method of servers with snapshots or files is described in the DRP instructions.

2. Permanent back-up

The backup software is used to keep long term data backup which allow to recover older data. A weekly version is kept 40 days, a monthly version 13 month. In this case, the purpose the get back further in time, when some data is erased or altered or if a server is corrupted must be restored on basis of an older version, that doesn’t appear in the snapshots.

Smaller or larger set of these backups can be restored with ease if users wish to recover older versions of files, records or mail inbox. User can introduce a request for this purpose to the helpdesk.

3. Security backup of personal data related to the legal patient record.

Those data are placed, with help of automatic services, on a dedicated device, where they are stored in encrypted form and only accessible by means of special access rights. This HIPAA accredited device prohibits all data modifications and use very strict procedure of encryption/decryption and erasing of data.

Data retention period is by default of 30 years. After expiry of the retention period, the data can be deleted, this in a definitive way.