ADDENDUM TO SUPPLIER AGREEMENT CONCERNING DATA PROTECTION

Between the undersigned

UZ Brussel, with business unit number 2.143.464.230 and located with registered office at Belgium, 1090 Brussels, Laarbeeklaan 101 with VAT number 0449.012.406, as part of Vrije Universiteit Brussel – VUB, established in accordance with the Belgian Law of 28 May 1970 as published in the Belgian Official Gazette of June 25, 1970 with registered head office in Belgium, 1050 Brussels, Pleinlaan 2, with regard to this agreement duly represented by prof. dr. Mark De Ridder, CEO,

Hereinafter referred to as "**the Hospital**"

AND

…… [*supplier data to be completed*]

Hereinafter referred to as "**Supplier**"

Hereinafter jointly referred to as the "**Parties**"

Considering that

The Supplier provides services for the Hospital, as described in the Basic Agreement, these services entail the processing of personal data and the parties, through this Addendum, wish to establish the arrangements for the processing of personal data in the context of the services.

The Supplier is an expert in the products and/or services that are the subject of the Basic Agreement, the Supplier has the necessary resources to fulfill the products and/or services according to the rules of the trade, and this can be demonstrated through relevant and reliable references.

the following has been agreed:

If the Parties wish, by mutual agreement, to make adjustments to the text of this Addendum, such adjustments – in so far as they comply with the Data Protection Legislation and fall within the scope of the contractual freedom of the Parties – shall be recorded, stating the reason, in Annex 1 to this Addendum.

Changes to Annex 1 shall be valid only if they have been signed and dated by both parties.

1. DEFINITIONS

1.1 For the application of this Addendum, the following definitions shall apply:

- **General Data Protection Regulation (GDPR)**: 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, and repealing Directive 95/46/EC, with its amendments and European implementing legislation;

- **Data Protection Legislation**: the General Data Protection Regulation, other European legislation containing provisions concerning data protection and privacy, as well as the applicable national legislation on data protection and privacy in the Member States, with its amendments and implementing decrees, including the approved codes of conduct applicable to the sector.

- **Personal data, Processing, Controller, Processor, Data Subject, Consent**: the definitions as set out in the General Data Protection Regulation;

- **Basic Agreement**: the agreement between the Hospital and the Supplier of …… [date] concerning …… …… [complete title of agreement, any reference number].

1.2 The Supplier shall provide services to the Hospital on the basis of, and as defined in, the Basic Agreement.

For the processing activities as specified in **Annex 2** to this Addendum, the following qualification shall apply:

- the Hospital shall determine the purpose and at least the essential means of processing and shall consequently be the controller;
- the Supplier shall carry out the processing of personal data on behalf of and according to the instructions of the Hospital as controller, and shall consequently be the processor.

2. SCOPE AND RELATIONSHIP TO THE BASIC AGREEMENT

2.1 This Addendum shall form an integral part of the Basic Agreement concluded between the Hospital and the Supplier. The provisions of this Addendum shall apply in full to all processing of personal data performed by the Supplier in the context of the implementation of the processing activities specified in Annex 2.

2.2 The provisions of this Addendum (and Annexes) shall take priority over the (possibly contrary) provisions concerning data protection and processing and confidentiality of data in the Basic Agreement, and shall replace these provisions.

3. PROCESSING IN ACCORDANCE WITH THE REGULATIONS AND THE WRITTEN INSTRUCTIONS OF THE HOSPITAL

3.1 When processing personal data, the Parties shall act in accordance with the Data Protection Legislation.

3.2 The Supplier shall process the personal data exclusively on the basis of the written instructions of the Hospital, unilaterally determined by the Hospital and as set out in **Annex 2** to this Addendum. If the written instructions are not clear, the Supplier shall notify the Hospital of this in writing, whereupon the instructions shall be clarified by common accord.

3.3 Unless otherwise stipulated in this Addendum, the Supplier shall not process the personal data for its own purposes or for those of third parties, or provide the personal data to third parties without having received a written instruction to do so from the Hospital. Processing in accordance with the instructions of the Hospital may also mean that the processing must be stopped (immediately).

3.4 If European or national legislation requires the Supplier to undertake specific processing, the Supplier shall inform the Hospital in writing, prior to the processing, of that legal requirement, unless this legislation prohibits such notification for important grounds of general interest.

3.5 The Hospital shall give instructions to the Supplier in accordance with the Data Protection Legislation and shall ensure that all personal data entrusted to the Supplier have been obtained lawfully and can be processed under the Basic Agreement.

4. APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES

4.1 The Parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in accordance with Article 32 of the GDPR.

4.2 When determining the measures, the state of the art, the costs of 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 persons, shall be taken into account.

4.3 The measures shall include, inter alia, as appropriate:

- Pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

4.4 In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

4.5 The Supplier shall adhere to the standards of approved codes of conduct and certification mechanisms as applicable within the sector. It shall supply evidence thereof in an Annex to this Addendum.

4.6 The Supplier shall describe in **Annex 3** the appropriate technical and organisational measures it has implemented. It shall report to the Hospital, on its own initiative, changes made to the measures, as set out in Annex 3, within a period of fourteen days of making the changes.

5. PROCESSING BY A "SUB-PROCESSOR" OR EMPLOYEE

5.1 The Supplier shall ensure that its representatives, agents, subcontractors and employees comply with the provisions of this Addendum. The Supplier will only share or make available personal data of the Hospital to the representatives, agents, subcontractors, and employees who are directly involved in the execution of the Basic Agreement based on the 'need-to-know' principle.

The Supplier shall ensure, in line with this:

- that persons authorised to process personal data have undertaken to maintain confidentiality or are bound by an appropriate statutory obligation of confidentiality;
- that measures have been implemented to ensure that any natural person acting under its authority who has access to the personal data, shall not process these data except on instructions from the Hospital, unless required to process them by European or national legislation.

.

5.2 The Supplier is only allowed to engage a third party as a sub-processor if he has informed the Hospital in a timely manner and, in any case, in advance about the identity of the sub-processor, and provided that the Hospital does not raise objections against it. If the Hospital raises any reasonable objections within 14 days after receiving the Supplier's notification regarding the proposed new sub-processor, the Supplier will not disclose any personal data of the Hospital to the proposed sub-processor, except with the prior written and explicit consent of the Hospital.

5.3 The Supplier shall provide the Hospital with the complete details of the processing taken over by the sub-processor(s) in **Annex 2** to this Addendum.

If during the term of the agreement, the Supplier engages other sub-processors than those initially mentioned in Annex 2 or if there are changes regarding the information in Annex 2, the Supplier will promptly inform the Hospital about this. If the Hospital raises any reasonable objections within 14 days after receiving the Supplier's notification regarding the proposed new sub-processor, the Supplier will not disclose any personal data of the Hospital to the proposed sub- processor, except with the prior written and explicit consent of the Hospital. In such cases, Annex 2 will be amended.

If the Supplier has recourse to a sub-processor, the Supplier shall impose on this sub-processor by agreement the same obligations concerning data protection as those

applying between Processor and Controller. The Supplier shall provide the Hospital with the agreement with the sub-processor on first request.

5.4 If the sub-processor fails to comply with its data protection obligations, the Supplier shall remain fully liable in relation to the Hospital for complying with the sub-processor's obligations.

6. TRANSFER OF DATA TO A COUNTRY OUTSIDE THE EUROPEAN ECONOMIC AREA

6.1 If personal data is transferred to a country or organization outside the European Economic Area, the Supplier shall comply with the safeguards of Chapter 5 of the GDPR and provide appropriate safeguards. The Supplier shall inform the Hospital about the following for each transfer outside the European Economic Area:
- the country of the transfer
- the transfer instrument
- the analysis and assessment regarding the additional measures that need to be taken to facilitate the transfer (Transfer Impact Assessment (TIA))

6.2 When the Supplier will process personal data or will have the personal data processed outside the European Economic Area, the Hospital may request the aforementioned analysis and assessment of the law and/or applicable practices of the third country, as well as the additional measures, from the Supplier. The Supplier shall provide this assessment (Transfer Impact Assessment) upon the first request from the hospital.

6.3 If the specific transfer instrument referred to in Articles 45 to 49 of the GDPR is not effective and no additional measures are taken to ensure the level of data protection as established in the GDPR, the Supplier is not allowed to transfer the personal data outside the European Economic Area, unless the Hospital has provided its prior written consent.

6.4 This article also applies to any transfers carried out by the sub-processors engaged by the Supplier for the processing of personal data on behalf of the Hospital.

7. PROVISION OF ASSISTANCE WITH RESPECT TO THE OBLIGATIONS REGARDING THE DATA PROTECTION POLICY OF THE HOSPITAL

7.1 Taking into account the nature of the processing and the information available to it, the Supplier shall undertake to provide assistance to the Hospital with respect to the responsibility of the Hospital to comply with the following data protection obligations:

- Implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk;
- Notification of a personal data breach to the supervisory authority;
- Communication of a personal data breach to the data subject;
- Carrying out a data protection impact assessment;
- Consultation of the supervisory authority prior to processing where the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Hospital to mitigate the risk.

7.2 The time and resources spent by the Supplier in providing the assistance shall be at the Supplier's own expense.

7.3 Pursuant to Article 7.1, the Supplier shall inform the Hospital in detail and immediately of a (suspected) personal data breach as well as of any data leak (at the sub-processor too) as soon as the Supplier has become aware of this. The notification shall take place in such a way that the Hospital can satisfy in time its legal obligations as controller under the Data Protection Legislation. The Supplier shall indemnify the Hospital in accordance with Article 10.2.

The Supplier shall use the report form in **Annex 4** for the reporting.

7.4 The Supplier shall also provide assistance in the investigation and the mitigation and remediation of a personal data breach. In this respect, it shall provide assistance, inter alia, with a view to the documentation of measures such as data protection by design and data protection by default.

7.5 The Supplier shall notify the Hospital immediately of any complaint, accusation or request made (including if it comes from a regulator) with regard to the processing of personal data by the Supplier. The Supplier shall offer all necessary cooperation and support that the Hospital can reasonably expect with regard to such a complaint, accusation or request, including by providing full information on such a complaint, accusation or request, together with a copy of the personal data concerning the data subject in the possession of the Supplier.

8. PROVISION OF ASSISTANCE FOR REQUESTS BY THE DATA SUBJECTS

8.1 Taking into account the nature of the processing, the Supplier shall provide the Hospital with assistance by appropriate technical and organisational measures in fulfilling the Hospital's obligation to respond to requests to exercise the rights of the data subject, as specified in the Data Protection Legislation.

This implies, inter alia:

- that the Supplier provides all the personal data requested by the Hospital within the (reasonable) period of time requested by the Hospital, in any case including the full details and copies of the complaint, communication or request and any personal data in its possession concerning the data subject;
- that the Supplier implements technical and organisational measures that permit the Hospital to reply effectively and in a timely manner to relevant complaints, communications or requests.

8.2 The time and resources spent by the Supplier in providing the assistance shall be at the Supplier's own expense.

8.3 Pursuant to Article 8.1, the Supplier shall undertake to inform the Hospital without delay if it receives one of the following requests from a data subject (or third party acting on behalf of a data subject):

- a request for access to the data subject's personal data processed;
- a request for rectification of incorrect personal data;
- a request for erasure of personal data;

- a request for restriction of the processing of personal data;
- a request to obtain a portable copy of the personal data, or for transmission of a copy to a third party;
- an objection to any processing of personal data; or
- any other request, complaint or communication concerning the obligations of the Hospital under the Data Protection Legislation.

8.4 The Supplier shall not reply to the requests and applications by the data subject itself, unless there are any written agreements to the contrary between the Hospital and the Supplier.

9. RIGHT OF CONTROL BY THE HOSPITAL

9.1 The Hospital shall have the right at any time to check compliance by the Supplier with the Addendum.

9.2 The Supplier shall make all information available to the Hospital which is needed to demonstrate compliance with the obligations under the Data Protection Legislation.

9.3 The Supplier shall make audits possible, including inspections, by the Hospital or an auditor authorised by the Hospital, and shall contribute to them. These audits can be announced or conducted without prior notice in case of suspected irregularitiesThe Supplier shall grant full cooperation with regard to such an audit and, at the request of the Hospital, shall supply evidence of compliance with its obligations under this Addendum.

9.4 The Supplier shall inform the Hospital immediately if, in its opinion, an instruction under Article 9.1 breaches the Data Protection Legislation.

10. LIABILITY

10.1 The Parties shall each be responsible and liable for their own actions. The liability regulated in this Article shall relate exclusively to the liability arising from a breach of the Data Protection Legislation and this Addendum.

10.2 The Supplier shall reimburse and indemnify the Hospital for all claims, actions, demands by third parties and for all damage and losses (also including fines imposed by the data protection authority) arising directly or indirectly from processing of personal data if, during the processing, it has not complied with the obligations of the Data Protection Legislation addressed specifically to processors or if it has acted outside or contrary to the lawful instructions of the Hospital.

10.3 The Parties shall ensure sufficient cover of their liability.

11. END OF THE AGREEMENT

11.1 If the Supplier fails to comply correctly with the obligations arising from this Addendum or fails to implement appropriate measures within a maximum period of two months,

the Hospital – without prejudice to other forms of termination as provided for in the Basic Agreement – may terminate the Basic Agreement immediately after the aforementioned period of two months and/or stop the processing assignment.

11.2 This agreement shall form an integral part of the Basic Agreement and shall therefore follow the fate of the Basic Agreement. However, if the Basic Agreement comes to an end, the provisions of this Addendum shall apply as far as necessary for winding up the obligations in accordance with the Data Protection Legislation.

11.3 Immediately on (no matter which) termination or expiry of the Basic Agreement or after the expiry of the storage period, the Supplier – at the discretion of the Hospital – shall return the personal data to the Hospital and/or irrevocably erase the personal data entirely and remove existing copies. If the Hospital opts for the removal of the personal data, the Supplier shall demonstrate to the Hospital, on written request, that the removal has in fact occurred.

11.4 The Supplier may derogate from paragraph 1 if the storage of the personal data is required under European or national legislation.

12. FINAL PROVISIONS

12.1 In the event of nullity or voidability of one or more provisions of this Addendum, the other provisions shall remain in full force.

12.2 This Addendum shall be subject to Belgian law. Disputes shall be brought before the courts/tribunals of Brussels (Belgium), which shall have exclusive territorial jurisdiction.

Thus agreed and drawn up in duplicate.

The Hospital :	**The Supplier :**
Prof. Dr. Steven Droogmans Medical Director ICT **UZ Brussel**	[NAME] [FUNCTION]

Annexes

Annex 1: Adjustments to the addendum under contractual freedom of the parties
Annex 2: The processing assignment and instructions, as specified by the hospital
Annex 3: Information security
Annex 4: Model form for reporting of data leaks
Annex 5: European Standard Contractual Clauses (ESCCs) - Optional

ANNEX 1 – ADJUSTMENTS TO THE ADDENDUM UNDER CONTRACTUAL FREEDOM OF THE PARTIES

The Addendum contains a standard text which implements the obligations arising from the Data Protection Legislation. Certain aspects fall (within certain limits) under the contractual freedom of the parties.

If the Parties wish to regulate certain aspects differently or more specifically or wish to add certain matters, these are determined explicitly in this Annex.

Contractual freedom can cover, for example:

- the periods within which the Supplier must inform the Hospital or must provide assistance (but in each case within the period within which the Hospital must itself report to the supervisory authority or the department concerned);
- specification of whether specific or general consent is applied for the sub-processor(s);
- …

Changes in this Annex are valid and enforceable only if this Annex has been signed and dated by both parties.

Article	Text which lapses or may lapse	Replacement or additional text	Reason

Thus agreed and drawn up in duplicate at …….. on ……. .

The Hospital :	**The Supplier :**
Prof. Dr. Steven Droogmans Medical Director ICT **UZ Brussel**	[NAME] [FUNCTION]

ANNEX 2 - THE PROCESSING ASSIGNMENT AND INSTRUCTIONS AS SPECIFIED BY THE HOSPITAL

Accompanying note

This Annex describes the specific processing by the Supplier, for which the Hospital gives instructions at the time of the conclusion of the Basic Agreement or on signing the Addendum.

Changes and/or supplements to this Annex 2 occur in each case via a separate document which is added as an Appendix to this Annex 2 (Appendix 1 to Annex 2; Appendix 2 to Annex 2, etc.), which is dated and which shows the explicit and written instruction and/or agreement of the Hospital.

I. The purpose of the processing of personal data

The processing of Personal Data by the Supplier takes place under the implementation of the Basic Agreement concerning…… *[to be completed by supplier]*.

Description of the services under the Basic Agreement and nature and purpose of the processing of personal data in the context of the services:

……
……
……

II. The categories of personal data which the Hospital instructs the Supplier to process (indicate what is applicable and if necessary supplement):

- contact details
- financial data
- invoice data
- wage data
- medical data
- marketing data
- data on the use by the Hospital of the services and related products of the Supplier
- other (to be specified):

  ……
  ……
  ……

III. The categories of data subjects whose personal data are processed (indicate what is applicable and if necessary supplement):

- Hospital patients

- trusted persons, representatives and contact persons of the Hospital patients
- carers of the Hospital patients
- Hospital staff members
- other (to be specified):
  ……
  ……
  ……
  ……

IV. The processing of the personal data (indicate what is applicable and adapt/supplement where necessary):

The Hospital hereby gives the following instructions for the processing of personal data (without prejudice to the instructions arising directly from the provisions of the Basic Agreement or this Addendum or which are reasonably required for the Supplier to fulfil its obligations correctly):

- Consultation of personal data
  This refers to services provided by the Supplier whereby personal data of the Hospital can be viewed by staff or Subcontractors of the Supplier, including, but not limited to, servicedesk Services, (remote) monitoring Services, system management Services, technical application management, vulnerability scanning Services, reporting Services in governance and software asset management Services.

- Storage of personal data
  This refers to services provided by the Supplier whereby personal data of the Hospital are stored in a storage system delivered by the Supplier, such as, but not limited to, cloud storage Services, cloud back-up Services, file Services, directory Services, managed file transfer, mail & calendaring and logfile processing, providing support (helpdesk, remote monitoring, etc).

- Transmission of personal data
  This refers to services provided by the Supplier whereby personal data of the Hospital are transmitted by, to or between applications on a platform managed by the Supplier, including, but not limited to, LAN Services, Wide Area Network Services, data centre interconnectivity Services, Loadbalancing, SAN switch interconnects and Services provided using the Voice over Internet Protocol (VoIP).

- Adaptation or alteration of personal data
  This refers to services provided by the Supplier whereby personal data of the Hospital can be adapted either manually or automatically, such as in an automated job flow supported by a job scheduling system.

- Software tests
  This refers to services provided by the Supplier in which databases of the Hospital containing personal data (personal data which have not been anonymised) are used outside the production environment (in test, acceptance, etc.) as part of the testing process of the Hospital software application.

- [To be completed - optional]

IV. The storage periods of the (various categories of) personal data:

The Supplier stores the processed personal data in an appropriately secure manner for the period necessary to perform the written instructions of the Hospital, and with regard to the categories of personal data below, for the period specified below **[complete if storage period can be expressed in months]**:

- for **[complete category of data]** for **[XX months after/from…. e.g. the last use]**
- for **[complete category of data]** for **[XX months after/from…. e.g. the last use]**

V. The Data Protection Officer or other responsible contact persons for data protection and processing :

For the Hospital
Contact details: gegevensbescherming@uzbrussel.be and/or dpo@vub.be.

For the Supplier (complete)
Name:
Contact details:

VI. List of sub-processors

Depending on the agreed upon master agreement(s), the processor will use some or all of the following sub-processors and locations for its service provision. Please complete the list with all sub-processors, including apps, SaaS platforms, online accounts, cloud providers, software plug-ins, cookie-based exchanges, etc.

name sub-processor	*Registered office address*	*Location of processing*	*Nature of processing (description of the processing nature, assets, etc)*

VII. List of transfers to third countries

Data exporter	*Data importer*	*Country where the personal data is processed*	*Transfer instrument (SCC, BCR, …) and additional measures (if necessarys) (*)*

(*) if the Hospital is the data exporter and the European Standard Contractual Clauses (ESCCs) of the European Commission are used, these ESCCs will be added as Annex 5 to the data processing agreement.

ANNEX 3 – INFORMATION SECURITY

Questionnaire on information security and data protection for the processor

Name of the organisation (third party)	Name: ..... Address: .... Business number (Crossroads Bank): .....
First name, Surname & e-mail address of the chief information security officer (CISO) (mandatory)	....
First name, Surname & e-mail address of the information security contact person (assistant CISO) (optional)	....
First name, Surname & e-mail address of the data protection officer (DPO) (mandatory)	....
First name, Surname & e-mail address of the local data protection contact person (assistant DPO or representative) (optional)	....
First name, Surname & e-mail address of the person responsible for day-to-day management (CEO, mandatory)	....

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
1	Do you have a formal, up-to-date information security policy approved by the person responsible for day-to-day management?	☐ YES ☐ NO	
2	Do you have a risk assessment for each process/project for information security/data protection which you use for the provision of services?	☐ YES ☐ NO	
3	Within your organisation: • is there a department responsible for information security reporting directly to the person responsible for day-to-day management of the organisation?	☐ YES ☐ NO ☐ YES ☐ NO	
4	Do you have an information security plan approved by the person responsible for day-to-day management?	☐ YES ☐ NO	
5	How many hours are worked by the CISO and his/her team? • CISO • Team How many hours of training on information security have the DPO and his/her team followed? • DPO • Team	1) hours/month 2) hours/month 3) hours/year 4) hours/year	
6	Do you have procedures for the development of new systems or major changes to existing systems so that the project leader can take account of the security requirements described in the minimum security standards?	YES ☐ NO ☐ N/A ☐	
7	Do you take appropriate measures so that the professional, confidential and sensitive data stored on mobile media are accessible only to authorised persons?	☐ YES ☐ NO	
8	Do you take appropriate measures, depending on the access medium, for the information security of the access from outside your organisation to the professional, confidential and sensitive data?	☐ YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
9	Do you have teleworking facilities arranged in such a way that at the teleworking location (at home, in a satellite office or in another location) no information is stored on external appliances without encryption and that possible threats from the teleworking location do not reach the IT infrastructure?	☐ YES ☐ NO	
10	Do you call the attention of each staff member each year to information security and data protection and do you carry out an annual evaluation of compliance with this policy in practice?	☐ YES ☐ NO	
11	Have you secured access by means of a clear access procedure and have you implemented a (logical or physical) access system to prevent any unauthorised access?	☐ YES ☐ NO	
12	Do you have a classification system for personal data for which you are providing the services and do you apply this classification system?	☐ YES ☐ NO	
13	Have you processed the rules, specified in an 'E-mail, online communication and internet use' policy line, in an information security policy?	☐ YES ☐ NO	
14	Have you appointed at least one access manager when you make use of remote access to the healthcare institution?	☐ YES ☐ NO	
15	Have you encouraged your staff to read and apply extra security measures which the care provision imposes (if applicable)?	☐ YES ☐ NO	
16	If you wish to apply 'cryptography': • do you have a formal policy for the use of cryptographic controls? • do you have a formal policy for the use, protection and life of cryptographic keys for the entire lifecycle?	☐ YES ☐ NO ☐ YES ☐ NO	
17	Do you take the necessary measures to limit access to the buildings and premises to authorised persons and do you monitor this access both during and outside working hours?	☐ YES ☐ NO	
18	Do you take the necessary measures to prevent loss, damage, theft or compromise of equipment and interruption of the activities?	☐ YES ☐ NO	
19	In the case of reuse of the information carrier, do you use it again at a data classification level which is at least comparable?	☐ YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
20	Do you establish appropriate measures for the erasure of data contractually with the principal?	☐ YES ☐ NO	
21	Do you apply the rules relating to logging of access as stipulated by the principal?	☐ YES ☐ NO	
22	Have rules been laid down for the acquisition, development and maintenance of systems between the various parties concerned?	☐ YES ☐ NO	
23	Do all staff members work with ICT resources for the purposes of the assignment on the basis of minimum authorisation for the performance of their task?	☐ YES ☐ NO	
24	Have the access security requirements (identification, authentication, authorisation) been defined, documented, validated and communicated? Are these accesses logged?	☐ YES ☐ NO ☐ YES ☐ NO	
25	Are the security and data protection risks established contractually between you and any subcontractors?	☐ YES ☐ NO	
26	Do you use a checklist so that the project leader can obtain the assurance that all the information security and data protection policy lines have been evaluated correctly and if necessary implemented during the development phase of the project?	☐ YES ☐ NO	
27	Each time a project is put into production, do you carry out a check that the security and data protection requirements laid down at the beginning of the project were also in fact implemented?	☐ YES ☐ NO	
28	Under the supervision of the project leader, are there separated facilities for development, testing and/or acceptance and production – including the related separation of the responsibilities under the project?	☐ YES ☐ NO	
29	Is each access to personal and confidential data logged in accordance with a logging policy and the applicable laws and regulations?	☐ YES ☐ NO	
30	Is it included in project specifications how access to and use of systems and applications will be logged to contribute to the detection of divergences with regard to information security and data protection?	☐ YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
31	Does the log management at least comply with the following objectives? • The information to be able to determine by whom, when and how access was obtained to which information • The identification of the nature of the information consulted • The clear identification of the person	☐ YES ☐ NO	
32	Have the necessary tools been made available to allow the log data to be operated by the authorised persons?	☐ YES ☐ NO	
33	Do the transactional/functional log data correspond to the storage period corresponding to the data themselves (e.g. 30 years for medical data)?	☐ YES ☐ NO	
34	Are the project deliverables (processed data, documentation (source code, programs, technical documents, etc.) integrated in the back-up management system?	☐ YES ☐ NO	
35	In the course of the project development, have the requirements with regard to continuity of service provision been formalised, in accordance with your expectations?	☐ YES ☐ NO	
36	Have your continuity plan and the related procedures been updated in line with the development of the project, including continuity tests?	☐ YES ☐ NO	
37	Is a risk analysis carried out at the beginning of the project to define the emergency procedures?	☐ YES ☐ NO	
38	In the course of the project development, are the procedures concerning incident management formalised and validated?	☐ YES ☐ NO	
39	Is the CISO informed of security incidents and the DPO for incidents concerning data protection?	☐ YES ☐ NO	
40	During the lifecycle of the project, is the documentation (technical, procedures, manuals, etc.) kept up to date?	☐ YES ☐ NO	
41	Is all equipment, including purchased or developed systems added to the inventory of the operational resources?	☐ YES ☐ NO	
42	Is appropriate cooperation given to audits carried out in the form of the personnel being made available, documentation, log management and other information which is reasonably available?	☐ YES ☐ NO	
43	Are requirements concerning information security and data protection documented to mitigate risks concerning access to information tools?	☐ YES ☐ NO	
45	Are all relevant requirements concerning information security and privacy drawn up and agreed between you and third parties/suppliers (who	☐ YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
	read, process, store, communicate information of the organisation or supply ICT infrastructure components and ICT services)?		
46	Are the services provided to you by third parties/suppliers monitored, evaluated and audited?	☐ YES ☐ NO	
47	Are the changes in the provision of services to you by the third party/supplier managed, including keeping records of existing policy lines, procedures/measures for information security and data protection?	☐ YES ☐ NO	
48	Do you have a 'Cloud computing' policy line when you call on cloud services?	☐ YES ☐ NO	
49	When you wish to process professional, confidential or sensitive data in a cloud, do you satisfy the minimum contractual guarantees?	☐ YES ☐ NO	
50	Do you have procedures for establishment and management of incidents relating to information security or data protection with the related responsibilities and have you made these procedures known in-house?	☐ YES ☐ NO	
51	Do you have an agreement with all staff members that each staff member (permanent or temporary, in-house or external) is required to report unauthorised access, use, alteration, disclosure, loss or destruction of information and information systems?	☐ YES ☐ NO	
52	Are the incidents and weaknesses of information security or data protection relating to information and information systems made known to the principal so that you and the principal can take appropriate corrective measures in good time?	☐ YES ☐ NO	
53	Does the supplier have a procedure to communicate/report incidents concerning information security/data protection in-house as quickly as possible?	☐ YES ☐ NO	
54	In the case of information security or data protection incidents, is the evidence collected correctly in accordance with statutory and regulatory requirements?	☐ YES ☐ NO	
55	Is each information security or data protection incident formally validated so that procedures and control measures can be improved and are the lessons drawn from an incident communicated to your management for validation and approval of further actions?	☐ YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
56	Do you have a continuity plan for all critical processes and essential information systems?	☐ YES ☐ NO	
57	Are information security and data protection an integral part of your continuity management?	☐ YES ☐ NO	
58	Do you have your own continuity plan? Is this plan tested and adapted regularly with the necessary communication to your management for validation and approval?	☐ YES ☐ NO ☐ YES ☐ NO	
59	Do you carry out a conformity audit periodically with regard to the situation concerning information security and data protection?	☐ YES ☐ NO	
60	Do you have a formal disciplinary process for employees who have breached information security and data protection?	☐ YES ☐ NO	
61	Do you regularly collate all information to map the risks in connection with conformity with the GDPR and do you take the necessary actions as a result of a high 'residual' risk of non-conformity?	☐ YES ☐ NO	
62	Do you have an up-to-date central register of the controller or of the processor and do you have formal accountability for non-implementation of control measures focusing on compliance with the European Regulation for the specific processing?	☐ YES ☐ NO	

Date and signature of the CISO or data management officer (DPO) of the organisation (third party) (optional)	..... Date Signature
Date and signature of the person responsible for the day-to-day management of the organisation (third party) **(mandatory)**	..... Date Signature

******* END OF THIS DOCUMENT *******

ANNEX 4 – MODEL FORM FOR REPORTING OF DATA LEAKS

Details of contact person of the Hospital (contactable 24/7):
Department:
Telephone number

Date:
Company name:
Address:
Postcode:
VAT number
Who found the breach?
Name:
Job title:
When was the breach found?
Date:
Time:
Describe the security incident during which the breach of security of personal data occurred:

When did the breach take place?
a. On (date + time)
b. Between (date + time) and (date + time)
c. Not yet established
d. An anonymous report has been made by a third party
Establish context of the data involved in the breach:
Classification of the data:
a. None, the data cannot be attributed to an individual
b. Name and address data
c. Telephone numbers
d. E-mail addresses, Facebook IDs, Twitter IDs, etc.
e. User names, passwords or other login data, customer numbers
f. Financial data: account numbers, credit card numbers
g. National registration number
h. Copies of identity documents
i. Gender, data of birth, and/or age
j. Data concerning someone's religion or philosophy of life, race, political persuasion or membership of a trade union
k. Data concerning someone's health or sexual orientation
l. Personal data under criminal law or personal data about unlawful or annoying behaviour in connection with a prohibition imposed as a result of that behaviour
m. Data about someone's financial or economic situation, data on debts, salary and payment data
n. Derived financial data (income category, home ownership, car ownership)
o. Lifestyle characteristics (including family composition, housing situation, interests, demographic characteristics (age, gender, nationality, profession, education)
p. Data obtained from (public) social profiles (Facebook, LinkedIn and Twitter accounts, etc.)
q. Other, namely:
Classification of the context involved in the breach:

The breach involves the personal data of **how many** persons?
a. None, the data cannot be attributed to an individual
b. Not yet established
c. At least …… (number), but no more than ……..(number) involved
Describe the group of people whose personal data were involved in the breach:
Circumstances of the data leak:
a. Read only (an unauthorised third party was able to inspect (confidential) data. Processor still has the data in its possession.) – **Confidentiality is at risk**
b. Copy (an unauthorised third party was able to copy data. The data are still in the possession of Processor.) – **Confidentiality is at risk**
c. Alteration (an unauthorised third party was able to alter data in systems of the Processor – **Integrity is at risk**
d. Removal or destruction (an unauthorised third party removed data from the systems of the Processor or destroyed data.) – **Availability is at risk**
e. Theft – **Availability is at risk**
f. Not yet known
Were the Personal Data made incomprehensible or inaccessible for unauthorised third parties, for example by encryption and hashing?
Yes
No
Partly, i.e.
If so, how were the Personal Data encrypted?

Did the breach involve persons from other EU Member States?
Yes
No
If so, which EU Member States:
Which security measures (technical and organisational) have been implemented to tackle the breach and to prevent further breaches?
Who can be contacted for more information on the breach?
Name of contact person of the Supplier:
E-mail:
Telephone number:

ANNEX 5 – EUROPEAN STANDARD CONTRACTUAL CLAUSES (ESCCS) - OPTIONAL

[TO BE ADDED]