MYRIAN®
TERMS AND CONDITIONS OF SALE

1. VENDOR 'S IDENTIFICATION

INTRASENSE, a company with a capital of 2 613 100,75€ , whose registered office is located at 1231, avenue du Mondial 98, 34000 Montpellier, France and registered with the Trade and Companies Register of Montpellier, France under the number 452 479 504 (the "**Vendor**"), publishes and markets a medical imaging software named Myrian® , as well as all its optional modules, files, data and associated materials (the "**Software**") or services (the "**Additional Services and Options**").

2. PURPOSE AND SCOPE

2.1 These Terms and Conditions of Sales ("**TCs**") govern the relationship between the Vendor and any medical centre, hospital or healthcare professional wishing to purchase the Software sold by INTRASENSE (the "**Client**"). The Vendor and the Client are individually referred to as the "**Party**" and collectively as the "**Parties**".

2.2 These TCs may be modified at any time by the Vendor, without prior notice, in accordance with modifications made to the Software, changes in legislation, or for any other reason deemed necessary by the Vendor. In any event, the applicable TCs are those in force at the time the order is placed by the Client.

2.3 Any additional service or option relating to the use of the Software, subscribed to by the Client, may be the subject of special terms which will be fully applicable thereto.

2.4 The TCs, the ToU, the Data Processing Agreement, the Documentation, any applicable special conditions ("**Special Terms**") and the technical and commercial proposal (the "**Quotation**") constitute the entire agreement between the Parties (the "**Agreement**").

3. SOFTWARE FEATURES

3.1. The Software is made available on-premise, hosted by the Client itself on a dedicated server (the "**Server**") which is already installed within its information system, or which it wishes to acquire from the Vendor. Depending on the Client's requirements, the Software may be sold on its own or with the following components and services:

- Support and maintenance services as described in Article 5 and/or in applicable Special Terms;
- Third-party software distributed by the Vendor and technically linked to the Software in order to provide additional features;
- Specific integrated features;
- Server;
- Installation and configuration;
- Training for the Client and/or its staff.

3.2. The Client declares that it has been made aware of the essential characteristics and features of the Software, as well as the documentation drawn up by the Vendor in accordance with applicable regulations, and in particular Regulation (EU) 2017/745 concerning medical devices:

- Software's ToU;
- User guide;
- Privacy policy;
- Technical requirements.

(hereinafter together referred to as the "**Documentation**").

4. ORDER PROCESSING

4.1 Prerequisites

The Software is made available exclusively to healthcare professionals.

4.2 Evaluation phase

4.2.1 At the Client's request, and after approval of such by the Vendor, the Vendor makes available, free of charge and temporarily, the Software as well as the chosen Additional Services and Options, for evaluation purposes.
4.2.2 Where applicable, such evaluation phase shall for a maximum of fifteen (15) days. This eveluation period may be renewed once, subject to the agreement of both parties.
4.2.3 In the event of non-renewal or signature of a final agreement at the end of the evaluation phase, Client shall uninstall and cease all use of the Software, as well as to delete any installation or configuration carried out during this period. Vendor shall not be responsible for the retention of the data generated during such evaluation phase.

4.3 Order terms and conditions

4.3.1 At the Client's request to use or to continue using the Software, and after approval of such by the Vendor, the Vendor shall draw up a commercial proposal including *at least* the license price, a description of the Software, and if any (at the Client's specific request) the integration of specific features, the supply of a Server, the installation

of the Software, and/or training for the Client's staff (the "**Quotation**"). The Client then returns the signed Quotation to the Vendor for acceptance.

4.3.2 Acceptance by the Vendor of the Subscription shall not take place prior to receipt of full payment by the Client of the amount specified in the Quotation. Any Subscription shall only be deemed accepted by the Vendor if confirmed in writing by the Vendor within five (5) business days from the date of receipt of full payment of the price as set out in the Quotation.

4.3.3 By taking out a Subscription, the Client shall use the Software in accordance with the Agreement.

4.3.4 Any modification of the Subscription or waiver, after confirmation by the Vendor, shall be agreed in writing by the Vendor. The Vendor reserves the right to refuse the modification or waiver requested by the Client.

4.4 Term; Renewal

4.4.1 The duration of the Software's license and/or Additional Services and Options are set out in the Quotation.

5. FINANCIAL TERMS AND CONDITIONS

5.1 Applicable rates

The price is set in Euros excluding VAT, based on a price list drawn up by the Vendor and regularly updated.
The Software and/or Additional Services and Options is invoiced at the rate in force on the day of the order.

5.2 Payment terms

Payment terms are set in the Quotation. In the event that the Client fails to pay the amounts due to Vendor under the Agreement, and more specifically under the terms and conditions of the Quotation, the Agreement shall be suspended under the terms set out below.

5.3 Price's revision and indexation in case of renewal

5.3.1 Indexation

Unless specific indexation terms are indicated in the Quotation, the Vendor shall revise the Quotation price in case of a renewal, ipso jure and without prior notice, in line with changes in the French SYNTEC index, in accordance with the following formula:

$$P_1 = P_0 \frac{S_1}{S_0}$$

P1: revised price
P0: original Agreement price
S0: latest SYNTEC index published by French INSEE on the date of signature of the original Quotation or on the date of the previous revision.
S1: latest SYNTEC index published by INSEE on the revision date.

5.3.2 Revision of rates to reflect changes in the Software

Prices may also be revised in case of renewal of this Agreement, depending on changes (updates and/or enhancements) made by the Vendor to the Software. Where applicable, such revision reflects the implementation of new features.
The new pricing conditions, subject to acceptance by the Client, shall only apply from the date of renewal of the Agreement.

5.4 Early termination in the event of late payment

5.4.1 In the event of late payment of more than sixty (60) days, the Vendor is entitled to terminate the Agreement, notwithstanding any payment of its debt corresponding to the amount of the Subscription. Access to the Software and any Additional Services and Options shall then be suspended.

5.4.2 In this case, Client shall cease all use of the Software and undertakes to uninstall it from the Server immediately.

5.5 Late payment penalties

5.5.1 Any delay in payment shall bear interest, without prior notice to the Client, at a rate equal to the interest rate applied by the European Central Bank its most refinancing operation, increased by ten (10) percentage points. Client shall be liable to pay a fixed indemnity for collection costs of forty (40) euros, without prejudice to the Vendor's right to claim additional compensation should the actual recovery costs exceed this fixed sum.

5.5.2 Payment of late penalties begins on the first day following the end of the payment period and ends on the day of actual payment by the Client.

5.5.3 The Vendor may suspend the Subscription until full payment of the price still due by the Client.

5.6 Audit

5.6.1 The Vendor may, at its own expense and upon a fifty-day (15) prior notice to the Client, to audit the Client's use of the Software in compliance with the terms of this Agreement and/or the Documentation. Such audit may be

conducted by the Vendor or an independent third party selected by the Vendor.

5.6.2 The Client agrees to provide the Vendor or its designated auditor with access to all relevant records, systems, and personnel necessary to conduct the audit. The Client shall fully cooperate with the audit and provide any assistance reasonably requested by the Vendor.

5.6.3 In the event that the Client fails to comply with the audit request or is found to be in material breach of the terms of this Agreement, the Vendor reserves the right to impose the following penalties: immediate suspension of the Client's access to the Software until compliance is achieved; termination of this Agreement, with no refund of any fees paid and reimbursement of all costs incurred by the Vendor in the framework of such audit.

6. OBLIGATIONS OF THE VENDOR

6.1 Software delivery

6.1.1 After receipt of initial payment by the Vendor, the Vendor provides the Client items specified in the Quotation (Software with or without Server and installation, Additional Services and Options).

6.1.2 The Vendor shall provide an electronic copy of the Software via SharePoint Myrian delivery, with unique serial/activation numbers ("**Activation Keys**"), by email or by any other method agreed between the Parties in the Quotation.

6.1.3 The Software is accompanied by the Documentation, enabling it to be installed and used.

6.2 Provision of the Software

6.2.1 The Software is hosted on the Client's Server.

6.2.2 In the event that the Server is not correctly configured for installation of the Software (non-compatible operating system, prior installation of certain software components, etc.), the Vendor may, at the Client's request and in accordance with the Quotation, provide the elements required for the said installation.

6.2.3 Installation of the Software on the Server may be accompanied by training to enable the Client and/or any of its staff (the "**Users**"). This additional service shall be mentioned in the Quotation or may be the subject of a specific quotation.

6.3 Software installation

6.3.1 The Client shall ensure that an authorized person is available, either on-site or online, on the day of the installation of the Software and/or additional components and options to validate the installation. Once such installation is completed, the Vendor shall conduct tests to ensure the proper functioning of the Software. The Client shall confirm the proper functioning of the Software by signing the commissioning form provided by the Vendor, which shall constitute the final acceptance of the Software. Client's representative is deemed to be authorized, and any lack of delegation or authorization cannot be invoked against the Vendor.

6.3.2 In the event of installation delays due to difficulties in accessing or arranging the Client's premises, installation date shall be postponed, as such delays are considered attributable to the Client. The Client shall inform the Vendor in writing of any foreseeable delays resulting from difficulties in accessing or arranging its premises.

6.3.3 The Parties will use all means necessary to minimize such installation delays and will keep each other informed of the corrective measures taken.

6.4 Contractual warranty and Maintenance Packs

When placing an order, the Client may choose between the two following options for maintenance services:

- The Contractual Guarantee;
- The Premium Maintenance Pack.

Such options are further described in sections 6.4.1 and 6.4.2.

6.4.1 Contractual Guarantee

The Vendor supplies the Client for a period of twelve (12) months at no extra cost:

- Technical support, or if necessary;
- The option of making an appointment for "Premium" assistance for a fee;
- Corrective updates for the Software, which are supplied remotely.

Client support may be accessed:

- By telephone: +33 (0) 4 67 130 134
- By mail : support@intrasense.fr

The contractual Guarantee period begins upon Software's activation made by Client using the Activation Key.

6.4.2 Premium Maintenance Packs

If the Client opts for a Premium Maintenance Pack it shall benefit, throughout the maintenance period subscribed to, from a set of products and services, as detailed in the Quotation and herein, and which includes:

- Commissioning of the Software;
- Premium technical support;
- Monitoring and preventive maintenance;
- Two training sessions (initial; continuing);
- Access to major updates of the Software.

At the end of the initial commitment period, the Premium Maintenance Pack shall be renewed for the same duration, unless the Client notifies the Vendor in writing, with a certain date, at least six (6) months before the renewal date.

6.4.3 Post-contractual guarantee and post-Premium Maintenance Pack

At the end of the Contractual Warranty or Premium Maintenance Pack period, the Client will no longer be able to benefit from the services provided hereunder. Only corrective updates following medical device vigilance cases will be made available to the Client, free of charge. Client may request the Vendor for any additional services, such as support services (remote support, under terms available on Vendor's websites), training, or access to new versions of the Software that have obtained CE marking ("Major Versions"). Such services are subject to a detailed pricing schedule made available to the Client upon request.

6.4.4 Corrective maintenance

The Vendor shall provide correction of design and/or performance defects, bugs not attributable to the Client and other non-compliance of the Software with the Documentation (the "Errors"), subject to:

- Payment by the Client of the price set out in the Quotation;
- The Software not having been modified by the Client and/or the installation of a third-party application or system without the written prior agreement of the Vendor;
- The Client's infrastructure or computer system meeting the technical prerequisites set out in the Documentation;
- The Error not resulting from a use of the Software non-compliant with its medical purpose.

For the purposes of contacting the Vendor, the Client shall designate a dedicated contact person. Such Client's contact person shall inform the Vendor of any Error by e-mail or telephone. The Vendor will endeavour its best efforts to determine the cause of the Error(s), resolve such, or propose a workaround solution as soon as practicable. Only corrective maintenance necessary to remedy Error proven not to be attributable to the Client shall be handled by the Vendor. In the event that the Error is attributable to the Client, the Vendor's intervention shall be at the Client's sole expense, in accordance with the Vendor's current rates.

6.4.5 Updates

The Vendor may provide with new functions, corrections and improvements to the Software, depending on the type of maintenance selected by the Client:

- During the Contractual Guarantee term, the Client will benefit from updates aimed at correcting Errors, including those subject to medical device vigilance.
- The Client who have opted for a Premium Maintenance Pack will benefit, in addition to the updates listed above, from Major Versions throughout the subscribed maintenance period.

Where applicable, the Vendor will notify to the Client when updates are made available.

As the Vendor's intervention is carried out remotely, the Vendor's team will carry out the updates in coordination with the IT department Client's or any other person designated by the Client, in order to minimize the time taken to interrupt the service.

If it is not possible to access the Server remotely, an update script will be sent so that the IT department or any other person designated by the Client can carry out the update manually.

6.5 Backup

The data processed by the Software is periodically backed up using the *Picture Archiving and Communication System* (PACS) installed and administered by the Client to which the Software is connected to. The Vendor shall not be held liable for the functioning of such PACS, which depends on the Client's information system. Furthermore, it is the sole responsibility of the Client to ensure that the backup media remains accessible.

7. CLIENT'S OBLIGATIONS

7.1 Client's declarations

The Client declares to be acting and using the Software provided by the Vendor within the scope of their professional activity. The Client thus shall use the

Software and Additional Services and Options solely for medical purposes, in accordance with the Agreement.

7.2 Acknowledgement of technical prerequisites

The Client confirms having reviewed the technical specifications of the Software as well as the usage and installation prerequisites stipulated in the Documentation and acknowledges the compatibility of its equipment with such. The Client is informed that, in the absence of such compatibility, the Vendor may undertake the installation of necessary additional Components, subject to the financial terms specified in the Quotation.

7.3 Responsibility of the Client in the use of the Software

The Client is solely responsible for the use of the Software supplied by the Vendor, for medical purposes, in accordance with this Agreement, the Documentation, including the Terms of Use (the "**ToU**"), available on https://intrasense.fr.
In this respect, it is the sole responsibility of the Client, as a healthcare professional, to provide the necessary information to the patients and obtain their consent prior to the use of the Software.

7.4 Software security and data

7.4.1 Once the Software has been installed, the Client shall implement and maintain appropriate security measures to protect the Software against unauthorized access, alteration, unauthorized disclosure, or destruction. It is the Client's responsibility to actively monitor the Software for potential vulnerabilities and to implement the security patches and updates provided by the Vendor, where applicable. In the event of a security incident affecting the Software, the Client undertakes to inform the Vendor immediately and to apply any necessary corrective measures that may be communicated by the Vendor.
7.4.2 The Client is solely responsible for monitoring the Server, its proper operation and storage capacity, and for monitoring access to the Software and the Data hosted on it.

8. RIGHTS OF USE GRANTED TO THE CLIENT

8.1. The Vendor grants the Client a non-exclusive and non-transferable right to use the Software and the Additional Services and Options, in accordance with their intended purpose, this Agreement and the Documentation. This right of use, granted to the Client and/or Users, is granted for the territory in which the Client access the Software, for the duration of the Subscription. This right of use enables the Client to load, display and execute the Software.

8.2 . The Client is not authorized to:

- reproduce the Software made available, in whole or in part, by any means and in any form, either permanently or temporarily;
- translate, adapt, arrange or modify the Software, export it or merge it with any third computer software;
- make any copy of all or part of the Software, except as authorized herein;
- alter, adapt, in particular by translating, arrange and more generally modify all or part of the Software;
- decompile the Software for the purposes of reproduction not authorised hereunder;
- sell, rent, sub-license, distribute in any way whatsoever, transfer the Software;
- compile, decompile, disassemble, analyse, reverse engineer Software's source-code or attempt to do so, except to the extent permitted by law.

8.3 The Vendor is entitled to intervene on the Software to enable it to be used in accordance with its intended purpose. The Client is not authorized to have a third party directly or indirectly intervene on the Software. The license granted herein does not entail any transfer of intellectual property rights to the Software.

9. WARRANTY; LIABILITY

a) The connection to and use of the Client to the Software are under the sole responsibility of the Client. It is incumbent upon the Client to take all necessary measures to maintain such access. The Vendor shall be not held liable in the event of an inability to access the Software due to the Client's equipment and technical infrastructure and more generally due to non-compliance of the Client with the Agreement and/or the Documentation. The Client is informed that the Software may, due to its own actions or those of a third party, experience unavailability, slowdowns, interruptions, outages, and more generally, malfunctions inherent to the Client's network.

b) The Vendor shall be not held liable in the event of any damage, whether direct or indirect, arising from non-compliance of the Client with the Documentation. The Vendor shall not be held liable for damages not

directly and exclusively resulting from a failure of the Software.

c) The Vendor shall not be held liable for any damage, whether indirect or direct, caused by the Client's equipment or server infrastructure, which remains under the sole and entire responsibility of the Client. The Client shall take all necessary measures to protect its own data and/or software stored on their computer equipment. The Client shall be responsible for the integrity and compliance with applicable regulatory requirements of the diagnostic data hosted by the Client on the Software.

d) The Vendor shall not be held liable for any damages not directly and exclusively resulting from a failure of the Software. Therefore, the Vendor shall not be held liable for indirect or unforeseeable losses or damages of the Client, Users, or third parties, including but not limited to, loss, inaccuracy or corruption of files or data, loss of revenue or profit, loss of clientele, loss of opportunity, or the cost of obtaining a substitute product, service, or technology.

e) The Software is provided "as is". Unless otherwise stated in the Agreement, the Vendor makes no warranty regarding the Software, express or implied, including implied warranties of merchantability and non-infringement.

f) In any event, the liability of the Vendor is limited to the amount paid by the Client under the Quotation. The Vendor may only be held liable for any damage within one (1) year from the date of the damage.

10. CONFIDENTIALITY

The Parties shall keep confidential and not to disclose, communicate to third parties or use for personal purposes or for the benefit of third parties, any elements or information that may have been exchanged between them in the context of the negotiation of the Quotation or the performance of the Agreement.

11. INTELLECTUAL PROPERTY RIGHTS

Any modification of the Software, reproduction - in whole or in part - of trademarks, designs, models, or any other industrial property rights held by the Vendor, is prohibited. The intellectual property rights (including, but not limited to, patents, trademarks, and designs) associated with the Software shall remain the exclusive property of the Vendor. Failure to comply with the aforementioned obligations shall render the Client liable and may result in legal action.

The Vendor also reserves the right to oppose or to seek compensation for any use that it deems unfair, constituting an act of parasitism or unfair competition.

12. SOFTWARE SOURCE CODES

The Client will be able to continue to access the Software, in the latest version updated with the French Computer Program Protection Agency ("APP") on the date of the transmission request made by the Client, in the event of:

- cessation of the Vendor's business without a buyer having been officially appointed; or
- liquidation proceedings initiated against the Vendor.

As this grant of rights is personal to the Client, the latter may not grant sub-licences to third parties without the express agreement of the Vendor's representative, or the representative appointed for the liquidation.

13. PROCESSING OF PERSONAL DATA

For the purposes of this Agreement, the Vendor may process personal data ("Personal Data") as a processor within the meaning of European Regulation (EU) 2016/679 (hereinafter "GDPR"). Where applicable, the Vendor shall process Personal Data in compliance with GDPR and in accordance with the Appendix "Processing of Personal Data".

14. LIFETIME OF THE SOFTWARE AND ITS ADDITIONAL SERVICES AND OPTIONS

The lifespan of a Major Version of the Software, along with its additional services and options, is three (3) years. Once this period has expired, the version of the Software is considered obsolete and should no longer be used for clinical purposes. The Vendor shall not be held liable for any clinical use after the expiration of such lifespan. Vendor recommends contacting customer support at least three (3) months before the end-of-life date of their device to plan a software upgrade. This upgrade is included for clients who have subscribed to Premium Maintenance. The Client may subscribe to a Software upgrade service by contacting Vendor's sales department.

15. FORCE MAJEURE

Neither Party will be responsible for any delay or failure in performing any of its obligations hereunder due to causes of force majeure, which are the result of circumstances or events which are not reasonably foreseeable and are beyond such Party's reasonable control. The Party affected by a Force Majeure Event will advise the other Party in reasonable detail of the Force Majeure Event as promptly as practicable and keep the other Party reasonably apprised of progress in resolving the Force Majeure Event.

The Party affected by any Force Majeure Event is entitled to suspend the obligations arising from the Agreement for the duration of such Event. If, however, performance of the obligations becomes impossible for a period of more than two (2) months, either Party may terminate this Agreement without compensation by notifying the other Party by registered letter with acknowledgement of receipt.

16. MISCELLANEOUS

16.1 Severability

If any provision of this Agreement is found to be null and void under the applicable law or final judicial decision, it shall be deemed unwritten, without affecting the validity of the other provisions of the Agreement. In such a case, the Parties shall endeavor to substitute the nullified clause with one that closely approximates its legal and economic content.

16.2 Publicity

Client hereby grants to Docebo the express right to use Client's company logo and/ or name in its quarterly press releases, related earnings calls, investor presentations and its website to identify Client as a Docebo customer. Other than as expressly stated herein, neither Party shall use the other Party's name and/or logos without the prior written permission of the other Party.

16.3 Electronic signature

The Parties agree that the Agreement electronically signed :

- is drawn up in such a way as to guarantee the identity of the signatories and the integrity of the Agreement;
- is valid and enforceable between them. The Parties undertake not to contest the enforceability of the elements of the Agreement signed electronically on the basis of their electronic nature, nor the authenticity of the electronic signature;
- shall be considered as literal proof of the identity of the signatories and of their wish to approve its content under the same conditions and with the same probative force as a handwritten signature.

The version of the Agreement signed electronically and the associated certificate together constitute the original of the Agreement. Each Party undertakes to keep the original of the Agreement by its own means and not to damage its certificate.
Client's signatory is authorised by the Client and has the legal capacity to take out the Subscription, thereby committing the Client to the terms of the Agreement.

16.4 Assignment

The Client may not assign this Agreement without the Vendor's prior written consent, which consent shall not be unreasonably withheld or delayed, except that Client may assign or transfer this Agreement in connection with a sale of all or substantially all of Client's assets by providing the Vendor with prompt written notice of such assignment. Any assignment in violation of this section shall be void and of no effect. The Agreement shall be binding upon and inure to the benefit of the Parties and their successors and permitted assignees.

17. GOVERNING LAW. VENUE.

Any disputes arising from this Agreement shall governed by French law.
In the event of a conflict relating to the conditions of formation and/or execution of the Agreement, the Parties shall make their best efforts to reach an amicable settlement within one (1) month.
If no settlement is reached, any dispute arising from the Agreement shall be settled by the Commercial Court of Montpellier.

Appendix I: Data processing agreement

PREAMBLE
In order to provide assistance to the Client (hereinafter the "Controller"), during the management of incidents and/or any other request related to the Software within the framework of maintenance operations, INTRASENSE (hereinafter the "Processor") may occasionally need access to the Client's personal data.

The Controller and the Processor intend to comply with data processing requirements, including Regulation (EU) 2016/679 ("General Data Protection Regulation" or "GDPR").

Under this Data Processing Agreement (hereinafter "DPA"), the Controller and the Processor wish to define the purpose and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, as well as the obligations and rights of the Controller.

Article 1. Purpose and scope
a) The purpose of this Data Processing Agreement (hereinafter "DPA") is to ensure that the processing of personal data carried out as part of the performance of the Agreement complies with Article 28(3) and (4) of the GDPR.
b) These clauses apply to the processing of personal data as described Annex I.
c) These clauses are without prejudice to the obligations to which the Controller is subject under the GDPR.

Article 2. Interpretation
Where terms defined respectively in the appear in this DPA, they shall be understood as in the GDPR.

Article 3. Description of the processing operation(s)
Details of the processing operations, and in particular the categories of personal data and the purposes for which personal data are processed on behalf of the Controller, are set out in Annex I.

Article 4. Obligations of the parties

a) The Processor shall only process personal data on the basis of documented instructions from the Controller, unless it is required to do so under EU law or the law of the Member State to which it is subject. In this case, the Processor shall inform the Controller of this legal obligation prior to processing, unless prohibited by law on important grounds public interest. Instructions may also be given subsequently by the Controller throughout the processing of personal data. These instructions shall always be documented.

b) The Processor shall immediately inform the Controller if, in its opinion, an instruction given by the Controller constitutes a breach of the GDPR.

c) The Processor processes personal data solely for the specific purpose(s) of the processing, as defined in Annex I, unless otherwise instructed by the Controller. Processing by the Processor only takes place for the period specified Annex II.

d) The Processor shall implement at least the technical and organisational measures specified Annex II to ensure the security of personal data. These measures include the protection of data against any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data (personal data breach).

e) The Processor shall only members of its staff access to the personal data being processed to the extent strictly necessary for the performance, management and monitoring of the Agreement. The Processor shall ensure that the persons authorised to process personal data undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality.

f) The Processor shall make available to the Controller all the information required to demonstrate compliance with the obligations set out in this DPA. At the request of the Controller, the Processor shall also allow audits of the activities covered by these clauses to be carried out, up to a limit of one (1) annual audit. Processor shall be informed at least thirty (30) days before the conduct of the said audit. The Controller may decide to carry out the audit itself or to appoint an independent auditor. Audits may also include inspections of the Processor's premises or physical installations.

Article 5. Use of a Sub-processor

a) The Processor benefits from a general authorisation from the Controller to sub-contract to a sub-processor, the processing operations that it carries out on behalf of the Controller to this DPA.
b) Where the Processor engages a Sub-processor to carry out specific processing activities, it does so by means of a contract which imposes on the Sub-processor, in substance, the same data protection obligations as those imposed on the Processor under this DPA.
c) The Processor remains fully responsible to the Controller for the performance of the obligations of the subsequent in accordance with the contract concluded with the Sub-Processor. The Processor shall inform the Controller of any failure by the subsequent to fulfil its contractual obligations.

Article 6. International transfers

a) Any transfer of data to a third country by the Sub-Processor is only carried out on basis of documented instructions from the Controller or in order to comply with a specific requirement of law.
b) Where the Processor recruits a subsequent in accordance with Article 5, a Sub-processor to carry out specific processing activities (on behalf of the Controller) and these processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, Processor may ensure compliance with the Sub-processor by using the standard contractual clauses adopted by the European Commission.

Article 7. Assistance to the Controller

a) Where applicable, the Processor shall inform the Controller as soon as possible of any request it has received from a data subject. It shall not itself follow up such a request, unless authorised to do so by the Controller.

b) The Processor assists the Controller in fulfilling its obligation to respond to requests from data subjects to exercise their rights, taking into account the nature of the processing.

c) The Processor also helps the Controller to ensure compliance with the following obligations, taking into account the nature of the processing and the information available to the Processor:
   a. the obligation to carry out a "data protection impact assessment" (DPIA) when a type of processing likely to present a high risk for the rights and freedoms of natural persons. The Processor has carried out such an impact analysis on the Software, which it can make available to the Controller on request;
   b. the obligations set out in Article 32 of the GDPR.

Article 8. Notification of personal data breaches

In the event of a personal data breach, the Sub-Processor shall cooperate with the and assist in complying with its obligations under Articles 33 and 34 of the Controller GDPR, whichever is applicable, taking into account the nature of the processing and the information available to the Sub-Processor.

Article 9. Non-compliance with clauses and termination

a) If Processor does not comply with its obligations under this DPA, the Controller may instruct the Processor to suspend the processing of personal data until the Processor has complied with the DPA or the Agreement is terminated. The Processor shall promptly inform the Controller if it is unable to comply with these clauses for any reason whatsoever.
   b. The liability of the Parties arising out of or in connection with this DPA is subject to the limitation of liability as defined in the Agreement.

Description of the Personal Data Processing

- **People concerned**

The Personal Data concern the following categories of data subjects:

- Patients ;
- Healthcare Professionals acting as users of the Software.

- **Data categories**

The personal data to which the Subcontractor may have access concerns the following categories of data:

- Patients
  - Surname, first name, title

  - Gender
  - Date of birth, time of birth, age
  - Personnel number
  - Referenced patient sequence of images
- Users
  - Title, surname, first name
  - Title

Processing operations
The Sub-Processor connects to the only Software remotely, for the sole purpose of carrying out support operations. The data is pseudonymised.

Duration of the processing
The Processor shall have access to the Personal Data for the duration of the Agreement.

Sub-processors : N/A

Annex II: Technical and organisational measures implemented by Processor

Subdomain(s)	Measures	Processor Confirmation
Policies for information security	Processor has established an information security policy approved by management, that defines Processor's approach to managing its information security objectives. The policy is communicated to relevant staff and external parties.	YES ☒ NO ☐
Contact with authorities	Processor has procedures specifying when and who to contact (Controller and authorities) and how identified information security incidents are reported in a timely manner	YES ☒ NO ☐
Contact with special interest groups		
Information Security in project management	Processor adopts a security by design approach, through which it is able to consider information security in any design activity.	YES ☒ NO ☐
Terms and condition of employment	Contractual agreements between Processor and staff and contractors specify the mutual responsibilities regarding information security. Furthermore, when necessary, the responsibilities specify the terms and conditions of employment continuing for a defined period after employment ends.	YES ☒ NO ☐
Information security awareness, education and training	Processor enforces, for all the personnel and (when relevant) contractors, appropriate awareness, education, training, and periodic updates on organizational policies and procedures through an information security awareness program, established in line with Processor's security policies and relevant procedures.	YES ☒ NO ☐
Termination or change of employment responsibilities	Processor defines and enforces responsibilities and duties related to information security that remain in effect after termination or change in employment.	YES ☒ NO ☐
Disposal of media	Processor establishes standardized media disposal procedures to minimize the risk of leakage of confidential information to unauthorized personnel. Disposal procedures of media containing confidential information are consistent with the criticality of that information.	YES ☒ NO ☐
Access control policy	Processor defines an access control policy which restricts the access to information, applications, networks and network services to specifically authorized users. The policy is defined accordingly to the need-to-use and need-to-know principles.	YES ☒ NO ☐
Passwords management	Processor enforces the use of complex passwords through definition of formal policies.	YES ☒ NO ☐

Subdomain(s)	Measures	Processor Confirmation
User registration and de-registration	Processor defines formal processes regarding registration and de-registration, to enable assignment of access rights. Processor, furthermore, defines a formal process for assigning or revoking access rights for all user types and all systems and services.	YES ☒ NO ☐
Information access restriction	Processor enforces the use of strong security measures (e.g. MFA) and secure log-on through formal policies.	YES ☒ NO ☐
Policy on use of cryptographic controls	Processor has a policy regulating the use of in-transit and at-rest cryptography. Furthermore, Processor regulates the use, protection, and durability of cryptographic keys through their entire life cycle.	YES ☒ NO ☐
Key management		
Protecting against external and environmental threats	Processor has policies in place to enforce equipment safety from environmental threats and hazards, as well as unauthorized access opportunities. Furthermore, the equipment disposal process is managed ensuring any critical data or licensed software to be securely removed before dismission or re-use.	YES ☒ NO ☐
Working in secure areas		
Secure disposal or re-use of equipment		
Documented operating procedures	Processor documents procedures for operational activities related to information processing facilities such as system on/off, backup, equipment maintenance, media and mail handling, and computer room security.	YES ☒ NO ☐
Control against malware	Processor has in place malware detection (i.e. endpoint security), prevention (i.e. Intrusion Prevention Systems) and remediation controls. Specifically, Processor enforces the implementation of controls which prevent or detect the use of unauthorized software, together with reducing vulnerabilities that could be exploited by malware, such as through technical vulnerability management and installing, and regularly updating, software for malware detection and repair.	YES ☒ NO ☐
Information backup	Processor enforces that backup copies of information, software, and system are made and tested periodically. Furthermore, backups are stored at a remote site, with a level of physical and environmental security consistent with the standards applied at the main site, to avoid any damage in the event of a disaster to the main site.	YES ☒ NO ☐
Event logging	Processor enforces the logging of events, user activities, exceptions, malfunctions, and information security events is performed, and the logs are maintained, and periodically reviewed. Furthermore, appropriate privacy protection measures are applied, since event logs may contain critical and personal data.	YES ☒ NO ☐

Subdomain(s)	Measures	Processor Confirmation
Management of technical vulnerabilities	Processor has procedures to check on technical vulnerabilities of information systems. Furthermore, once a potential technical vulnerability has been identified, Processor identifies the related risks and actions to be taken (i.e. patching vulnerable systems).	YES ☒ NO ☐
Separation of development, testing and operational environments	Processor enforces the separation between development, test, and production environments to reduce the risk of unauthorized access or changes to the production environment, identifying and implementing the necessary level of separation to prevent operational issues.	YES ☒ NO ☐
Network controls	Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements.	YES ☒ NO ☐
Segregation in networks	Processor enforces the network segregation on all the groups of information services, users and information systems.	YES ☒ NO ☐
Confidentiality management	Processor sets up non-disclosure and confidentiality agreements between employees or external parties when needed. Furthermore, requirements and validity time for the agreements are reviewed periodically.	YES ☒ NO ☐
Security requirement analysis and specification	Processor sets up a change management process, together with having set up best practices for secure software development. Those practices are identified using policies and procedures.	YES ☒ NO ☐
Monitoring and Review of Supplier Services	Processor establishes a policy to properly manage subprocessors' relationships to address processes and procedures implemented by Processor itself, as well as the information security responsibilities that Processor requires suppliers to enforce.	YES ☒ NO ☐
Reporting Information security events	Processor adopts procedures to ensure an effective and orderly response in case of information security incidents, in particular in case of data breach.	YES ☒ NO ☐
Planning information security continuity Implementing information security continuity	Processor implements a crisis management, disaster recovery plan and a relative program of exercising and testing to validate over time the effectiveness of its strategy, in order to minimize impacts and ensure restore and return business activities from the temporary measures adopted during and after a disruption.	YES ☒ NO ☐
Identification of Applicable Legislation and Contractual Requirements	Processor has procedures in place to ensure compliance with statutory and contractual requirements for the use of material on which intellectual property rights may insist and for the use of proprietary software products. Furthermore, a personal data protection and privacy policy are developed and implemented to properly manage the organization's data.	YES ☒ NO ☐