Hitachi DPA Processor Generalized for Website Use

- Data Protection and Confidentiality Annex (DPA)
  - Appendix 1: Subject of Personal Data processing
  - Appendix 2: Technical and Organizational Measures (TOM)
  - Appendix 3: Template for reporting a Personal Data breach
  - Appendix 4: Definitions

Hitachi Medical Systems Europe Holding AG
Sumpfstrasse 13, CH-6312 Steinhausen, Phone +41 41 748 63 33, Fax +41 41 748 63 32
welcome@hitachi-medical-systems.com, UID CHE-108.383.716
www.hitachi-medical-systems.eu

Data Protection and Confidentiality Annex (DPA)

between the customer as Controller ("Controller") and Hitachi as Processor ("Processor"),

applicable on the basis of paragraph 12.2 of the General Terms and Conditions (GTC) of Hitachi Medical Systems Europe Holding AG dated 01.10.2018, in the case none specific DPA has been agreed.

1 Preamble

(a) This Annex and its Appendices hereto specify the data protection obligations of the Parties and its Subsidiaries in relation to the Processing of Personal Data within the scope of the Agreement or in the amendment thereto. The Processor or any Processor Subsidiary may have Access to or Process Personal Data of the Controller or obtain or collect Personal Data from or on behalf of the Controller.

(b) The Processor and/or his Subsidiaries will only Process Personal Data of the Controller, which has been transmitted by the controller or expressly released for processing. The Processor or his Subsidiaries will not use any Personal Data of the Controller for any purpose other than for the performance of his obligations as set out in the Agreement and/or Appendix 1 "Subject of Personal Data Processing".

(c) The Controller shall exclusively remain the controller of such Personal Data concerned of the Controller.

(d) This Annex and its Appendices shall take precedence over the Agreement, unless the Agreement expressly refers to a specific section of this Annex or its Appendices.

2 Obligations of Processor

2.1 Compliance with Data Protection Laws and Regulations

The Processor will comply with the Data Protection Laws and Regulations applicable to the Processor and Controller. The Processor will ensure that actions or omissions on his part do not lead to a situation in which the Controller violates any of the Data Protection Laws and Regulations. A separate instruction going beyond this Annex and its Appendices is not necessary in this respect.

2.2 Purpose of Processing

It is in Controller's sole and absolute discretion to determine the purposes of Processing of Personal Data. Such purpose will be defined in the Agreement and/or Appendix 1. The Processor declares and warrants that he will carry out the Processing solely for the purposes stated in the Agreement and that he will not at any time otherwise Process any Personal Data and will not keep them longer than it is necessary for the performance of the Agreement and/or Appendix 1. The Parties specify in the Agreement and/or in the Appendix 1 the subject matter and duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects.

2.3 Acting only on documented instructions

The Processor will Process the Personal Data only in accordance with the documented instructions of the Controller. This particularly in connection with a Third Country Transfer of Personal Data, unless required to do so by applicable Laws and/or Regulations to which the Processor is subject. In such a case, the Processor shall inform the Controller of that relevant legal requirement before the Processing, unless that applicable mandatory law does not prohibit such information on important reasons of public interest.

The Processor shall in any event set up, implement and guarantee that his Subsidiaries and/or Subprocessors carrying out any Processing and/or Third Country Transfer on behalf of the Processor set up and also implement such Adequate Safeguards and security measures to carry out any Processing and/or Third Country Transfer. This also includes the conclusion of EU Standard Contractual Clauses in the name and on behalf of the Controller.

Each act or omission of the Processor or his Subsidiaries or Subprocessors that constitutes a breach of the Adequate Safeguards shall be deemed to be acts or omissions by the Processor, and therefore a

serious infringement for which the Processor is liable in accordance with this Annex. The Processor shall make a Third Country Transfer only after implementation of such Adequate Safeguards. In case that the Processor does not comply with this clause 2.3, the Controller has the right to terminate all or any part of the Agreement without further penalty.

2.4 Confidential Information and security

The Processor ensures that persons authorized to Process the Personal Data on behalf of the Processor, have committed themselves contractually to confidentiality and security in the Processing of Personal Data or are under an appropriate statutory obligation of confidentiality and security and do keep and treat Personal Data as Confidential Information.

As a general rule, the Processor will treat all non-public information obtained in connection with the Agreement confidential and in line with the applicable confidentiality obligations. This rule applies in particular to (i) all Confidential Information concerning all clients of the Controller, including knowledge of whether or not someone is a client of the Controller, (ii) any Personal Data of a person be it a client or any other person of the Controller e.g. an employee, or a Processor of the Controller (data protection / privacy) and (iii) all non-public Confidential Information about the business of the Controller, such as his organization, operational and technical processes, infrastructure and systems, products and Services of the Controller or information on employees and contractual relations with third Parties (manufacturing and trade secrecy).

The Processor shall not transfer or disclose any Personal Data except: (i) where necessary to provide the Services under this Agreement; or (ii) with the written approval of the Controller; or (iii) when using a Subprocessor pursuant to clause 2.5**Error! Reference source not found.** in this Annex; or (iv) when required and permitted by applicable mandatory law, in which case the Processor will give the Controller written notice prior to such transfer or disclosure. Only after this, the Controller can challenge such transfer or disclosure.

The Processor shall take all Adequate Safeguards to prevent any transfer or disclosure if such transfer or disclosure is not in compliance with Data Protection Laws and Regulations and in order to protect Controller's rights and position.

2.5 Subprocessor

The Processor is authorized by the Controller to use Subprocessor to carry out the Processing as outlined in Annex 1, after the Processor has entered into a contract with the Subprocessor containing provisions corresponding to those in this Annex, in addition to any other provisions which the Con-troller may require.

The Processor shall inform the Controller of any intended changes concerning the addition or re-placement of other processors, thereby giving the Controller the opportunity to object to such chang-es.If it is a Subprocessor from a third country, its involvement is only possible if the Personal Data or other data of the Controller are not subject to professional or official secrecy. In all other cases, if a Subprocessor is involved, it is ensured in particular that an adequate level of data protection exists for Switzerland or the EU.

The Processor will ensure that each Subprocessor does not Process any Personal Data in violation of this Annex and the Data Protection Laws or Regulations or other applicable laws, in particular that the Subprocessor implements Adequate Safeguards, such as outlined in the Appendix 2: “Technical and organizational measures”.

Upon conclusion of the contract, the Subprocessors listed in Appendix 1: "Subject of Data processing" shall be approved by the Controller.

2.6 Rights of Data Subjects

Each Party acting as a Controller under this Agreement remains solely responsible for the adherence to the rights of the Data Subjects (including information, correction, destruction, blocking).

The rights of the Data Subjects are to be asserted against the responsible Controller. In the event of lawsuits from a Data Subject, the Controller has the sole right of decision.

If the Controller has an obligation under Data Protection Laws and Regulations to provide information to

the Data Subject about the Processing of his/her Personal Data, the Processor acting as a processor will provide without undue delay the relevant information to the Controller to the extent that he is in a position to do so under the existing Agreement. Furthermore, upon request by the Controller, the Processor will provide assistance including e.g. with appropriate technical and organizational measures in order for the Controller to comply with the rights of the Data Subjects within due time.

The Processor represents and warrants that he promptly notifies the Controller of any queries from a Data Subject, supervisory authorities or any other authorities in relation to any Personal Data which the Processor Processes, and does not comment on as part of the provision of the Services as Processor.

The Processor, acting as a processor, will follow instructions given by the Controller regarding the rectification, deletion and/or updating of any Personal Data to the extent that he is able to do so under the Agreement. Cost consequences at the expense of the Controller remain reserved.

2.7 Copies of Personal Data

The Processor might create copies or duplicates of Personal Data, especially if such a creation is necessary to provide and document the Services.

2.8 Technical and organizational security measures

The Processor shall implement and document appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account 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 natural persons (“Adequate Safeguards”).

The parties agree in detail on the implementation of the technical and organisational measures set out in Appendix 2: "Technical and organisational measures".

The Processor has to inform the Controller without undue delay in the event of a serious interruption in operations, in the event of suspicion of breaches of data protection and especially data loss or other irregularities in the Processing of Personal Data. For the notification, the Processor shall use the form set out in Appendix 3: "Template for reporting of data protection breaches" or a message form or type in terms of content and meaning, such as electronic messages via pre-defined interfaces or communication channels.

The Processor assists the Controller in ensuring compliance with the technical, administrative and organizational measures to be taken in accordance with the Data Protection Laws and Regulations, taking into account the nature of Processing and the information available to the Processor.

3 Obligations and Rights of Controller

3.1 Lawful processing

The Controller represents and warrants that the Personal Data provided to the Processor were processed lawfully (e.g. lawful collection, compliance with obligation to inform).

Unless already specified in the Agreement and/or any other Agreement(s), the Controller is obligated to instruct the Processor about the categories of Personal Data and the data recipients. The Controller acknowledges that special categories of Personal Data such as particularly sensitive Personal Data and Profiles require higher security measures, which may lead to cost consequences under certain circumstances.

3.2 Right to audit and monitor

The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Annex and/or Agreement and allows for and contributes to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. The Processor shall without undue delay inform the Controller if, in its opinion, an instruction infringes Data Protection Laws and Regulations.

The Processor shall provide the Controller with a copy of any operational audit reports carried out by independent bodies. Without prejudice to any clauses in the Agreement which have the right of audit and

monitoring, the Controller shall be entitled (together with its appointed external auditors), in consultation with the Processor and subject to a reasonable notice period, to inspect any relevant aspects of the Processor's security measures and procedures and to conduct its own security audits by a third party approved by the Processor (including penetration tests) with respect to the Personal Data. Penetration tests can only be carried out on the assumption that they have no operational effects. The Controller shall be fully liable to the Processor for all damages (including indirect damage) in connection with penetration tests. The Processor shall co-operate fully with any such inspections and audits and shall implement the valuable recommendations resulting therefrom within an agreed timeframe and, where appropriate, implement them at the expense of the Controller. It may be necessary to have the Controller staff be present on Processor's premises, when it is in the Controller's opinion to do so.

4 Liability

In the event of a breach of obligations under this Annex, the Controller may, at his sole discretion, either request that the Processor remedy the breach free of charge or have the breach remedied by a third party and recover from the Processor all costs incurred in connection therewith and reduce the payments due under the relevant service agreement by an appropriate amount, withholds payment and makes the Processor liable irrespective of his fault, unless the Processor proves that he has not breached any contractual obligation.

Each Party shall be liable to the other for itself and its Representatives up to a maximum of one year's compensation or to the contractual agreed amount for the violation of the Data Protection Laws and Regulations and for the violation of this Annex or a data protection provision of a service agreement, unless the other Party is guilty of the violation intentionally or grossly negligently. This is the case, among other things, if the Processor was instructed by the Controller to take an action or omission which is not in compliance with the Data Protection Laws and Regulations despite being informed it.

Each Party shall indemnify the other Party upon first request by and against all claims of third parties (including the persons concerned) regarding a breach of this Appendix, the Data Protection Laws and Regulations or data protection provisions of a service agreement, irrespective of whether such breach was committed by the indemnifying Party or one of its Representatives, suppliers or sellers, provided that the indemnifying Party is legally responsible for the breach. The indemnity obligation of the indemnifying Party includes without limitation all claims for damages of third parties, including costs and expenses incurred by the receiving Party in connection with the infringement or defence of claims of third parties.

The Parties are jointly and severally liable to the persons concerned within the meaning of Art. 82 para. 4 GDPR, if applicable. Any limitations of liability between the Controller and the persons concerned shall also apply in favor of the Processor.

5 Final Provisions

The Personal Data, any copies or reproductions made thereof remain Controller's property. Any right of retention of the Processor in relation to the Personal Data without the express written consent of the Controller is excluded. Unless set out otherwise in the Agreement, upon request by the Controller or upon termination of the Agreement for any reason, the Processor returns to the Controller or irrevocably destroys, all Personal Data of the Controller in his possession or under his control, except to the extent that such return or destruction is prohibited by Data Protection Laws and Regulations in the country in which the Processor carries out the Processing. Where such a return or destruction is prohibited, the remaining Personal Data must be kept as Confidential Information and no longer be processed by the Processor and be irrevocably deleted as soon as legally permissible. Upon request by the Controller, the Processor confirms in writing that he has complied with the obligations of this sub-section.

The Processor informs the Controller without undue delay, if the Processor reasonably believes that Controller's Personal Data in his possession or under his control is threatened with seizure or confiscation (e.g. in the course of insolvency or settlement proceedings or as a result of actions of a third party). In such a case, the Processor will initiate all measures to protect Controller's rights and position, in particular inform all involved Group Members and persons that authority over the data lies with the Controller.

Changes and amendments to this Annex and all of its components, including any assurances by the Controller, require written agreement and an explicit statement that they represent a change or

amendment to these conditions. The same applies to the waiving of this formal requirement.

If any provision of this Agreement (or any part thereof) shall be determined to be or shall become invalid, illegal or unenforceable, the remaining provisions will remain in full force and effect. Such invalid, illegal or unenforceable provision should be substituted by a mutually agreeable, valid and enforceable provision the effect of which is as close as possible to the intended effect of the invalid, illegal or unenforceable provision while maintaining the economic purposes and other intentions of the Parties. The same shall apply in cases of omissions.

This Annex on data protection and confidentiality shall be interpreted on the basis of material Swiss Law (mandatory alternative: the law of the Controller's place, if located in the EU), excluding the rules of International Private Law Rules and rules of other multilateral or bilateral international agreements.

The exclusive place of jurisdiction is according to the GTC.

Appendix 1: Subject of Personal Data Processing

1 Subject of the Personal Data Processing

For Support and Maintenance Controller must remove Patient Data or any other Personal Data. In rare cases for Support and Maintenance, such removal is not possible. In this context, Processor receives access to Patient Data or other Personal Data (see Section 6 below).

2 Purpose of Personal Data Processing

The purpose of Processing is for Support and Maintenance.

3 Categories of Personal Data

Patient Name	Patient Occupation
Patient Birth Date	Sonographer
Relevant Doctor	Procedure ID
Patient ID	Accession Number
Patient Sex	Study ID
Patient Age	Study Description
Patient Height	Referring Physician
Patient Weight	Reporting Physician

4 Special categories of Personal Data

Patient Medical Data
Patient Ultrasonic Picture, in connection with Personal Data as shown in para. 6 above.

5 Categories of Data Subjects

Patients of Controller
Employee of Controller

6 Third Country Transfer

In general, no transfer to Third Countries of patient data is done, which do not have equivalent data protection level recognized by the European Data Protection Board. However in very rare cases the medical devices need to be transfer and with it patient data to Hitachi Medical Service and Logistics in Germany.

7 Approved Subprocessors + Place of Personal Data Processing

	Name	Address	Place of Personal Data Processing	Category of Personal Data
1.	Hitachi Vantara Corporation	2845 Lafayette St, USA-Santa Clara, CA 95050	USA / India with aequivalent data protection level (EU Contractual Standard Clauses)	Customer Data (contact person, no patient data)
2.	Intl. 2nd Level Support HMSE	Thyssenstrasse 12, DE-32312 Lübbecke.	Germany	Patient Data
3	Hitachi Medical Systems Logistics and Services, Branch Hitachi Medical Systems Europe Holding AG	Otto-von-Guericke-Ring 3,DE-65205 Wiesbaden	Germany	Patient Data
4	Transporter	n/a	In transition from your site to 2. or 3. In case repair is only possible on premise of repair center	Patient Data

Appendix 2: Technical and Organizational Measures (TOM)

1 Objective

Description of the technical and organisational security measures (TOM) implemented by the Processor to secure data and systems in accordance with the provisions of the EU Regulation (EU) 2016/679 on General Data Protection Regulation (hereafter "GDPR") and the Swiss Federal Act on Data Protection of 19 June 1992 (hereafter "FADP", SR 235.1), specifies all measures which the Processor has taken to ensure confidentiality, integrity, availability and resilience of systems and services.

This TOM is applicable, where it has been integrated by reference upon a specific agreement or due reference by paragraph 12.2 of the GTC.

It applies where the Processor has access to Controller's Data (hereafter "Data") and/or to Controller's systems respectively products on which Data is processed within the scope of contractual services (hereafter "Services").

The Controller and its Representatives must in advance and if technically possible delete and backup all Data from the system or product and/or close all applications that contain Personal Data, so that the Processor has during its Service no access and cannot use any Controller Data.

2 Principles

Security measures shall take into account 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 natural persons. The security measures of the Processor shall safeguard a level of security appropriate to the risk, including inter alia as appropriate:

(i) the pseudonymisation or encryption of Controller's Data;
(ii) the ability to safeguard the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(iii) the ability to restore the availability and access to Controller Data downloaded or transferred to systems of the Processor in a timely manner in the event of a physical or technical incident on these systems; and
(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Security measures shall comply with minimum security measures, if any, set forth by national data protection laws and regulations applicable to the Processor.

3 Risk Assessments

Processor performs regular risk assessments to:

(i) identify reasonably foreseeable threats that could result in unauthorized access, copying, use, processing, disclosure, alteration, transfer, loss or destruction of any of any of the Data,
(ii) asses the likelihood of these risks and the damage they might cause to data subjects and
(iii) to assess if the existing technical, administrative and organisational security measures are sufficient to comply with the data protection laws and regulations applicable to the Processor.

Processor shall provide the Controller with a written summary of the risk assessment on request.

4 Organizational Security Measures

Processor has the following organization, which supports the data security:

(i) Processor maintains and implements a documented IT Use and Data Policy, approved

by its senior management, published and available to all employees and contractors.

(ii) Processor ensures that all its Representatives comply with this TOM. Additionally communicated IT security measures by the Controller to Processor are subject to change procedure and might cause additional costs for the Controller;

(iii) Processor applies commercially reasonable measures to separate Patient Data of Controller by technical and organizational measures from Processor's infrastructure (examples of measures: physical or logical separation of Patient Data); and

(iv) only where Processor has access to Controller Patient Data due to the fact, that Controller has not saved and/or cleaned its system respectively product from Patient Data, Processor will use best efforts to avoid causing damage to the systems and/or products and Patient Data of the Controller by any act, omission or negligence of Processor or any of its Representatives.

5 Technical Security Measures

5.1 Access Controls

(i) Processor will aim to ensure that Controller Data, if any on Processor infrastructure, is maintained in a physically secure environment to which only Processor authorized Personnel have access ("**Access rights policies**")

(ii) Processor grants physical access to Processor's premises, systems, applications, networks used for the Services to the extent required only;

(iii) Processor implements appropriate security measures and procedures to protect, and prevent the unauthorized viewing, copying, alteration or removal of any media or systems containing Controller Data, wherever located, and in whatever form e.g. by restrict access to physical Data, implementing firewalls, network based security monitoring, intrusion prevention systems, remote network access secured with VPN, by applying clear desk/clear screen procedures or lock Data away.

(iv) Processor applies segregation of duties principle and documents it on Processors infrastructure;

(v) Processor reviews routinely access rights (incl. privileged access) to systems. Processor revokes access rights immediately, where no longer needed. Persons are entitled to access Controller Data only on a need to know basis and only after additional agreement with the Controller. Controller Patient Data is not copied, modified or removed without additional explicit authorization in the course of the processing or storage ("**Authorization procedures for persons entitled to access**"); and

(vi) Where Processor or its Representative have remote access to Controller Patient Data, Controller or its Personnel shall remove Patient Data before granting access or ensure appropriate adequate safeguards (e.g. EU Standard Clauses).

(vii) Processor has procedures in place to destructs electronic data carriers and printed document securely with Controller Patient Data ("**Secure media and Data destruction**");

(viii) appropriate security measures and procedures for strong authentication of authorized Personnel, including the following ("**Authentication credentials and procedures**"):

a. Strong passwords (minimum of 8 characters minimum, special characters, numbers and letters) are used on all systems and applications. Such passwords must be modified by the Personnel when they are first used as well as at least every three months thereafter;

b. The maximum number of failed consecutive login attempts are limited and if exceeded access blocked until the password is reset by authorized Personnel;

c. Passwords are issued and relayed in a secure manner and issued after verifying the identity of the requestor;

d. Default passwords are required to be changed when placed into production;
e. Password will not be stored or transmitted in readable form.
f. When privileged access (e.g. root or super user level access) is granted to Processors systems which handle Controller Data and/or are used to provide Services, such access shall only occur from Subprocessor authorized by Controller;
g. Access to Processor Data are anti-virus and anti-malware protected and active and signature updates are installed in a timely manner.
h. Processors Personnel end user devices are encrypted.
i. Critical OS patches are installed in a timely manner.

(ix) It is the duty of Controller to back up data and remove Patient Data before any access and Processing of such data by Processor. Processor Personnel on Controller premiss might see Patient Data. Only in the extraordinary case a Processor product needs to be returned to Processor (e.g. system crash), Controller Patient Data might be accessed and processed by Processor and/or Subprocessor. In such a case additional consent from Controller is required.

(x) For some Processor Products, Patient Data shall be pseudonymized before any downloading is performed by Processor.

(xi) In any event, Processor will not store Patient Data as a principle, unless it is an approved and documented Process by Processor and additional explicit consent of the Controller is given.

5.2 Integrity Controls

(i) Except as necessary for the provision of the Services in accordance with the Agreement, Controller Data must not be read, copied, modified or removed without authorization during transfer or storage and it must be possible to establish to whom Controller Data was transferred to ("**Prohibition of processing beyond the aim of processing**").

(ii) Controller Data being processed by a Processor must be processed solely in accordance with the Agreement and related instructions of Controller ("**Data processing control**").

(iii) Processor has measures and procedures in place to aim to ensure that it is possible to check and establish whether, when, and by whom Controller Data has been inputed into Processor's information systems, or accessed, copied, modified, or removed ("**Data input control**").

(iv) Processor has appropriate security measures and procedures to protect the integrity of the Controller Data, to prevent the unauthorized recording, alteration or erasure of Controller Data, and to ensure that it is subsequently possible to determine when, by whom and which Controller Data were recorded, altered or erased. ("**Data integrity controls"**).

5.3 Availability

(i) Controller must back-up Controller Data to protect its Data from loss and from accidental destruction. In case the Processor has access to Controller Data, he will first back up Controller's Data on Controller systems and only where specially agreed on Processors systems. In both cases Controller will only after a secure back-up work on the systems / products without Controller Data on it (**"Data availability control"**).

(ii) All hosts operating systems of Processor are secured, which includes but is not limited to:

a. Inactivity timeouts;

b. Unused ports/services are turned off;
c. Systems are patched and using up-to-date and supported software versions; and
d. Virus are any viruses, worms trojans, malware and other malicious codes or malfunction software, code or tools, software locks, backdoors, time bombs, program access denials, similar disabling codes or other shutdown mechanisms, and any other features or devices that would impair or hinder, in any way, the use or operation of the product or the Data (hereafter “Virus”). Processor will use Anti-Virus solutions, including application of timely application of signatures. Processor will check against Viruses software or data provided or introduced to Controller before providing or introduction it. All Virus checks performed by the Processor will be carried out before use upon state-of-the-art anti-Virus software (then available to the software industry). Processor and Controller shall perform Virus checks on its own systems in accordance with its own policies and procedures and evidence of this having been completed shall be provided the other party reasonable request.

5.4 Vulnerability Scans

Processor maintains the following technical and administrative measures in the context of vulnerabilities:

(i) Servers, end-points, networks and applications on side of the Processor are scanned on a periodic basis;
(ii) Vulnerabilities are remediated taking into consideration the risk and impact of those vulnerabilities;
(iii) Processor has a formal vulnerability management program in place that drives remediation of vulnerabilities

6 Training and education

Processor shall institute an appropriate training and education program to ensure that its Personnel are trained to, and will, implement and comply with its IT Use and Data Policy, and to ensure that they are adequately aware of their responsibilities under the IT Use and Data Policy.

7 Subprocessors

If Processor uses Subprocessor, then Processor shall ensure that Subprocesor shall comply with security measures commensurate with those described in this TOM.

8 Incident management/escalation

Processor shall develop and implement an incident response plan for dealing with any security incidents which is in the context of the provisioning of the Service, to be shared with Controller, including escalation paths to senior management based on the incident classification or severity, incident contact lists, initial responses, investigation log, system recovery, issue and eradication, reporting and review and follow up procedures, including appropriate reports to regulatory and law enforcement agencies. Processor shall review the incident response plan regularly in order to verify that the incident response plan remain accurate, comprehensive and up to date.

Processor shall without undue delay report to Controller all incidents that may in any way affect the operations of Controller, the confidentiality, availability or integrity of Controller Data, Processor's information systems or the Services provided by the Processor. Processor shall reasonably co-operate with Controller and any persons acting on its behalf to enable Controller

to investigate any such incident.

9 Documentation, Review and Investigation

Processor shall document and give access to review and investigation as outlined below:

(i) Logs are kept for 3 (three) months in order that the processing steps that were actually performed, in particular modifications, consultations and transmissions, can be traced to the extent necessary with regard to their permissibility.

(ii) Processor shall promptly provide Controller with a copy of a summary of operational audit reports, which have been completed by any independent body.

(iii) Without prejudice to any clauses in the Agreement dealing with the right to audit and monitor, Controller shall be entitled (together with its external auditors or any regulatory authority), in consultation with Processor and observing a reasonable notice period, to inspect any aspect of Processor's security measures and procedures and to conduct its own security tests (including penetration tests) with respect to the Controller Data. Costs of such audit shall be fully born by Controller.

(iv) Processor shall implement any reasonable resulting recommendations within an agreed timeframe thereafter. Where in Controller's reasonable opinion, it is necessary to have its Personnel be present on Processor premises, Processor agrees to accommodate the presence of any Controller's Personnel at Controller's expense.

Appendix 3: Template for reporting a Personal Data Breach

Reporting Organisation and Controller Information

Organisation, where Data Breach occurred

Role: ☐ Controller ☐ Processor ☐ .....

Name of Organisation: .....

Address of Organisation: .....

Specific Department: .....

Affected Systems: .....

Website (if affected): .....

DPO or CDP Name: .....

DPO or CDP Contact Information: .....

Reporting Person

Full Name: .....

Function in Organisation: .....

Contact Information: .....

Controller of affected Data *[if Data Breach did not happen at Controller]*

.....

Name of Organisation: .....

Address of Organisation: .....

DPO or CDP Name: .....

DPO or CDP Contact Information:

Personal Data Breach Information

Type

☐ Data Theft	☐ Data Loss	☐ Data manipulation
☐ Cyberattack	☐ Ransomware	☐ Malware
☐ Phishing	☐ Misdelivery of data	☐ Erroneous deletion of data

☐ .....

Dates

Incident Date: .....

Time Span of the Incident: .....

Date of Discovery: .....

Description

[What's the situation? / Where did it happen? / How was it discovered? / Who was informed?]

.....

.....

.....

Data Subject and Personal Data affected

Category of Data Subject

☐ Employee	☐ Client / Customer	☐ Supplier
☐ User (Service)	☐ User (Website)	☐ Minors

☐ .....

Category of Data Records

☐ Name	☐ Postal Address	☐ Date of Birth
☐ ID/Passport Number	☐ Tax Identification Number	☐ Social Security Number
☐ E-Mail Address	☐ Username	☐ Password
☐ Location/GPS Data	☐ Photos / Videos	☐ Biometric Data
☐ Banking Details	☐ Credit Card Information	☐ Financial Records
☐ Health Records	☐ Professional Secrecy	☐ Trade Secrets
☐ Criminal Records	☐ Sexuality	☐ Politics
☐ Ethnic	☐ Religion	

☐

Dimension

Number of affected…

Data Subjects: ..... Data Records: .....

Consequences of the Personal Data Breach

Consequences in General

occurred (o) / potential (p)

o	p		o	p		o	p	
☐	☐	Data Loss	☐	☐	Breach of Confidentiality	☐	☐	Restriction of Availability
☐	☐	Data Released						
☐	☐	.....						

Consequences for Data Subjects

occurred (o) / potential (p)

o	p		o	p		o	p	
☐	☐	Financial damage	☐	☐	Reputational Damage	☐	☐	Identity Theft or Fraud
☐	☐	Revelation of Secrecy	☐	☐	Social Impact	☐	☐	Economic Impact
☐	☐	.....						

Prevention

Measures

taken (t) / proposed (p)

t	p		t	p		t	p	
☐	☐	System Shutdown	☐	☐	System Disconnected	☐	☐	Evidence Secured
☐	☐	Report to Controller	☐	☐	Report to Data Subject	☐	☐	Report to Police / Authority
☐	☐							

If, at the time of notification, one or more facts cannot yet be established, the reporting organisation may make a further notification at a later date.

Legally binding confirmation of the correctness and completeness of the information:

Place, Date: …….....

…….....
Management of the reporting organisation

…….....
Counselor Data Protection (CDP) / Data Protection Officer (DPO) of the reporting organisation

Appendix 4: Definitions

Access or Remote Access	means the activity or capability of creating, viewing, modifying, transmitting, storing, or the Processing of Controller's or Processor's assets, such as values, media and data carriers, etc.;
Agreement	means the agreement between the Parties on the basis of which the General Terms and Conditions (GTC) and this Data Processing Agreement (DPA) have become applicable;
Adequate Safeguards	means all measures for the Processing of Personal Data in accordance with the Laws and Regulations on Data Protection in order to ensure a level of protection appropriate to the risk and is specified in Appendix 2: "Technical and organisational measures";
Confidential Information	means all non-public information relating to a Party or any of its Group Members which is in oral, written, electronic or any other form disclosed by a Party or one of its Group Members (herein referred to as "Disclosing Party") to the other Party or one of its Group Members (herein referred to as "Recipient") or which the Recipient otherwise learns or becomes aware of during the performance of Services under the Agreement. Confidential Information shall include, but not be limited to, technological or organizational processes, customers, personnel, business activities, databases, intellectual property, the terms and conditions of any Agreement and other information in relation to it, and any other information which is reasonably or customarily considered to be of a confidential or otherwise sensitive nature, whether or not it is specifically marked confidential, such as manufacturing and business secrets. Confidential Information shall not include any information, which (i) was in Recipient's lawful possession without a confidentiality obligation prior to the disclosure and was not obtained by Recipient either directly or indirectly from the Disclosing Party, or (ii) is or becomes publicly available through authorized disclosure by the owner of such information, or (iii) is rightfully obtained by the Recipient from a third Party, who has the right to transfer or dis-close it on a non-confidential basis, or (iv) is independently developed by the Recipient without any reference to Confidential Information of the Disclosing Party, as evidenced by the records of the Recipient;
Controller	means the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;
Data	means any Personal Data of the Controller, such as employee Personal Data as well as Patient Data of the Controller or any other confidential data to which Processor has access in the provisioning of the Service;
Data Protection Laws and Regulations	means laws and regulations regulating data privacy and/or the Processing of Personal Data in respect of Controller and Processor such as but not limited to the Regulation 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 (General Data Protection Regulation) and the Swiss Federal Act on Data Protection, SR 235.1; including the National Data Protection Laws and Regulations applicable to each Controller and/or each Group Member of the Controller;

Data Subject(s)	means an identified or identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, IP-address, location data, an online identifier or to one or more factors specific to the physical, physio-logical, genetic, mental, economic, cultural or social identity of that natural person, except that Data Subject shall also include (i) persons other than living individuals and (ii) legal entities to the extent that the Processing of a legal entity's Personal Data is regulated by a Data Protection Laws or Regulation;
EU Standard Contractual Clauses	means the standard contractual clauses as per the European Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, as amended by Commission Decision 2004/915/EC of 27 December 2004, and as further amended from time to time. In case of amendments of the EU Standard Clauses by a competent supervisory authority, reference to the EU Standard Clauses shall be deemed to be addressed to the amended EU Standard Clauses as appropriate;
Controller Personal Data	includes but is not limited to Personal Data of its Representatives, customers and/or Processors of Controller;
Group Member	means Controller or its Affiliates and Subsidiary or Processor or Processor Entity, as the case may be;
Party / Parties	means the party or parties defined in the Agreement and includes any permitted assignees and successors of such Party;
Patient Data	means any Personal Data of the Controller's patients;
Personal Data	means any information relating to a Data Subject, including data concerning health and genetic data in accordance with this Agreement and Data Protection Laws and Regulations;
Personnel	means a Representative of Controller or Controller entity;
Processing / Process	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as Access, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Processor	means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of the Controller;
Pseudonymisation	means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure re-identification is not possible;
Representatives	shall include personnel, directors, officers, employees, agents, advisers, contractors, Subprocessors, and any other type of authorized representatives and advisers of any Party as applicable, as well as Personnel, as the case may be;
Third Country Transfer	means a transfer of Personal Data to a Subsidiary which is in a country which (for the purposes of this Annex) does not provide an Adequate Safeguard;

Services	include (1) the services, functions and responsibilities described in the Agreement, including the provision of deliverables, if any, and which might include as well as any warranty remedies provided by Processor or Processor Entity free of charge to Controller and/or its Subsidiary (2) the services, functions and responsibilities reasonably related to the Agreement and being performed in the months prior to the applicable service commencement date by or on behalf of Processor, its Subsidiary or third Party Processor, whose services, functions or responsibilities shall be eliminated as a consequence of the Agreement, even if not specifically described in any of the Agreements; and (3) any services, functions or responsibilities not specifically described in any of the Agreements but that are required for the proper performance and provision of the services as described in (1) and (2);
Subprocessor(s)	means any agent, contractor or other third party mandated by Processor;
Subsidiary(ies)	means any partially (more than 51% voting rights) or fully controlled subsidiary, branch, affiliate or representative office.