Data Processing Agreement

This Data Protection Agreement and its annexes ("DPA" or "Contract") establishes minimum data protection and cyber-security standards and related requirements and forms part of the contract, including a commercial agreement, a service agreement or an order (the "Agreement"). This DPA is entered into by and between the Customer (as defined in the Agreement) and Leica (as defined in the Agreement,) and shall continue in full force and effect for the duration of the Agreement. Leica Biosystems (hereinafter referred to as the "Contract Processor") and Customer (hereinafter referred to as the "Responsible Entity" or "Controller") are hereinafter individually referred to as a "Party" or collectively as the "Parties".

The Parties agree that where there is Processing of Personal Data under the Agreement, the terms of this DPA will apply to that Agreement, whether or not expressly referenced in that Agreement.

Preamble

As far as the Contract Processor conducts any installation, maintenance (remote maintenance and maintenance in the premises of the Responsible Entity) or repair work of the systems delivered to the Customer by Leica Biosystems ("Data Processing Systems") on behalf of the Responsible Entity or trains the Responsible Entity on the Data Processing Systems or provides any other support services with respect to the use of the Data Processing Systems, any access to Personal Data of the Responsible Entity within the meaning of the Applicable Law cannot be excluded.

For these reasons, the Parties conclude this Contract in the above-mentioned cases. This Contract sets out the obligations of the Contract Parties with respect to data processing resulting from the contract processing by the Contract Processor for the Responsible Entity according to the Applicable Law.

Any details on software installation, remote training, software diagnostics, or other support services with respect to the Data Processing System will be defined amicably by the Parties within the existing business relationships.

§ 1 Definitions

(A) "Applicable Law" means any law (including all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question including, where applicable, EU Data Protection Law), rule or regulation applicable to the Agreement, the Services, or Parties and applicable industry standards concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling or Processing (including retention and disclosure) of Personal Data, as may be amended, regulated, restated or replaced from time to time.

(B) "Controller", "Processor", "Data Subject", "Personal Data or Personal Information", "Process", "Processing", "Special Categories of Personal Data" and "Sensitive Personal Information" shall have the meanings given in Applicable Law.

(C) "Data Breach" means, (i) the loss or misuse (by any means) of Personal Data; (ii) the inadvertent, unauthorized, and/or unlawful disclosure, access, alteration, corruption, transfer, sale, rental, destruction, or use of Personal Data; (iii) any other act or omission that compromises or

may com-promise the security, confidentiality, or integrity of Personal Data, or (iv) any breach of security safeguards.

(D) “EU / UK / Swiss Data Protection Law” means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation (“EU GDPR”); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) in Switzerland the Federal Act on Data Protection of 19 June 1992 (revised version) (the “FADP”); (iv) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under or pursuant to (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

(E) “Personal Data” means, in any form, format or media, any (a) confidential information of Responsible Entity; and/or (b) data which means any information that can identify an individual. For clarity, Personal Data also means Personal Information.

(F) “Restricted Transfer” means either an EEA Restricted Transfer, a Swiss Restricted Transfer or a UK Restricted Transfer.

(G) “Standard Contractual Clauses” means Module 2 of the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, located at http://data.europa.eu/eli/dec_impl/2021/914/oj and as incorporated herein by reference.

(H) “Swiss Restricted Transfer” shall mean a transfer of Personal Data from or which originated in Switzerland to a country outside of Switzerland that is not considered to provide an “adequate level” of data protection by the Swiss Federal Data Protection and Information Commissioner (“FDPIC”) and where such transfer is subject to the FADP. where the FADP applies, the model contracts and standard contractual clauses recognized per the Swiss Federal Data Protection and Information Commissioner (“FDPIC”) pursuant to Article 6 paragraph 2 letter a of the FADP in accordance with the statement of the FDPIC of 27 August 2021 (“Swiss Addendum”)

(I) “UK Restricted Transfer” means a transfer of Personal Data from or which originated in the UK to a country outside of the UK that is not considered to provide an “adequate level” of data protection by the UK Government and where such transfer is subject to the UK GDPR.

(J) “UK Addendum” means the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner’s Office, located at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf and as in force as of the date of execution of the Agreement, and as incorporated herein by reference.

(K) “Services” means those services that Leica Biosystems performs pursuant to the Agreement.

(L) “Sub-Processor” means any entity or person to whom the Processor sub-contracts its responsibilities.

§ 2 Scope of application and responsibility

(1) As far as the Contract Processor performs remote support, training and diagnostics of the laboratory instruments of the Responsible Entity on behalf of the Responsible Entity, any access to the Personal Data mentioned in Attachment A cannot be excluded.

(2) If access to Personal Data occurs, Responsible Entity appoints Contract Processor as a Processor to Process the Personal Data described in Attachment A to this DPA on behalf of the Responsible Entity only for the purpose and within the scope defined there. Any data will only be handled upon instruction of the Responsible Entity. Each Party shall comply with the obligations that apply to it under Applicable Law.

(3) The Contract Processor uses Leica Biosystems Remote Service. The use of Leica Biosystems Remote Service also requires the Personal Data mentioned in Attachment A to be transferred and saved. The purpose requiring the transfer and storage is also mentioned in Attachment A.

(4) Due to this responsibility of the Responsible Entity, the Contract Processor is obliged:

a) during the term of this contract, to immediately correct, delete or block data upon instruction of the Responsible Entity, as far as this is necessary to comply with the privacy laws, and

b) after termination of the contract works, at the latest upon determination of the main contract, to delete potentially transmitted data in compliance with the Applicable Law as soon as the data are no longer required to provide any Services.

Documentation serving as evidence of the due data processing according to the order must be preserved by the Contract Processor according to the respective retention periods even beyond the end of the Contract. It can deliver them to the Responsible Entity at the end of the contract as discharge.

§ 3 Duties of the Contract Processor

(1) With respect to the data to be processed, the Contract Processor is responsible for compliance with the Applicable Law. It may only process the data required for the Agreement processing according to the instructions of the Responsible Entity. If it thinks that an instruction of the Responsible Entity violates the Applicable Law, it must immediately indicate this to the Responsible Entity.

(2) The Contract Processor designed its internal company organization in such a way that it fulfills the specific requirements of data protection. According to relevant Applicable Law, it has taken technical and organizational measures to appropriately protect the data of the Responsible Entity from misuse and loss. The measures taken by the Contract Processor are described more in detail in Attachment B. The technical and organizational measures are subject to technical progress and further development. Insofar, the Contract Processor may also realize alternative adequate measures. In doing this, the safety level of the imposed measures must not be fallen short of. Any essential changes must be documented.

(3) The Contract Processor knows that it is obliged to secrecy within this Contract. This does not apply to facts that are obvious or, by their significance, do not require any secrecy. The Contract Processor permits access to Personal Data only by employees who need to access the relevant Personal Data as reasonably necessary for the purposes of the Agreement. The Contract Processor shall ensure that the employees charged with the processing of the Responsible Entity's data treat the data to be processed according to the provisions of this Contract, treat them confidentially and have been informed about the protective provisions of the Applicable Law and the secrecy obligation and their consequences in terms of criminal justice in case of a Data Breach of the secrecy obligation.

(4) The Contract Processor shall immediately inform the Responsible Entity in case of any severe disturbances of the operative processes, in case of suspected Data Breach (also by any employees of the Contract Processor and, if applicable, commissioned subcontractors) or any other irregularities in the processing of the Responsible Entity's data. It is known that, according to Applicable Law, there can be information duties in case of a Data Breach of protection of Personal Data. Therefore, such events must immediately be notified to the Responsible Entity, irrespective of their cause. The Contract Processor must, upon consultation of the Responsible Entity, take appropriate measures to protect the data and reduce any detrimental consequences for any Concerned Persons. As far as the Responsible Entity must bear any obligations according to Applicable Law, the Contract Processor will support it appropriately in doing this. The Contract Processor is obliged to maintain a directory of the processing activity according to Applicable Law.

(5) The Contract Processor shall immediately inform the Responsible Entity on any control acts and measures of the supervisory authority according to Applicable Law. This also applies as far as a competent authority conducts any investigation at the site of the Contract Processor.

(6) Any provided data carriers as well as all copies or reproductions made thereof remain the property of the Responsible Entity. The Contract Processor must carefully preserve them excluding any third-party access. The Contract Processor is obliged to provide information to the Responsible Entity upon its request any time as far as its data and documents are concerned. As soon as the data carriers are no longer required to provide the services, at the latest upon the termination of this Contract, the Contract Processor will return any provided data carriers to the Responsible Entity. The Contract Processor will assume the deletion of Personal Data according to the Applicable Law described more in detail in Attachment A.

(7) Responsible Entity acknowledges and agrees that Contract Processor may engage its affiliates and/or third-party sub-processors in connection with the provision of the Services. Contract Processor remains fully liable to Responsible Entity for such third party and enters into a written and enforceable agreement with such third party that includes terms that are no less restrictive than the obligations applicable to Responsible Entity under this DPA. The data will be processed in European Economic Area. But in addition, the data are also transferred to the United Kingdom, Australia, India and the USA and can be inspected and stored there because system administrators there have respective access rights enabling them to inspect the data transferred by Leica Biosystems Remote Service. In these cases, the Contract Processor ensures that the appropriate level of data protection for data transmission outside of Europe by concluding EU standard contractual clauses (Implementing Decision (EU) 2021/914 of the EU Commission of June 4th, 2021 - Az. C (2021) 3972, OJ EU No. L 199/31 of June 7th, 2021) and - if necessary - the agreement of additional measures is guaranteed. Upon request, the Contract Processor shall provide the Responsible Entity with evidence of the conclusion of the aforementioned EU standard contractual clauses.

§ 4 International Transfers

(1) In case of international transfer, the Parties agree that when the transfer of Personal Data is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses, Swiss Addendum, and/or UK Addendum.

(2) Where the EU SCCs are deemed entered into and incorporated into this DPA by reference between the Parties the EU SCCs will be completed as follows:

(i) Module Two will apply to the extent that Customer is a controller of the Personal Data;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 2 will apply, and the EU SCCs will be governed by the law of the jurisdiction of establishment for the data exporter;

(vi) in Clause 18(b), disputes shall be resolved before the country courts of the data exporter;

(vii) Annex I of the EU SCCs shall be deemed completed;

(A) Part A: with the information set out in Attachment A to this DPA;

(B) Part B: with the relevant Processing description set out in Attachment A to this DPA; and

(C) Part C: in accordance with the criteria set out Clause 13 (a) of the EU SCCs;

(viii) Attachment B: with the Minimum Security Measures; and

(3). Where the UK Addendum is deemed entered into and incorporated into this DPA by reference between the Parties, the UK Addendum will be completed as follows:

a. The EU SCCs, completed as set out above in § 4.2 of this DPA, shall also apply to transfers of such Personal Data, subject to §4 3.b of this DPA below;

b. Tables 1 to 3 of the UK Addendum shall be deemed completed with the relevant infor-mation from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the Effective Date.

(4). Where the Swiss Addendum is deemed entered into and incorporated into this DPA by reference between the Parties, the Swiss Addendum will be completed as follows:

a. The EU SCCs, completed as set out above in § 4.2 of this DPA, shall also apply to trans-fers of such Personal Data, subject to §4 4.b below;

b. the Standard Contractual Clauses incorporated per reference shall protect the Personal Data of legal entities in Switzerland until the entry into force of the revised FADP.

(4). If neither § 4.2, § 4.3 nor § 4.4 of this DPA applies, then Parties shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the Applicable Law without undue delay.

§ 5 Duties of the Responsible Entity

(1) With respect to the data to be processed, the Responsible Entity is responsible for complying with the Applicable Law.

(2) The Responsible Entity must immediately and completely inform the Contract Processor if it detects any mistakes or irregularities with respect to privacy provisions in checking the processing results.

(3) The Responsible Entity is obliged to maintain the directory on the processing activity according to the Applicable Law.

(4) The Responsible Entity agrees to adhere to the principle of data minimization by ensuring that only the data which is strictly necessary for the purpose of Service provision is transferred to the Contract Processor. Where possible, the Responsible Entity shall anonymize Personal Data before transferring it to the Processor.

§ 6 Concerned Persons' inquiries to the Responsible Entity/Contract Processor

(1) If the Responsible Entity is obliged to provide information on the collection, processing or use of Personal Data of Data Subject towards that person due to any Applicable Law, the Contract Processor will support the Responsible entity in providing such information according to the Applicable Law. This requires that the Responsible Entity have prompted the Contract Processor in writing or in text form to do this. The Contract Processor will not reply to any information request and insofar refer the Data Subject to the Responsible Entity.

(2) As far as a Data Subject directly contacts the Contract Processor to have his/her data corrected or deleted, the Contract Processor will refer the Data Subject to the Responsible Entity.

§ 7 Control right

(1) The Contract Processor undertakes to provide all information required for a comprehensive order control to the Responsible Entity upon written request within an appropriate period.

(2) The Responsible Entity is entitled to convince itself before the beginning of the data processing and then regularly, however not more often than once per year, of the realization of the technical and organizational measures taken with the Contract Processor. In principle, such a control is realized by postal mail. A control on site is only admissible in exceptional cases and requires an agreement with the Contract Processor on the scope of the audit. In such case, the Responsible Entity is entitled to convince itself or any suitable commissioned third Parties bound to professional secrecy of the compliance with the technical and organizational measures upon timely notice at least four weeks in advance in the premises during usual business hours without interrupting the course of operations. The result of such controls will be respectively documented and must be signed by both Parties. The costs of such audits must be borne by the Responsible Entity.

§ 8 Subcontractors

(1) Subcontractors may be charged by the Contract Processor with the processing of Personal Data within this data processing contract only with the consent of the Responsible Entity.

(2) If any subcontractors are commissioned by the Contract Processor, the Contract Processor must conceive the contractual agreements in such a way that they correspond to the requirements on confidentiality, privacy and data safety of this Contract between the Parties. Control and examination rights according to § 7 must be granted to the Responsible Entity. Such controls/examinations shall be realized in coordination with the Contract Processor. Likewise, the Responsible Entity is entitled, upon written request, to receive information from the Contract Processor on the essential contract content and the realization of the privacy obligations of the subcontractor (Sub-Contract Processor), if necessary, also by inspecting the relevant contractual documents.

(3) Services used by the Contract Processor provided by third Parties as ancillary services to support the contract processing are not deemed subcontractor services within the meaning of this provision. This includes e.g. telecommunications services, services from logistics companies, set up of water treatment systems related to maintenance, cleaning personnel, auditors or the disposal of data carriers. However, the Contract Processor is obliged, in order to guarantee the safety and protection of the data of the Responsible Entity, to conclude appropriate lawful contractual agreements also for outsourced ancillary services and to take control measures.

§ 9 Limitation of liability & indemnity

(1) The Contract Processor is liable without limitation for any damages caused by the Contract Processor, its legal representatives or agents with gross negligence or intent. Further, the Contract Processor is liable without limitation for any damages caused by culpable injury to life, body or health.

(2) Only in case of a breach of essential contractual duties, the violation of which jeopardizes the Contract purpose and on the fulfillment of which the Responsible Entity could rely to a significant extent, the Contract Processor is also liable in cases of simple negligence. This liability is limited to the compensation for damages that were typically foreseeable at Contract conclusion. In addition, the liability for all damage events falling into the same contract year is limited to the total amount of 100% of the remuneration that the Contract Processor has acquired for the services provided in relation to this Contract Processing in the respective contract year.

(3) As far as the Responsible Entity processes Personal Data, it must guarantee that it is entitled to do that according to the applicable provisions, in particular under privacy law, and shall indemnify the Contract Processor against any third party claims in case of any breach.

§ 10 Term

(1) The term of this Contract is determined by the term of / the use of the services to be provided on the basis of the existing business relationship of the Parties with respect to the Data Processing System.

(2) A cancellation always requires the written form.

§ 11 Other

(1) If the data of the Responsible Entity are jeopardized with the Contract Processor by a seizure or confiscation, by insolvency or composition proceedings or other events or measures by third parties, the Contract Processor must immediately inform the Responsible Entity thereof. The Contract Processor will then inform all persons responsible in this context about the fact that the sovereignty over and the property of the data only lie with the Responsible Entity as the “Responsible Person” within the meaning of the Applicable Law.

(2) Changes and amendments to this Contract and all of its components – including any covenants of the Contract Processor – require a written agreement.

(3) In case of any potential contradictions, the regulations of this Contract prevail over regulations of the Agreement. If any parts of this Contract are invalid, this does not affect the validity of the remainder of the Contract.

(4) If applicable, the Standard Contractual Clauses, including Attachments A-B and § 4, shall govern and control in the event of any conflict or inconsistency between the terms of this DPA and the Standard Contractual Clauses.

(5) Attachments A and B are essential components of this DPA.

Attachment A to the Data Processing Agreement – Remote Service solution

Subject matter and duration of the assignment:	Remote Screen Access of the LBS Medical Equipment or devices' screen throughout the time that LBS Service actively supports a customer.
Nature of the processing: Scope, type, and purpose of the intended data processing:	Use of the Remote Service by LBS Service for remote troubleshooting, product maintenance and configuration and/or, to provide guidance or training to laboratory users on how to use the LBS products. Use of Remote Service by LBS service to retrieve logs and assess the problem remotely before visiting the customer site. Use of Remote Service by LBS service to gain insights on the instrument health through telemetry messages. Use of Remote Service by LBS service to deploy and install vulnerability patches or other OS critical patches remotely via screen sharing access. The BOND database may be retrieved to troubleshoot a problem observed on customer site. However, only the anonymized database would be removed, not the full database containing PHI."
Categories of Personal Data:	No PHI needs to be accessed to use this functionality; however it is possible that PHI could inadvertently be viewed. PHI (Patient name and test) and PII (doctors name, laboratory personnel name) data, may potentially show up in the User Interface during LBS Service performing a remote screen sharing on the LBS Product Screen Instrument Diagnostics Logs might be retrieved. Although these logs do not contain any PHI or PII of patients, it may contain usernames of laboratory users of the system.
Categories of Data Subjects:	Patients of the Responsible Entity may be potentially affected if the responsible entity is not using procedures to protect PHI (e.g. local lab staff supervision of remote sessions) or are not adequately trained on what

	PHI exists in the system and how to best protect PHI before authorizing the LBS service personnel to take screen share access via Remote Service.
Deletion, blocking and correction of data:	LBS Service gets full control of the LBS Products software, remotely via screen sharing as part of the troubleshooting task, however any kind of correction of configurations of the LBS Products will be performed based on the authorization from the lab in-charge.
Frequency of transfer	Personal Data will be Processed on an ad-hoc basis
Competent Authority and Applicable Law	This will be the supervisory authority of the EU member State where the exporter is established, the Information Commission if the exporter is established in the United Kingdom ("UK") or the FDPIC if the exporter is established in Switzerland. Where the exporter is not established in an EU member State, the UK or Switzerland but it is subject to EU/UK/Swiss Data Protection Law, this will be the supervisory authority in the jurisdiction where Leica Biosystems representative is established (as required under EU/UK/Swiss Data Protection Law).

Attachment B to the Data Processing Agreement

Technical and Organizational Measures (TOM)

of Leica Biosystems Remote Service solution

1. Confidentiality in accordance with Art. 32 (1) (GDPR)

Access

Measures that are suitable for denying unauthorized access to data processing equipment with which personal data is processed or used. Access control measures can include automatic access control systems, the use of chip cards and transponders, access control by porter services and alarm systems. Servers, telecommunications equipment, network technology and similar equipment must be protected in lockable server cabinets. In addition, it makes sense to support access control by means of organizational measures (e.g. official instructions that provide for the closure of the premises in the event of absence).

Technical measures	Organizational measures
Granting access to personal data only to authorized personnel	Clearly defined access control policies
Multi-factor authentication	Role based access control design
Session management controls	Staff training on data access controls.

Administrative access is restricted to appropriate personnel with elevated privileges within Leica Biosystems organization	Mandating strong login passwords for remote service software
	Regular review and update of access permissions

Authentication

Measures that are suitable to prevent data processing systems (computers) from being used by unauthorized persons. Access control refers to the unauthorized prevention of the use of equipment. Options include, for example, boot password, user ID with password for operating systems and software products used, screensavers with passwords, the use of chip cards for login, and the use of callback procedures. In addition, organizational measures may also be necessary, for example, to prevent unauthorized inspection (e.g. specifications for the installation of screens, issuance of guidance for users on how to choose a "good" password).

Technical measures	**Organizational measures**
Users of RSS application are authenticated and authorized by Azure Active Directory. No direct access to the storage location is provided.	Only authorized LBS Service personnel (employees of Leica Biosystems) are allowed to configure the LBS systems remotely via remote service features
Service login through service key and secure PIN delivered through remote service secure channels to the LBS products (14-day policy set for changing service key) establishing 2-factor authentication	Regularly review and update access permissions
Time-outs implemented to ensure logging out of remote service solution due to inactivity	
Secure HTTPS ensures secure communication between RSS and RSA	
Complex password policy and periodic renewal as an organizational practice	

Authorization

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, altered, or removed without authorization during processing, use and storage. Access control can be ensured, among other things, by suitable authorization concepts that enable differentiated control of access to data. In doing so, it is important to differentiate between the content of the data and the possible access functions to the data. Furthermore, suitable control mechanisms and responsibilities must be defined in order to document the granting and withdrawal of authorizations and to keep them up to date (e.g. in the event of recruitment, change of job, termination of the employment relationship). Particular attention must always be paid to the role and possibilities of the administrators.

Technical measures	**Organizational measures**
Files stored on the storage accounts on cloud are accessible by RSA only after a short-lived SAS token has been issued by RSS. Further, users from RSS application will be able to download the files on to the local laptop from storage account, only if they are authorized to do so.	Access to RSS application and all the associated data it collects from laboratory instruments is restricted to employees of LBS only within the service and support organisation.
All data stored in Azure storage is segregated by region, customer, and product. LBS technicians can only access specific region, customer and product based on the permissions they are assigned.	Regularly review and update access permissions
	Only LBS employees from the service and support organization who have completed product and service trainings will have capability to troubleshoot laboratory instruments through remote service features. e.g. : Remote Screen Sharing

Separation control

Measures to ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logically and physically separating the data.

Technical measures	Organizational measures
Segregation of Production, dev and test environment is maintained.	Control via authorization concept
Segmenting customer data by name, products owned and location for improved organization and access control	Data collection is restricted to what is absolute necessary for instrument diagnosis purposes only. Further, customer email and contact details are collected and maintained to reach out to them in the event of an issue/ instrument analysis.

Pseudonymisation (Art. 32 (1) (a) GDPR; Art. 25 (1) GDPR)

The processing of personal data in such a way that the data can no longer be associated with a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

Technical measures	Organizational measures
Remote Service Log Storage only contains all product logs and does not store any PII of patients or PHI.	Internal instruction to anonymize / pseudonymize personal data as far as possible in the event of disclosure
In the event of need to collect/transfer instrument's database to cloud, the instrument software will anonymise the contents of database before the transfer	Training FSEs not to look at screens that contain PHI and never remove the instrument database if it us not anonymized.
	Recommendation to Lab staff to supervise the activity when the screen is shared.

2. Integrity (Art. 32 (1) (b) GDPR)

Disclosure control

Measures to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and determine where personal data is intended to be transferred by data transmission facilities. To ensure confidentiality in electronic data transmission, encryption techniques and virtual private networks can be used, for example. Measures for the transport or transfer of data carriers include transport containers with locking devices and regulations for the destruction of data carriers in compliance with data protection regulations.

Technical measures	Organizational measures
Transport layer security using TLS1.2 between following communicating components. 1. RSA and RSS 2. RSA (AzCopy) and Azure storage account 3. BeyondTrust Jump client and BeyondTrust Virtual appliance 4. LBS Personnel laptop and RSS	Activity auditing at Instrument and RSS.
Secured protocols like HTTPs and MQTTs used for communication between Leica Biosystems instruments and Remote Service cloud	All data in storage accounts are encrypted at rest.

Input control

Measures to ensure that it is possible to subsequently verify and determine whether and by whom personal data has been entered, altered, or removed from data processing systems. Input control is achieved through logging, which can take place at different levels (e.g. operating system, network, firewall, database, application). It must also be clarified which data is logged, who has access to logs, by whom and at what occasion/time they are checked, how long retention is required and when the logs are deleted.

Technical measures	Organizational measures
	Access to personal data collected at RSS for notifying the laboratory staff is restricted to employees of LBS only within the service and support organisation.

3. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

Availability check

Measures to ensure that personal data is protected against accidental destruction or loss. This covers topics such as an uninterruptible power supply, air conditioning, fire protection, data backups, secure storage of data carriers, virus protection, raid systems, disk mirroring, etc.

Technical measures	Organizational measures
Enabling Geo-Redundant Storage on the cloud storage accounts where the logs are stored	Data collected from instruments are deleted once they are marked as not needed.
Leveraging Microsoft azure provided reliability and availability of 99.99% SLA	

4. Procedures for regular review and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 (1) GDPR)

Data Protection Management

Technical measures	Organizational measures
	Employees are GDPR trained with annual follow-up on trainings.
	The organization responds to the information and pursuant to Art. 13 and 14 GDPR
	Annual penetration testing to ensure the data protection principles in place are intact.

Incident-Response-Management

Assistance in responding to security breaches.

Technical measures	Organizational measures

Use of Azure Defender, a cloud workload protection solution in place that notifies the R&D team of Remote Service	Documented process for detecting and Security Incident Reporting / Data breach as well as post-processing of safety cases.
Use of Azure Front Door for URL routing and intelligent threat protection	