Data Processing Terms for Services

As of: 30th April 2025, version 1.0

SECTION I

Clause 1
Purpose and scope

(a) The purpose of this Data Processing Terms (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) Olympus Sverige AB, Råsundavägen 12, 2169 56 Solna Sweden, including its branches acting on its behalf, Olympus Sverige Aktiebolag filiale Latvija and Olympus Sverige Aktiebolag Lietuvos filialas (processor), and the controller agree to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex I.

(d) Annexes I to III are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2
Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 3
Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex I.

Clause 4
Obligations of the Parties

4.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

4.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I, unless it receives further instructions from the controller.

4.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex I.

4.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex II to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

4.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

4.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list in Annex III. The processor shall specifically inform the controller of any intended changes of that list through the addition or replacement of sub-processors at least four weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

4.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 4.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 5
Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 5(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

   (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex II the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 6
Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

6.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breacFh is likely to result in a high risk to the rights and freedoms of natural persons.

6.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 7
Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

DESCRIPTION OF THE PROCESSING

Processing activity: Service, Support, Consulting, Administration, Remote Maintenance

- The start of data processing is: start of the service contract
- The planned duration of data processing is: Upon termination of the service contract

The data processing background and obligations of the Parties regarding the commercial contractual relationship are specified in the **service agreement** between the Controller and the Processor.

The categories of the data subjects, the nature/purpose of processing, the data categories, and any special categories of personal data depend on the type of service provided the services to which the services relate, and the personal data stored by the customer to which Olympus has access in the course of providing the service.

Categories of data subjects	**Processing operations**	**Data categories**	**Special categories of personal data – if applicable**
☒ Patients ☒ Contact persons ☒ Employees ☒ Former employees ☒ Suppliers and their employees	☒ Operation and maintenance of IT systems and infrastructure, e.g., analytical systems ☒ Consulting on product usage ☒ IT support ☒ Technical Support ☒ Administration ☒ On-site or Olmpus repair center-based repair, testing or maintenance ☒ Remote hardware diagnostics for hardware prducts ☒ Remote service testing/maintenance for software products ☒ Provision of loan devices	☒ Account information ☒ Company ☒ Date of birth ☒ Device consent and permissions ☒ Device ID, Device name ☒ Device login data ☒ E-Mail address ☒ Gender ☒ ID (analytics, contract, device) ☒ Language ☒ Location ☒ Logs; ☒ Name ☒ Username ☒ User master data ☒ Usage data (IP-address, logging, telephone record	☒ Health data (e.g., patient name medical information)

		☒ Usage data devices, systems ☒ Image and video data	

The work on the device may require copying and analyzing the device's log file. The log file may contain patient names. First- and second-level support is provided within the EU. Third-level support is provided by a U.S.-based Olmpus entity ("Olympus Surgical Technologies America"). Therefore, if third-level support is required for trouble shooting, it may be necessary to transfer data to the United States. To ensure an adequate level of protection, Olmpus has concluded appropriate internal data processing agreements (DPAs) with its affiliated U.S. entities.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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, Processor shall implement the following technical and organisational measures:

MEASURE	DESCRIPTION
1. CONFIDENTIALITY	
a) Access control – Olympus locations	The buildings of Olympus are closed and guarded all around. Employees can enter the buildings only using their personal identification card. Visitors can only enter the buildings via the reception and accompanied by staff. Unauthorized persons are denied access to the buildings. The following security measures are implemented: - Employee/visitor badges - Access control system, card reader, transponder, magnetic or chip cards - Lobby/receptionist/doorman - (Controlled) keys/key assignment - Door lock (electric door opener, doors with outside knob, etc.) - Factory security, doorman - Surveillance system, alarm system, video/TV monitor
b) Access control – systems	All systems are installed in secure data centers and protected by personal ID cards in combination with PIN. The following security measures are implemented: - Secure password procedure (including special characters, minimum length, regular password changes) - Automatic locking mechanisms (e.g. password or pause switch, automatic desktop lock) - Instruction for manual desktop lock - Set up and management of a user profile and master record - Firewall, anti-virus software for servers and clients

	- Use of VPN for remote access - Mobile Device Policy
c) Access control - rights management: read and editing authority Olympus Internal IT systems	Systematic rights management for the use of the IT systems is in place. Access to systems is only possible with user names and passwords. The authorizations differ between reading and writing permissions. The following security measures are implemented: - Differentiated authorization concept and need to know-based access rights (profiles, roles, transactions and objects)
d) Separation control Olympus Internal IT systems	Remote maintenance is carried out separately for each customer. The following security measures are implemented: - Multi-client capability of relevant applications - Earmarking - Function separation of productive and test environment - Physical separation of systems, databases and data carriers - Definition of database rights
e) Encryption	An encryption of the communication is preferred. The encryption method is state of the art.
2. INTEGRITY	
a) Transfer control Olympus Internal IT systems	The following security measures are implemented: - Email encryption is possible in the network - No unauthorized reading, copying, modification or removal within the system - Use of VPN, as well as provision via encrypted connections such as sftp, https
b) Entry control	Changes in the systems are logged. The following security measures are implemented: - Logging of access - Log evaluation systems and traceability of input, modification and deletion of data by individual user names - Assignment of rights via personalized user accounts - Document management
3. AVAILABILITY AND RESILIENCE	

a) Availability control; data protection measures Olympus Internal IT systems	Personal data is secured. Protection against accidental or willful destruction or loss will be ensured as well as the control of the availability of the data. The following security measures are implemented: - Backup procedure: description of the rhythm and medium of the backup, storage time and location for backup (online/offline, on-site/off-site) - Mirroring hard disks, e.g. RAID procedure - Uninterruptible power supply (UPS) - Separate storage or partition for operating systems and data - Virus protection and firewall - Reporting channels and emergency plans - Fire extinguishers and alarm systems in buildings, in particular in the server room, where temperature/humidity is also monitored, and protective socket strips are installed
b) Rapid recovery	The recovery of data is the responsibility of the Controller.

4. PROCEDURES FOR REGULAR REVIEW, EVALUATION AND ASSESSMENT

a) Order control Olympus Internal IT systems	The effectiveness of the measures taken is regularly reviewed. The order control is checked on a random basis. The following security measures are implemented: - Clear contract design - Formalized order placement - Selection of the contractor under due diligence aspects (with regard to data protection and security) - Conclusion of the necessary agreement for order agreement or EU standard contract clauses - Instructions in writing or in text form to the contractor - Obligation of the contractor's employees to data secrecy - Obligation to appoint a data protection officer by the contractor if the obligation to order exists - Agreement on effective control rights vis-à-vis the contractor

	- Regulation on the use of additional subcontractors - Ensuring the destruction of data after completion of the order - Ongoing verification of the contractor and its level of protection
b) Privacy and Incident Response Management	- Central documentation of all procedures and regulations for data protection with access for employees as required/authorized - Internal Information Security and Data Protection Officer - Regular employee training and commitment to confidentiality/privacy - Documented process for recognition and reporting of security incidents / data breakdowns (also with regard to mandatory reporting to supervisory authorities) - Documented procedure for dealing with security incidents and data breaches - Formalized privacy impact assessment and process for handling information requests from data subjects

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name and Address	Contact person's name, position and contact details	Description of the processing	If applicable, safeguards for third country transfers
Olympus Europa SE & Co. KG Wendenstraße 20 20097 Hamburg Germany	Stefan Limbacher Data Protection Officer EMEA privacy@olympus.com	2nd Level Support for repair, maintenance and remote maintenance of software and medical devices	n/a, Sub-Processors is located in Hamburg, Germany
Olympus Surgical Technologies Europe **Olympus Winter & Ibe GmbH** Kuehnstraße 61 22045 Hamburg Germany	privacy@olympus.com	3rd Level Support for repair, maintenance and remote maintenance of software and medical devices	n/a, Sub-Processors is located in Hamburg, Germany
Olympus Medical Systems Corporation 2951 Ishikawa-machi, Hachioji-shi Tokyo 192-8507 Japan	privacy@olympus.com	Complaint handling including investigation for malfunction and unexpected errors.	Adequacy Decision (EU) 2019/419 by the EU Commission

Olympus Surgical Technologies America 800 W Park Dr. Westborough, MA 01581 USA	privacy@olympus.com	Complaint handling including investigation for malfunction and unexpected errors.	Standard Contractual Clauses
Tata Consultancy Services GmbH Friedrich-Ebert-Anlage 49 60308 Frankfurt am Main Germany	privacy@olympus.com	IT Infrastructure and service provider	n/a, Sub-Processors is located in Frankfurt, Germany
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen Germany	privacy@teamviewer.com	Computer monitoring and control	n/a, Sub-Processors is located in Göppingen, Germany
ImageStreamMedical One Monarch Drive Littleton, MA 01460 USA	privacy@cision.com	3rd Level Support for repair, maintenance and remote maintenance of software	Standard Contractual Clauses
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521 Ireland	privacy@microsoft.com	Various Cloud services	n/a, Sub-Processors is located in Ireland

RealVNC Limited 50-60 Station Road Cambridge Cambridgeshire CB1 2JH Vereinigtes Königreich von Großbritannien und Nordirland	privacy@realvnc.com	Provider of remote control software for SPiN Planning Laptop Workstation – No data storage, only encrypted screen sharing	Adequacy decision for the United Kingdom