DATA PROCESSING AGREEMENT TERMS AND CONDITIONS

PREAMBLE
WHEREAS, under the Services Agreement concluded between Controller and Processor ("**Services Agreement**"), Processor agreed to provide certain services to the Controller as further specified in the Services Agreement and in Annex 1 to this DPA (the "**Services**");

WHEREAS, in rendering services to Controller, Processor may from time to time be provided with, or have access to information which may qualify as Personal Data within the meaning of the Applicable Data Protection Laws;

WHEREAS, Controller engages Processor as a Processor and/or Service Provider acting on behalf of Controller as described in Applicable Data Protection Laws;

NOW, THEREFORE, and in order to enable the Parties to carry out their relationship in a manner that is compliant with applicable laws, the Parties have entered into these Data Processing Agreement Terms and Conditions as follows:

THE DATA PROCESSING AGREEMENT TERMS AND CONDITIONS (hereinafter referred to as "DPA") CONTAINED HEREIN SHALL GOVERN IN THE EVENT OF ANY CONFLICT BETWEEN THESE TERMS AND THOSE OF ANY UNDERLYING, ANCILLARY OR INCORPORATING DOCUMENT.

1. Definitions

For purposes of this DPA, the terminology and definitions as used by the GDPR shall apply. In addition:

"**Applicable Data Protection Laws**" shall mean the applicable data protection and data privacy laws, including but not limited to the **GDPR** (as defined below), other applicable European Union or Member State data protection laws and provisions, the **CCPA** (as defined below), and all other applicable data protection and data privacy laws and provisions;

"**CCPA**" means the California Consumer Privacy Act of 2018;

"**Controller**" means Intuitive Surgical or the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

"**Data Privacy Framework**" means the legal transfer mechanism adopted by the relevant authorities certifying that the United States ensures an adequate level of protection – compared to that of the European Economic Area, United Kingdom and Switzerland - for Personal Data transferred from the EU, UK and/or Switzerland to US companies participating in a Data Privacy Framework, including the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework and the Swiss-US Data Privacy Framework, and any expansion of an existing Data Privacy Framework, as well as additional or similar data privacy frameworks or similar mechanisms as adopted by the relevant authorities certifying that the law of a certain country ensures an adequate level of protection for Personal Data transferred to such country.

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

"Member State" means a country belonging to the European Union or to the European Economic Area;

"Non-Adequate Country" means a country that does not provide an adequate level of data protection in accordance with the Applicable Data Protection Laws.

"**Personal Data**" means, in any form, format, or media, any data or information (i) relating to, describing, is capable of being associated with, or could reasonably be linked to (directly or indirectly) an identified or identifiable natural person or household (or the Processing of which is otherwise regulated under the Applicable Data Protection Laws) and that is Processed by Processor and/or Service Provider in connection with its performance of the Services Agreement;

"**Processing**" (including its cognate, "**Process**") means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, including, but not limited to, use, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction;

"**Processor**" means Supplier or the entity which Processes Personal Data on Controller's behalf. Processor is also a Service Provider as defined in the CCPA;

"**Sale**" or "**Sell**" has the same meaning set forth in the CCPA;

"**Security Incident"** means any actual or reasonably suspected compromise to the availability, confidentiality or integrity of Personal Data and/or the Services, including without limitation the unauthorized or unlawful disclosure, access, acquisition, alteration, destruction, corruption, use, or other processing of Personal Data or any interference with or breach of the security or loss of systems owned or controlled by the Processor;

"**Service Agreement**" means the agreement or agreements between Controller and Processor pursuant to which Processor agreed to provide the Services to the Controller, including (but not limited to) a Purchase Order or Master Services Agreement; the terms of which shall govern except to the extent they conflict with the terms of this DPA.

"**Service Provider**" has the meaning given to in the CCPA;

"**Standard Contractual Clauses**" means the clauses approved by the relevant authorities in accordance with the Applicable Personal Data Protection Laws including, but not limited to, the European Commission standard contractual clauses ("EU/EEA SCCs"), the UK standard contractual clauses ("UK SCCs"), the Swiss standard contractual clauses ("Swiss SCCs"), the ASEAN Model Clauses for Cross-Border Data Flows, and any other executed agreement between the Parties on this subject matter or, where applicable, based on templates published by the relevant authorities, or any other standard contractual clauses under the Applicable Data Protection Laws.

"Subprocessor" means any further legal or natural person that is engaged by Processor as a sub-contractor for the performance of the Services or parts of the Services on behalf of Controller provided that such Subprocessor has access to the Personal Data exclusively for purposes of carrying out the subcontracted Services on behalf of Controller.

2. Details of the Processing

(a) The details of the Processing operations provided to Processor by Controller (e.g., the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of data subjects) are specified in Annex 1 to this DPA.

(b) The Processor shall Process Personal Data only for the purposes of performing the Services Agreement, unless otherwise required by the applicable laws to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The Processor will not retain, use, Sell, disclose or otherwise Process Personal Data for any purposes other than those consistent with this paragraph 3(b).

3. Obligations and responsibilities of Controller

The Controller is responsible for implementing appropriate technical and organizational measures to protect Personal Data under its responsibility.

4. Instructions

(a) The Processor shall Process the Personal Data only on behalf of the Controller and in accordance with the Services Agreement, this DPA and any documented instructions given by the Controller.

(b) The Controller's instructions are provided in this DPA and the Services Agreement. At any time, Controller may give specifications to such instructions as well as further instructions. Such specifications and/or further instructions shall be given generally in writing (including by email or other electronic communication), unless the urgency or other specific circumstances require another form (including verbally).

(c) The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes any Applicable Data Protection Laws or any other applicable laws ("**Challenged Instruction**"). In this case, the Processor is not obliged to follow the Challenged Instruction, unless and until the Controller has confirmed or changed it.

5. Obligations of Processor

(a) The Processor shall ensure that persons authorized to Process Personal Data on behalf of the Controller, in particular the Processor's employees and other workforce members as well as employees or other workforce members of any Subprocessors, have committed to confidentiality or are under an appropriate statutory obligation of confidentiality, and that such persons shall Process Personal Data in compliance with the Controller's instructions, this DPA and the Applicable Data Protection Laws.

(b) The Processor shall implement appropriate technical and organizational measures including but not limited to those specified in Annex 2 before Processing the Personal Data on behalf of the Controller notably to ensure the security, integrity and confidentiality of the Personal Data. The Processor may amend the technical and organizational measures from time to time provided that the amended technical and organizational measures are at least as protective as those set out in Annex 2. Substantial and material amendments to the technical and organizational measures that are not at least as protective as those agreed upon in Annex 2 shall be agreed upon in writing between the Parties prior to their implementation. The Processor shall document changes to the technical and organizational measures and provide the Controller with such documentation within thirty (30) days of implementing such measures.

(c) The Processor shall allow for and contribute to audits and inspections as required by data protection authorities, in connection with a Security Incident or as needed by Controller in accordance with Applicable Data Protection Laws. The Processor shall make available to the Controller any information and documents necessary to demonstrate compliance with (i) the obligations of Processor laid down in this DPA, (ii) the obligations under Art. 28 of the GDPR (or any equivalent obligation under the Applicable Data Protection Laws), (iii) other Applicable Data Protection Laws, and as required for Controller to demonstrate its compliance with the Applicable Data Protection Laws.

(d) The Processor shall notify the Controller in writing via data.privacy@intusurg.com without undue delay and in no event later than three (3) business days of any complaint and/or request received from a data subject (e.g., regarding access, rectification, erasure, restriction of Processing, data portability, objection to Processing of data, automated decision-making), and provide all relevant details, including a copy of the complaint or request, without responding to that complaint and/or request unless the Processor has been otherwise authorized in writing by the Controller to do so and to the extent permissible under the Applicable Data Protection Laws. The Processor shall provide any necessary assistance that the Controller may require to respond to such complaint and/or request in a timely manner so as to allow the Controller to meet its legal and regulatory obligations.

(e) In the event of any Security Incident, the Processor shall, at its sole cost and expense: (i) without undue delay (and in no event later than twenty-four (24) hours after becoming aware of the Security Incident) notify Controller in writing viadata.privacy@intusurg.com; (ii) promptly undertake an investigation of the Security Incident and cooperate with Controller in connection with its investigation, including by preserving and making available to the Controller all relevant records, logs, files, or other relevant materials and regular updates; and (iii) as directed by Controller, promptly undertake appropriate remediation measures, including, without limitation, development and delivery of notices to data protection authorities and/or individuals, credit monitoring and any other measures required by applicable law or otherwise commensurate with the nature of the Security Incident. The Processor shall promptly reimburse Controller for all costs and expenses (including legal fees) reasonably incurred by the Controller in connection with a Security Incident caused by or within the control of the Processor, including any act or omission by Processor. The Processor shall not publicize or deliver any notices referencing a Security Incident (including notices to data protection authorities and/or individuals) in a manner that identifies the Controller without prior written approval from the Controller.

(f) The Processor shall assist the Controller with its obligation to carry out a data protection impact assessment as may be required (e.g., by Art. 35 of the GDPR, or any equivalent obligation under the Applicable Data Protection Laws). The Processor shall assist the Controller in case of a consultation with the supervisory authority as may be required(e.g., by Art. 36 of the GDPR or any equivalent under the Applicable Data Protection Laws), that relates to the Services provided by the Processor to the Controller under the Services Agreement by means of providing the necessary and available information and documents to the Controller.

(g) Upon request of the Controller and upon termination or expiration of the Services Agreement, the Processor shall, at the choice of the Controller, (i) delete or return to the Controller all the Personal Data which is Processed by the Processor on behalf of the Controller under this DPA, and (ii) shall cease Processing the Personal Data, and (iii) shall delete any existing copies of the Personal Data within thirty (30) days of the Controller's request or termination of the Services Agreement, unless the applicable laws require the Processor to retain such Personal Data, in which case the Processor shall continue to protect such Personal Data in accordance with the terms of this DPA and the Applicable Data Protection Laws until such time that it can reasonably return or securely delete such Personal

Data. Upon deletion, the Processor shall provide the Controller with a written attestation that all Personal Data have been deleted by the Processor and its Subprocessors.

(h) The Processor shall provide to the Controller the respective records of processing activities according to Art. 30 (2) of the GDPR (or equivalent obligation under the Applicable Data Protection Laws) relating to the Services, to the extent necessary for the Controller to comply with its obligation to maintain records of Processing activities.

(i) If the Processor designates a data protection officer and/or a representative under the Applicable Data Protection Laws, the Processor shall provide such contact details to the Controller. Processor shall inform Controller in writing of Processor's Data Protection Officer's name and contact details.

(j) The Processor shall notify the Controller immediately if the Processor makes a determination that the Processor or its Subprocessors can no longer comply with this DPA or the Applicable Data Protection Laws. In this case, the Processor shall cease Processing or take other reasonable or appropriate steps to remediate.

(k) Processor agrees that Personal Data transferred under this DPA is transferred only for the purpose of performing the Services specified in the Services Agreement and is not transferred independently for valuable consideration as defined in the CCPA.

(l) Processor shall not (i) Process Personal Data for its own purposes (including in de-identified, pseudonymized, or anonymized form); (ii) attempt to link, identify, or otherwise create a relationship between Personal Data and information that is not Personal Data or any other data, or re-identify any anonymous or de-identified data without the express authorization of Controller; or (iii) Sell Personal Data.

(m) Where the Processor is required by law or a valid request from a government or any authority under the applicable law to Process or disclose Personal Data, the Processor shall (i) promptly inform Controller of such request; and (ii) use its best efforts to limit the nature and scope of the required Processing and disclosures; and (iii) shall only Process or disclose the minimum amount of Personal Data necessary. Moreover, Processor shall challenge any such request that is overbroad, excessive, inappropriate, or inapplicable.

(n) Any limitations and exclusions of liability in the Services Agreement shall not apply if the Processor breaches the Applicable Data Protection Laws, this DPA, or any other provisions regarding data privacy between the Parties. In particular, the Processor shall be fully liable for and shall indemnify Controller for any damages in connection with Processor's failure to comply with its obligations under the Applicable Data Protection Laws, this DPA, or any other data protection provisions between the Parties, or where Processor has acted outside or contrary to lawful instructions of the Controller. For the avoidance of doubt, the Processor's liability for damages and indemnification also applies in case of any acts or omissions by third parties or persons within the Processor's control or acting under the instructions of the Processor.

6. Data subject rights

(a) The Controller is primarily responsible for handling and responding to complaints and requests made by data subjects.

(b) The Processor shall assist the Controller with any appropriate and possible technical and organizational measures to respond to complaints and requests for exercising the data subjects' rights required by Applicable Data Protection Laws.

7. Subprocessing

(a) The Processor shall not subcontract any Processing of Personal Data without the Controller's prior specific written authorization. The Processor shall submit the request for specific authorization least thirty (30) calendar days prior to the engagement of the Subprocessor, together with information necessary to enable the Controller to make a decision on the request for authorization.

(b) The Processor shall enter into a written contract with the Subprocessor (the "**Subprocessing Agreement**") and such Subprocessing Agreement shall (i) impose upon the Subprocessor obligations at least as restrictive as imposed by this DPA upon the Processor, to the extent applicable to the subcontracted Services, (ii) describe the subcontracted Services, and (iii) describe the technical and organizational measures the Subprocessor has to implement pursuant to Annex 2, as applicable to the subcontracted Services. The Controller has the right to request a copy of the Subprocessing Agreement. The Processor shall ensure that all Subprocessors implement and maintain measures at least as restrictive as those listed in Annex 2.

(c) The Processor shall inform the Controller of any intended changes concerning the addition or replacement of a Subprocessor by providing the Controller prior written notice of at least thirty (30) calendar days before the intended addition or replacement. This notification shall clearly indicate the subcontracted Services, and the identity, contact details and location of the Subprocessor. Controller may reasonably and in a duly substantiated manner object to the use of a Subprocessor within fourteen (14) business days after receipt of notice.

(d) Where the Subprocessor fails to fulfil its Personal Data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the Subprocessor's obligations.

8. Data Transfer Requirements

(a) Where the Personal Data originating from a country requiring an adequate level of protection for Personal Data is transferred outside the country of origin, the Processor shall not transfer the Personal Data outside the country of origin without the prior written authorization of the Controller. When applicable, the Processor shall ensure that appropriate legal and/or contractual safeguards are in place for such authorized transfers as required by the Applicable Data Protection Laws. The Processor warrants that its Subprocessors are bound by obligations for Personal Data transfers at least as restrictive as those set forth in this DPA. Upon the Controller's request, the Processor shall provide documents evidencing such legal and contractual safeguards, and such safeguards shall become an integral part of this DPA.

(b) When the performance of the Services Agreement involves Personal Data transfers to a Non-Adequate Country as between the Parties, the Parties shall ensure that appropriate legal and/or contractual safeguards are in place for such transfers as required by the Applicable Data Protection Laws, such as Standard Contractual Clauses including but not limited to those set forth in Annexes of this DPA.

(c) Intuitive Surgical, Inc. and Intuitive Surgical Operations, Inc. (completed with other Intuitive US entities certified under the Data Privacy Framework, if applicable) are certified under the Data Privacy Framework. Where applicable, Personal Data transfers by Controller are covered by the Data Privacy Framework. In case the Data Privacy Framework does not apply or no longer applies for any reason whatsoever, the Standard Contractual Clauses, attached in Annex 3 of this DPA, shall apply, and, where the Data Privacy Framework no longer applies, shall automatically and retroactively replace the Data Privacy Framework for covering the Personal Data transfers as required by the Applicable Data Protection Laws.

9. Term and termination

The term of this DPA is identical with the term of the Services Agreement. Except as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Services Agreement, unless otherwise stated herein.

10. Miscellaneous

(a) The Parties shall comply with the Applicable Data Protection Laws.

(b) If and to the extent necessary to comply with mandatory provisions under the applicable laws regarding the performance of the Services Agreements, the Controller may require any necessary changes (including amendments) to the provisions of the Service Agreement, this DPA or its annexes. If the Controller and the Processor are not able to agree upon changes required to meet mandatory legal requirements within thirty (30) days of the Processor's receiving written notice of the mandatory changes, the Controller shall have the right to terminate this DPA and the associated Services Agreement with thirty (30) days' notice in writing.

(c) In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' Personal Data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' Personal Data protection obligations, this DPA shall prevail. In case of inconsistencies between this DPA, any Standard Contractual Clauses or any applicable Personal Data transfer mechanisms, where applicable, the latter shall prevail.

(d) Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, should this not be possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omission.

(e) If the Services Agreement does not designate an EU Member State law as governing this DPA and an EU Member State court as having exclusive jurisdiction to resolve any dispute arising out of or in connection with the Services Agreement, the Parties agree that French law shall apply to this DPA, and the courts of France shall have exclusive jurisdiction over any dispute arising out of or in connection with this DPA.

ANNEX 1
Details of Processing

Nature and purpose of the Processing
The Personal Data transferred may be subject to the following basic processing activities: 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 of Personal Data.

The purpose of the Processing is for the Processor to provide the Services to the Controller under the Services Agreement.

Categories of Data Subjects
The Personal Data Processed may concern the following categories of data subjects:

- Past, present and prospective employees and contingent workers.
- Past, present and prospective end users, website visitors, and customers, including but not limited to surgeons and healthcare professionals, participants in the operating room during the procedure.
- Past, present and prospective advisors, consultants, suppliers, contractors, subcontractors and agents.
- Beneficiaries and relatives.
- Patients of past, present, and prospective customers.

Categories of Personal Data
The Personal Data Processed by Processor on behalf of Controller may concern the following categories of Personal Data:

- Identification and contact details (e.g., name, gender, nationality, date and location of birth, e-mail address, work or home address, phone and fax number, social media related data (e.g., profile, photo/background photo and address)
- Professional or employment data (e.g., company /employer name, affiliation, job title, grade, professional identification number/title/role and photo, ID/passport/driver's license, education (e.g., academic titles/ certifications), professional experience (e.g., career caseload in open/minimally invasive/robotic surgery)
- IT systems related data (e.g., user ID and password, profile photo or background photo, device identification data, computer or domain name, IP address and cookies)
- Controller's system-related technical data (e.g., log in and log out time, use of instruments)Data subject's email content and data relating to the sending, routing and delivery of emails
- Services, benefits or goods provided to or for the benefit of data subjects
- Financial data (e.g., credit, payment/salary/benefits/pension/insurance plan, and bank account details).
- Location data (e.g., demographic or geo-location data)
- Video and audio data

Special Categories of Personal Data (if appropriate)
The Personal Data transferred may include information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union opinions, memberships or activities, social security files, and data concerning health (including physical or mental health or condition), sexual life

and information regarding criminal offences or alleged offences and any related court proceedings and shall include special categories of data as defined in the GDPR.
When applicable, health data may include patient data including health status (e.g., physical status classification), BMI and diagnosis (e.g., medical diagnosis, characteristics affiliated with this diagnosis), pre-operative radiological imaging, surgery details (e.g, intraoperative and postoperative complications), histology report, procedure related data (type, date and time, location, duration, etc.) and follow-up data (e.g., readmission, re-operation, return to work etc.).

Processor will notify Controller in writing to the extent Processor needs to collect additional sensitive data beyond those listed above in order to provide the Services.

ANNEX 2
Description of the Technical and Organizational Measures (TOMs) implemented by Processor in accordance with Applicable Data Protection Laws:

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 data subjects (as defined under Applicable Data Protection Laws), the Processor shall implement the following technical and organizational measures to ensure a level of security appropriate to the risks for the rights and freedoms of data subjects. In assessing the appropriate level of security, the Controller and the Processor took account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction loss, alteration, unauthorized disclosure of, or access to Personal Data (also, Intuitive Data) transmitted, stored or otherwise processed.

This description of TOMs does not limit other obligations of the Processor, including under the Service Agreement or the DPA or any applicable laws. To the extent this description conflicts with the Service Agreement and or the DPA, Processor shall promptly notify Controller of this conflict and shall comply with the requirement that is more restrictive.

1. Encryption

Processor shall use strong and effective encryption to protect transmitted records and files containing Intuitive Data that will travel across networks, with encryption at a strength that is commercially reasonable given the nature of the data transmitted and the transmission method (including strong encryption for stored passwords and sensitive data). In particular, Processor shall use appropriate encryption controls such as such as TLS 1.2 or greater for transmission of Intuitive Data that is considered Confidential Information. Processor must use latest industry standard of encryption such as AES 256 bit or hashing standards for storage of Intuitive Data that is considered Confidential Information.

2. Confidentiality of the processing systems and of the services

Processor shall ensure that effective measures are implemented to address the confidentiality of the processing systems and of the services and in particular that any Processor personnel authorized by Processor to process Intuitive Data is subject to an obligation of strict confidentiality and will also be required to agree to confidentiality obligations. Furthermore, Processor will, at the minimum, prevent data processing systems from being used without authorization, ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that Intuitive Data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage; ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged; ensure that data collected for different purposes can be processed separately.

For the above purposes, Processor shall ensure that the system (Network, Hosting and Application) is designed in compliance with the least privilege principle; shall ensure that the separation of duty

principle is rigorously applied; shall enforce the use of strong passwords for all systems (Network, Hosting, and Application). Processor shall ensure that credentials are never sent in clear text format; shall ensure that access to the system (Network, Hosting and Application) is logged and access to the log file is restricted. Also, for administrative accounts, Processor shall use a multi-factor authentication.

3. Integrity of the processing systems and of the services

Processor shall make sure that effective measures are implemented to address the integrity of the processing systems and of the services so as to ensure that Intuitive Data may not be unmodified and to ensure that it is possible to check and establish whether and by whom Intuitive Data have been input into data processing systems, modified or removed, and also to ensure protection by technical and organizational means regarding authorizations, protocols/logs including analyzing protocols, audits.]

In particular, Processor must, at the minimum, implement operating system hardening for hosts/infrastructure handling Controller's products and/or data. Operating system hardening includes, but is not limited to, the following configurations and practices: strong password authentication, inactivity time-out, turning off unused ports/services, implement log management and disabling or removal of unnecessary or expired accounts, timely patching and updates to system software. In addition, Processor must implement strong access control and restrict access to operating system configurations to privileged users for hosts/infrastructure handling Controller's products or data.

Processor must have a documented patch management program and regularly perform patch management on all systems that host or handle Intuitive Data. Processor must implement critical patches within processor recommended timeframes on all systems that hosts or handles Intuitive Data, not to exceed 30 days. Processor must implement specific controls to track and verify activities of users with elevated privileges to systems that host or handle Intuitive Data, including, but not limited to maintaining log files, separation of duties, cameras, etc. Processor must, at a minimum do quarterly assessment of system-level vulnerabilities and remediate critical vulnerabilities within 30 days.

3.1. Entrance control:

Processor must make sure that unauthorised persons are denied the access to facilities in which personal data is being processed. Notwithstanding any of the foregoing, Processor, must adopt appropriate physical, technical, and organizational security measures in accordance with industry standards, including but not limited to building access control, employee security awareness education, etc.

3.2. Personal data carrier control:

Processor must make sure that unauthorised persons are prevented from reading, copying, altering or removing data carriers. In particular, Processor shall enforce the use of strong passwords for all systems (Network, Hosting, and Application). Processor shall ensure that credentials are never sent in clear text format. Processor shall also ensure that access to the system (Network, Hosting and Application) is logged and access to the log file is restricted. For administrative accounts, Processor shall use a multi-factor authentication.

3.3. Transport control:

Processor shall implement appropriate measures so as the disclosure of Intuitive Data as well as during the transport of data carriers, the unauthorised reading, copying, alteration or deletion of data must be prevented. In particular and regarding Network-Level Requirements:

a. Processor must use firewall(s) to protect hosts/infrastructure handling Controller's products, proprietary information, or data. The firewall(s) must be able to effectively perform the following functions: stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing. Processor may use NIST SP800-41 provided guidelines for handling firewall(s).

b. Processor must have network-based security monitoring for the segment(s) on which hosts handling Intuitive Data are logically located.

c. Processor must assess network-level vulnerabilities through penetration testing and a vulnerability assessment conducted by a third-party/independent group and remediate critical vulnerabilities within 30 days. This third-party/independent group assessment must be conducted, at a minimum, annually or after significant changes have been made to network architecture. Processor shall employ ongoing, active network scanning to assess potential vulnerabilities, and shall remediate those vulnerabilities within a reasonable time, not to exceed 30 days.

d. If Processor is receiving remote access to Controller's systems, Processor will abide by Controller's 3rd Party Connectivity Standard.

3.4. Disclosure control:

Processor must make sure that data recipients to whom Intuitive Data is disclosed by means of devices for data transmission must be identifiable.

3.5. Storage control:

Processor shall, at the minimum, ensure that unauthorised storage in the memory as well as the unauthorised knowledge, alteration or deletion of stored personal data is prevented.

3.6. Usage control:

Processor shall, at the minimum, ensure that the use by unauthorised persons of automated data processing systems by means of devices for data transmission must be prevented.

3.7. Access control:

Processor shall ensure that the access by authorized persons is limited to Intuitive Data that absolutely required for the fulfilment of its tasks. Furthermore, Processor shall ensure that the system (Network, Hosting and Application) is designed in compliance with the least privilege principle. Processor shall also ensure that the separation of duty principle is rigorously applied.

3.8. Input control:

Processor shall ensure that when automated systems are used, it is possible to carry out a retrospective examination of what Intuitive Data was entered at what time and by which person; data files must be structured so that the data subjects are able to assert their right of access and their right to have data corrected.

4. Availability of the processing systems and of the services

Processor shall ensure that effective measures are implemented to address the availability of the processing systems and of the services e.g., measures that ensure that Personal Data is available in a permanent and unlimited way and is available if needed, such as measures to ensure that Personal Data is protected from accidental destruction or loss; ensure that, in the case of commissioned processing of Personal Data, the data is processed strictly in accordance with the instructions of the principal.

5. Resiliency of the processing systems and of the services

Processor shall ensure that effective measures are implemented to address the resiliency of the processing systems and of the services and in particular measures that ensure systems and services are designed in a way that they can handle punctual or constant high load of processing operations; this is especially related to storage, access and performance capacity.

6. Ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident

Processor shall ensure that effective measures are implemented to address the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident: Such measures shall, at the minimum, include a backup concept, a redundant data storage, cloud services, fall back IT infrastructure, mirror data centers.

In addition, and related to Data Breach and Security Incident Notification Requirements:

Processor must notify Controller immediately within the timeframe stated in the Agreement or the DPA, if a Data Breach or Security Incident occurs involving confidential Intuitive Data including any Personal Data transferred from or associated with the Controller. If no specific timeframe is stated in the Agreement or DPA, Processor must notify Controller within 24 hours upon becoming aware of a Data Breach or Security Incident.

Processor must work with the Controller promptly and in good faith as required to resolve the Data Breach or Security Incident, and in conjunction with any associated investigations in accordance with Processor's obligations as stated in the Agreement and/or DPA, and applicable laws.

7. Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures

Processor shall make sure effective measures are implemented to address the regularly testing, assessing and evaluating of the effectiveness of technical and organizational measures e.g., security concept, review by the data protection officer, external reviews, audits, certifications.

In particular - Third Party Review or Assessment, Processor shall provide, maintain and renew an independent, third-party assessment, audit or review which attests to the effectiveness of controls related to the requirements defined below. Processor shall provide to Controller the applicable

certification, third party assessment, audit or review, to be conducted at Processor's expense, within 90 days of the proposed solution in place and annually thereafter within 90 days of the expiration of the applicable certification or third-party assessment, audit or review.

For the purposes of this section, Controller will accept any of the following Third-party assessments; Acceptable Options	**Description**
ISO 27001	**International Standards Organization (ISO) Cybersecurity Framework https://www.iso.org/isoiec-27001-information-security.html**
SOC1 Type 2	**Systems and Organization Controls (SOC) 1 Type 2: Applies to Financial Organizations https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement**
SOC2 Type 2	**Systems and Organization Controls (SOC) 2 Type 2: Applies to Service Organizations https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement**
HiTrust CSF	**HiTrust Cybersecurity Framework https://hitrustalliance.net/**
CMMC 2.0 Level 2	**Cybersecurity Maturity Model Certification (CMMC) Aligned with NIST SP 800-171 https://www.acq.osd.mil/cmmc/about-us.html https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final**
CMMC 2.0 Level 3	**Cybersecurity Maturity Model Certification (CMMC) Aligned with NIST SP 800-172 https://www.acq.osd.mil/cmmc/about-us.html https://csrc.nist.gov/publications/detail/sp/800-172/final**
FISMA	**Federal Information Security Modernization Act (FISMA) Aligned with NIST SP 800-53 https://csrc.nist.gov/projects/risk-management/fisma-background**

8. System Administrators

Processor shall ensure that, at the minimum, the following specific arrangements are adopted with regard to system administrators:

All-Level Requirements:

a. Processor shall ensure that the system (Network, Hosting and Application) is designed in compliance with the least privilege principle.

b. Processor shall ensure that the separation of duty principle is rigorously applied.

c. Processor shall enforce the use of strong passwords for all systems (Network, Hosting, and Application). Processor shall ensure that credentials are never sent in clear text format.

d. Processor shall ensure that access to the system (Network, Hosting and Application) is logged and access to the log file is restricted.

e. For administrative accounts, Processor shall use a multi-factor authentication.

f. In case Processor requires access to Controller networks or systems or applications, then Processor should notify Controller of status changes such as terminations, etc. effective immediately.

g. Processor shall that ensure that an established strict policy against phishing (which included policy for passwords, internet usage and personal devices) and frequent awareness-raising campaigns for employees are implemented.

Furthermore, Processor shall take appropriate measures to ensure:

Individual appointment of system administrators with detailed description of scope of activities are allowed to be carried out based on relevant authorization profile; An updated list of system administrators with identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request is maintained; Outsourcing: If system administration services are outsourced necessary to keep the information required to identify the system administrators and their duties and obligations as per the Regulation; Regular Checks: yearly audit of system administrators' activity to assess compliance with assigned tasks, instructions received by Processor and applicable laws; Access Logging: adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for at least six months.

Annex 2*bis*

Applicable only if the Processor processes Personal Data of data subjects located in Israel, in addition to the Technical and Organizational measures in Annex 2 above, the Processor shall implement the following measures:

1. For the purpose of this Annex 2*bis*, the following definitions shall apply :
    a. "**Database**" – a collection of Personal Data held by magnetic or optical means intended for computerized processing, except for: a collection of Personal Data that is designated for personal, non-commercial use; and collection of Personal Data that only includes names, addresses, and the communication method, which in itself does not create a characterisation that violates the privacy of the individuals whose names are included therein, provided that the Controller of the such collection or any entity under its control does not have another collection.
    b. "**Database Systems**" – information systems (including but not limited to, software, interfaces, infrastructure, hardware components and communications components) that the Processor operates servicing the Database which have a significance in terms of information security.
    c. "**Authorized Individuals**" – individuals who were granted access to Personal Data by the Processor, for the purpose of performing the Processor's obligations under the Services Agreement and this DPA.

2. The Processor shall develop, implement and enforce an information security policy and procedures that shall include at least the following ("**Information Security Policy**") :
    a. instructions regarding the physical and environmental security measures taken by the Processor regarding the Database Systems containing Personal Data;
    b. Instructions regarding the manner in which access to the Database Systems is managed and the means of controlling access to Personal Data and the actions taken in it;
    c. Guidelines for Authorized Individuals to access Personal Data and Database Systems;
    d. A review of the risks to which the Personal Data is exposed to as part of the Processor's ongoing activities;
    e. Instructions regarding the means of recording, monitoring and identifying threats to which the Database Systems are exposed, and events in which there is a risk of breach of information security;
    f. Instructions regarding periodic audits as stated in sections 11 and 12 below;
    g. Instructions regarding the manner in which the Processor shall handle Security Incidents;
    h. Instructions and procedures regarding periodical backup and restoration and the documentation of monitoring the access to the Database Systems as stated in section 12(b) below;
    i. Instructions regarding the manner in which development activities in the Database Systems are performed and documented, including access by development personnel to the Personal Data.

The Processor shall review the need to update the Information Security Policy on a yearly basis, including when substantial changes to the Database Systems or processing operations are performed or new technological risks in relation to the Database Systems are revealed.

3. The Processor shall prepare an inventory list that includes all components of the Database Systems. The Processor shall update the list from time to time and shall only disclose the document to individuals who require access to it for the performance of their job functions.

4. The Processor shall manage access rights to Personal Data, including providing its Authorized Individuals with 'Least Privileges' based on their 'Need to Know', for the purpose of carrying out their tasks, and shall take measures in order to prevent access by unauthorized individuals to Personal Data. In addition, the Processor must maintain an up-to-date listing of all Authorized Individuals and prevent the access of any individual who is not required to access the Personal Data.

5. The Processor shall implement security and monitoring measures through which the Processor shall record each access made to the Database Systems.

6. The Processor shall maintain logical separation between the Database Systems and the computer systems used by the Processor that are not directly related to the Processing of Personal Data on behalf of the Controller. In the event of connection of the Database Systems to the Internet or to another public network, the Processor shall install appropriate means of protection against Security Incidents.

7. The Processor undertakes to enable authentication of Authorized Individuals to the Database Systems only by a physical means subject to their exclusive control in addition to a password-based identification measure.

8. To the extent possible, the Processor shall prevent connection of portable devices to the Database Systems.

9. The Processor shall regularly update the Database Systems, including the software installed in the Database Systems, with information security updates. In operating the Database Systems, the Processor shall not use any software or hardware components whose manufacturer does not support their security aspects.

10. The Processor shall monitor and document the activity carried out in sites which the Database Systems are located, including (but not limited to) documentation of attempts to access the sites as well as the setting and removing of equipment in and from the sites.

11. The Processor shall monitor and document, by an automated mechanism, access attempts to the Database Systems ("**Audit Mechanism**"). The Audit Mechanism shall collect at least the following data: the user identity, the date and time of the attempted access, the component of the system which was accessed, the type and scope of access, and whether or not access was successful.
    a. The log data generated by the Audit Mechanism shall be maintained for 24 months.

b. Processor shall backup all data generated by the Audit Mechanisms.
c. Processor will provide the Controller with the documentation from the Audit Mechanisms upon request.

12. Processor shall conduct, at least once in 24 months, an internal or external audit by an entity or a person with appropriate certification for auditing information security (who is not Processor's CISO), in order to ascertain the Processor's compliance with these provisions and the provisions of the Applicable Data Protection Laws.

13. If the Processor processes Personal Data of Israeli data subjects, the Processor shall not grant access to such Personal Data to Authorized Individuals, prior to: (i) reasonably confirming, as customary in candidate screening processes, that their background and reliability do not impose a concern on granting them access to Personal Data; (ii)); and (iii) training them on privacy protection and information security obligations applicable to Processor by virtue of the this DPA. Such training shall take place at least once every two years and as soon as possible after recruiting.

ANNEX 3
Standard Contractual Clauses

Depending on the jurisdictions of the Parties and the personal data transfers between the Parties under the Services Agreement, "Module 2 (Controller to Processor)" and/or "Module 4 (Processor to Controller)" of the 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 are fully incorporated in this DPA by reference, being specified that:

Optional Clause 7 (Docking clause) is included in Modules 2 and 4 as follows:

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

(…)

General Written Authorization of Clause 9 (Use of sub-processors) is included in Module 2 The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least thirty (30) calendar days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(…)

The optional provisions of Clause 11 (a) (Redress) are not included in Modules 2 and 4.

(…)

The optional provisions of Clause 13 (a) (Supervision) are included in Module 2 as follows:

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having

to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(…)

Option 1 of Clause 17 (Governing law) is included in Module 2 and completed as follows:

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 17 (Governing law) in Module 4 is completed as follows:

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18 (b) (Choice of forum and jurisdiction) in Module 2 is completed as follows:

(b) The Parties agree that those shall be the courts of France.

Clause 18 (Choice of forum and jurisdiction) in Module 4 is completed as follows:

Any dispute arising from these Clauses shall be resolved by the competent courts of France.

Only when the Processor also acts as sub-processor of the Controller (e.g. where the Controller itself is acting as a processor of its own customers) when performing part or all Services, "Module 3 (Processor to Processor)" of the 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 is fully incorporated in this DPA by reference, being specified that:

Optional Clause 7 (Docking clause) is included in Module 3 as follows:

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

(…)

General Written Authorisation Clause 9 (Use of sub-processors) is included in Module 2 as follows:

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least at least thirty (30) calendar days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-

processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(…)

The optional provisions of Clause 11 (a) (Redress) are not included in Module 3.

(…)

The optional provisions of Clause 13 (a) (Supervision) are included in Module 3 as follows:

(a) [Where the data exporter is established in an EU Member State]: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679]: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679]: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(…)

Option 1 of Clause 17 (Governing law) is included in Module 3 and completed as follows:

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 17 (Governing law) in Module 3 is completed as follows:

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18 (b) (Choice of forum and jurisdiction) in Module 3 is completed as follows:

(b) The Parties agree that those shall be the courts of France.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Intuitive Surgical Operations, Inc.

Located at 1020 Kifer Road, Sunnyvale CA 94086, USA

Contact person's name, position and contact details:

Wendi Wright, Data Privacy Officer, Intuitive Surgical Operations, Inc., 1020 Kifer Road, Sunnyvale CA 94086, USA

Activities relevant to the data transferred under these Clauses: See Annex 1 of the Data Processing Agreement.

Signature and date: [*Please complete.*]

Role (controller/processor): Controller

2. Intuitive Surgical Sàrl

Located at 1 chemin des Mûriers, 1170 Aubonne, Switzerland

Contact person's name, position and contact details:

Juha Viikki, Data Privacy Officer, Intuitive Surgical Sàrl, Chemin des Mûriers 1, 1077 Aubonne, Switzerland

Activities relevant to the data transferred under these Clauses: See Annex 1 of the Data Processing Agreement.

Signature and date: [*Please complete.*]

Role (controller/processor): Controller

3. Intuitive Surgical Deutschland GmbH

Located at Am Flughafen 6, 79108 Freiburg, Germany

Contact person's name, position and contact details:

Juha Viikki, Data Privacy Officer, Intuitive Surgical Sàrl, Chemin des Mûriers 1, 1077 Aubonne, Switzerland

Activities relevant to the data transferred under these Clauses: See Annex 1 of the Data Processing Agreement.

Signature and date: [*Please complete.*]

Role (controller/processor): Controller

4. Intuitive Surgical Ltd

Located at The Schrodinger Building, Oxford Science Park, Heatley Rd, Oxford OX4 4GE, United Kingdom

Contact person's name, position and contact details:

Juha Viikki, Data Privacy Officer, Intuitive Surgical Sàrl, Chemin des Mûriers 1, 1077 Aubonne, Switzerland

Activities relevant to the data transferred under these Clauses: See Annex 1 of the Data Processing Agreement.

Signature and date: [*Please complete.*]

Role (controller/processor): Controller

5. Intuitive Surgical SAS

Located at Cité de la Photonique, bâtiment Gienah, 11 avenue de Canteranne, 33600 Pessac, France

Contact person's name, position and contact details:

Juha Viikki, Data Privacy Officer, Intuitive Surgical Sàrl, Chemin des Mûriers 1, 1077 Aubonne, Switzerland

Activities relevant to the data transferred under these Clauses: See Annex 1 of the Data Processing Agreement.

Signature and date: [*Please complete.*]

Role (controller/processor): Controller

Data importer(s):

Name and Address: All entities listed in the Services Agreement

Contact person's name, position and contact details: As above

Activities relevant to the data transferred under these Clauses: Performance of the Services Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Annex 1.

Categories of personal data transferred

See Annex 1.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See Annex 1 (as applicable).

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis depending on the use of the Services by the Controller.

Nature of the processing

See Annex 1.

Purpose(s) of the data transfer and further processing

See Annex 1.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The period for which Personal Data will be retained will be the same as the duration of the Services Agreement, except as otherwise agreed in writing by the Parties or required by law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Processor will notify Controller in writing regarding the (sub-) processors that Controller is asked to authorize.

C. COMPETENT SUPERVISORY AUTHORITY

The French Data Protection Authority, i.e. *Commission nationale de l'informatique et des libertés (CNIL), France*

ANNEX II

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

See Annex 2.

ANNEX IV

APPLICATION OF THE STANDARD CONTRACTUAL CLAUSES TO COMPLY WITH SWISS LEGISLATION

Where a transfer of Personal Data from a Data Exporter to a Data Importer is subject to the FADP, this ANNEX IV will apply:

In order for the Standard Contractual Clauses to comply with Swiss legislation and thus be suitable for ensuring an adequate level of protection for transfers of Personal Data from Switzerland to a third country in accordance with Article Art. 16 paragraph 2 letter d of the Swiss Federal Act on Data Protection dated 25 September 2020 ("FADP, 235.1"), the following additional provisions shall apply:

1. The Parties agree to adopt the GDPR standard for all data transfers

2. References to the GDPR are to be understood as references to the FADP.

3. Supervisory authority:

(a) where the data transfer is exclusively subject to the FADP: the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner ("FDPIC"); or

(b) where the data transfer is subject to both the GDPR and the FADP: the competent supervisory authority is the FDPIC for data transfers governed by the FADP, and the competent EU supervisory authority for data transfer governed by the GDPR;

4. Applicable law for contractual claims under Clause 17 of the Standard Contractual Clauses:

(a) where the data transfer is exclusively subject to the FADP: Swiss law.; or

(b) where the data transfer is subject to both the GDPR and the FADP: French law

5. Place of jurisdiction for actions between the parties pursuant to Clause 18(b) of the Standard Contractual Clauses:

(a) where the data transfer is exclusively subject to the FADP: the courts of the canton of Vaud; or

(b) where the data transfer is subject to both the GDPR and the FADP: French courts

6. For the purposes of Clause 18(c), it is understood that any data subject located in Switzerland may also bring legal proceedings against the data exporter and/or data importer before the courts in Switzerland, being the courts he/she has his/her habitual residence.

In the context of jurisdiction for claims arising out of the Standard Contractual Clauses, the term "Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland).

ANNEX V

INCORPORATION OF THE UK INTERNATIONAL DATA TRANSFER ADDENDUM

Where a transfer of Personal Data from a Data Exporter to a Data Importer is subject to UK Legislation, this ANNEX V will apply.

In order for the Standard Contractual Clauses to comply with UK legislation and to ensure an adequate level of protection for transfers of Personal Data from the UK to a Non-Adequate Country, the terms of the transfer shall be governed by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as last published by the UK's Information Commissioner's Office, current version available on: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance (the "UK Addendum"), and the underlying Standard Contractual Clauses of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (included herein as Annex 3) which the UK Addendum amends with the following elections made and agreed to between the Parties for Part 1 (Tables) of the UK Addendum:

1. For Table 1 of the UK Addendum, the details of the parties are as set out in Annex I.A in Appendix to Annex 3 of this DPA.
2. For Table 2 of the UK Addendum,
   - (a) the selected option is the version of the EU SCCs, as amended pursuant to Annex 3 of this DPA;
   - (b) Modules 2 and/or 4 are selected as applicable and as described in Annex 3 of this DPA;
   - (c) Clause 7 (docking clause) (Modules 2 and 4) is selected;
   - (d) Option 2 (General Written Authorisation) of Clause 9a (Use of sub-processors) is included in Module 2.
   - (e) For Module 2, the time period for Option 2 of Clause 9a is at least thirty (30) calendar days in advance.
   - (f) Clause 11 will not apply.
   - (g) For Module 4, personal data received from the Importer is not combined with personal data collected by the Exporter, unless otherwise specified in the DPA.
3. For Table 3 of the UK Addendum,
   - (a) the details of the parties are as set out in Annex I.A in Appendix to Annex 3 of this DPA.
   - (b) the description of the transfer is as set out in Annex I.B in Appendix to Annex 3 of this DPA;
   - (c) the technical and organizational measures are as set out in Annex II in Appendix to Annex 3 of this DPA ; and
4. For Table 4 of the UK Addendum, Intuitive may end the UK Addendum as set out under Section 19.

ANNEX 4

ASEAN Model Contractual Clauses for Cross-Border Data Flows

Module 1: Contractual Provisions for Controller-to-Processor Transfers

1. Definitions

1.1. "AMS Law": Any and all written laws of an ASEAN Member State relating to data protection (or are, minimally, relevant to the transfer of Personal Data) which the Data Exporter or the Data Importer (or both) are subject to.

1.2. "Data Breach": Any loss or unauthorised use, copying, modification, disclosure, or destruction of, or access to, Personal Data transferred under this contract.

1.3. "Data Exporter": The Party which transfers Personal Data to the Data Importer under this contract.

1.4. "Data Importer": The Party which receives Personal Data from the Data Importer for Processing under this contract.

1.5. "Data Sub-Processor": Any person or legal entity which may be engaged by the Data Importer to assist in the Data Exporter's Processing of Personal Data on behalf of the Data Exporter.

1.6. "Enforcement Authority": Any public authority empowered by applicable AMS Law to implement and enforce the applicable AMS Law.

1.7. "Personal Data": Any information relating to an identified or identifiable natural person ("Data Subject") transferred under this contract.

1.8. "Processing": any operation or set of operations that are performed on Personal Data or on sets of Personal Data, whether or not by automated means, including, for example, collection, use and disclosure of Personal Data.

2. Obligations of Data Exporter

The Data Exporter warrants, represents and undertakes that:

2.1. The Personal Data has been collected, used, disclosed and transferred to the Data Importer under this contract in accordance with applicable AMS Law. In the absence of such law, where reasonable and practicable, the Data Subject has been notified of and given consent to the purpose(s) of the collection, use, disclosure and/or transfer of his/her Personal Data.

2.2. Intentionally omitted.

2.3. The Data Exporter shall implement adequate technical and operational measures to ensure the security of the Personal Data during transmission to the Data Importer.

2.4. The Data Exporter shall respond to enquiries from Data Subjects or Enforcement Authorities regarding the Processing of Personal Data by the Data Importer as required by applicable AMS Law, including requests to access or correct Personal Data, unless the Parties have agreed in writing that the Data Importer shall so respond, and such delegation is permitted by applicable AMS Law. Responses to such enquiries and requests shall be made within a reasonable time frame or within the time frame and in the manner, if any, required under the applicable AMS Law.

3. Obligations of Data Importer

The Data Importer warrants, represents and undertakes that:

3.1. The Data Importer shall Process the Personal Data only in compliance with the Data Exporter's instructions and for the purposes described in Appendix A.

3.2. The Data Importer shall not further disclose or transfer the Personal Data it receives from the Data Exporter to another person, Enforcement Authority or legal entity, including to Data Sub-Processors, unless it has notified the Data Exporter of such further disclosure or transfer in writing, and provided reasonable opportunity for the Data Exporter to object.

3.3. The Data Importer agrees that prior to any disclosure or transfer of Personal Data to third parties, including to Data Subprocessors, the Data Importer shall ensure that the third party shall be subject to and bound by the obligations of the Data Importer to the Data Exporter.

3.4. The Data Importer agrees to take reasonable steps to implement measures on the storage and Processing of Personal Data that comply with adequate security standards prescribed by the Data Exporter.

3.5. The Data Importer shall promptly communicate and refer to the Data Exporter any enquiries and requests from Data Subjects relating to the Personal Data transferred by the Data Exporter, including requests to access or correct the Personal Data.

3.6. At the reasonable request of the Data Exporter, the Data Importer shall provide access to its data processing facilities, data files, and documentation within a mutually agreeable time period for purposes of review and/or audit to verify compliance with the obligations set forth in this contract.

3.7. The Data Importer shall correct any error or omission in the Personal Data reasonably requested by the Data Exporter within a mutually agreeable time period, or such other time frame required by applicable AMS Laws, whichever is shorter.

3.8. Upon the termination of this contract or completion of Processing required under this contract, the Data Importer shall, at the election of the Data Exporter, either return to the Data Exporter the Personal Data held in its possession pursuant to this contract or cease to retain such Personal Data in manner approved of by the Data Exporter. The Data Importer agrees to confirm this with the Data Exporter in writing once action has been taken to cease to retain such Personal Data.

3.9. The Data Importer shall have in place reasonable and appropriate technical, administrative, operational and physical measures, consistent with applicable AMS Laws to protect the confidentiality, integrity and availability of Personal Data, in particular against risks of Data Breaches.

3.10. If the Data Importer becomes aware that a Data Breach has occurred affecting Personal Data in its possession or under its control, or in the possession or under the control of an importer of an onward disclosure or transfer of the Personal Data, it shall notify the Data Exporter within 24 (twenty-four) hours of becoming aware of the Data Breach.

3.11. The Data Importer shall promptly notify and consult with the Data Exporter regarding any investigation regarding the collection, use, transfer, disclosure, security, or disposal of the Personal Data transferred under this contract, unless otherwise prohibited under law.

3.12. The Data Importer shall provide prompt assistance to the Data Exporter upon request for the purposes of clause 2.4; and where the Data Importer has agreed in writing, to respond to enquiries and requests from Data Subjects or Enforcement Authorities regarding its Processing of Personal Data when notified by the Data Exporter.

APPENDIX A

To the ASEAN Model Contractual Clauses for Cross-Border Data Flows, Module 1: Contractual Provisions for Controller-to-Processor Transfers

TEMPLATE FOR DATA EXPORTERS AND IMPORTERS TO DESCRIBE PURPOSES FOR THE TRANSFER OF PERSONAL DATA

Name of Data Exporter	**Intuitive Surgical Operations, Inc. and its affiliates**
Name of Data Importer	See Annex 1
Description of the data subjects and groups of data subjects	See Annex 1
Description of purposes for the processing of personal data	See Annex 1