

Effective Date: March 31, 2024

This Privacy Notice (the "Notice") informs you as an Employee of Intuitive Surgical about how the Company collects and uses Employee Personal Information, and how Employees can exercise their rights with respect to their Personal Information.

The employee privacy policy is published on the internal company intranet site "Leo", as well as in our company policy library called "Agile". The list of Intuitive Surgical entities covered by this Notice ("Company") is available in Company [intranet](#) or can be requested from [data.privacy@intusurg.com](mailto:data.privacy@intusurg.com).

The Company is the controller of the Employee's Personal Information. The Employee may contact the Data Privacy Officer of the Company at [data.privacy@intusurg.com](mailto:data.privacy@intusurg.com), with regards to any issue related to the Processing of their Personal Information and to the exercise of their rights.

For purposes of this Notice, "**Personal Information**" (also known as identifiable information or personal data) means any information relating to an identified or identifiable natural person. "**Processing**" means any operation or set of operations which is performed on Personal Information, such as collection, recording, organization, structuring, storage, modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "**Employee**" means any employee, contractor, consultant or job applicant of the Company.

## 1. Collection, Processing and Disclosure of Personal Information

1.1. **Collection.** The Company collects Personal Information when the Employee submits their application to the Company, directly or through recruiting agencies, and throughout employment. The Company may collect the following categories of Personal Information:

- Identification Data: e.g., name, work and personal contact information, emergency contact information, date and place of birth, gender, marital status, citizenship, nationality, driving license information, ID card information, visa and work/residence permit, unique personal identifier, social security number and/or national identifier number, job title and role, signature.
- Recordings: e.g., photos, videos, still images, audio recordings.
- Education and Professional Data: e.g., education history, academic transcripts, qualifications, certifications, trainings, languages, professional memberships.
- Background Check Data: e.g., background check information, criminal background information, reference information.
- HR Data: e.g., CV, resume, cover letter, hire date, workplace, job details (business title, department, assignment status, working hours, work history etc.), information regarding compensation and benefits (healthcare, insurances, share awards, company car etc.), health information such as information related to occupational medical examination, travel information, military service information; holiday entitlement, leave of absences, performance-related information, disciplinary and grievance information, termination date and reason, family information such as children and spouse names and dates of birth;
- Financial data: e.g., bank account information, information related to personal tax situation, corporate expenses and payments, taxpayer ID;
- Judicial data: e.g., legal proceedings.

- Information system activity data: e.g., the Employee's use of Company information and communications systems; and/or,
- Any other information provided by the Employee

Where it is required under local or national laws or regulations, or where permitted by the Employee's express consent, the Company may also collect and Process sensitive personal information such as:

- Trade union membership.
- Information about health, including disability status, medical condition, health, and sickness records.
- Biometric data for identification purposes

**1.2. Processing.** The Company Processes Personal Information as necessary to perform a contract, to comply with legal obligations, or to pursue the legitimate interests of the Company. In some cases, Personal Information may be Processed only on the basis of Employee consent. Processing purposes may include the following:

Legitimate Interest of the Company/Performance of a Contract:

- a. Setting up a personnel file and managing employment matters
- b. Administering payroll, compensation, and benefits (e.g., insurance, car fleet)
- c. Employee performance management, salary review
- d. Management of holidays and leaves of absence; Work time management
- e. Corporate expense management
- f. Facilitating business travel and accommodation
- g. Granting access to the Company's software, and to provide hardware
- h. Grievance and disciplinary procedures
- i. Coordinating relocation
- j. Termination and post-termination matters

Legitimate Interest of the Company:

- k. Recruitment, background checks and replacement planning
- l. Managing information technology and communication systems, and related services
- m. Training
- n. Budgeting, financial management and reporting, and strategic planning
- o. Security measures and operations; fraud prevention; protecting data and assets
- p. Risk management
- q. Administrative tasks
- r. Event management, internal communication, rewards, and gifts to employees
- s. Maintaining licenses, permits, certifications and authorizations applicable to the Company's business operations

Legal Obligation:

- t. Employee complaint management (e.g., compliance hotline)
- u. Protecting the health and safety of Employees and third parties
- v. Managing legal claims, investigations, and disputes

- w. Meeting legal and regulatory requirements (e.g., taxation, social charges, social and insurance obligations, immigration, work, and residence permits)

1.3. **Disclosure.** The Company may disclose the Employee's Personal Information to:

(a) Third-parties under written contracts with the Company providing services or systems for: e.g., recruitment; background checks; human capital management; benefits & compensation; insurance; legal advice; medical and health care; training; time and absence management; financial services; accounting; payroll; corporate travel; information technology, security, and communication.

(b) Third parties where Company is bound by legal obligation: e.g., tax, regulatory, government agencies and other authorities; external auditors.

(jointly, "**Authorized Third Parties**").

(c) Under the DPF Principles, Company is liable if one of its agents processes personal information in a manner inconsistent with the DPF Principles, unless Company proves that it is not responsible for the event giving rise to the harm.

The Company may also disclose the Employee's Personal Information to other third parties when the Employee has provided their consent for doing so.

## 2. Transfer of Personal Information

As the Company is a global multinational corporation, Personal Information might be disclosed or transferred to, or Processed by any affiliate of the Company. Each affiliate is a data controller of the Employee's Personal Information within their control and may transfer it to Authorized Third Parties for the purposes described above. Each affiliate is liable if one of its agents processes personal information in a manner inconsistent with the DPF Principles, unless the affiliate proves that it is not responsible for the event giving rise to the harm. Your personal information may be transferred to countries where the local legislation provides a different level of protection for your personal information and rights. If that is the case, we use appropriate safeguards like standard contractual clauses to effectuate the transfer and will transfer the data only after having carried out an assessment of the level of protection of your rights on the territory of the third country where the recipient is established. The information that we collect about you may be stored in the EU/EMEA, Switzerland, UK, Israel, the United States and/or Mexico.

Intuitive Surgical, Inc., Intuitive Surgical Operations, Inc., Intuitive Surgical Holdings, LLC; Intuitive Surgical International Finance, LLC, Intuitive Venture Fund I, LLC, KindHeart, LLC, Orpheus Medical USA, Inc., and Intuitive Surgical Service Optic, Inc. (hereinafter: "Intuitive Surgical Entities Certified under the Data Privacy Framework") comply with and are certified under the EU-US Data Privacy Framework Principles ("EU-US DPF") and the UK Extension to the EU-US DPF ("UK-US Data Bridge") as set forth by the US Department of Commerce, with regard to the processing of personal data originating from the European Union and the United Kingdom. Intuitive has certified to the US Department of Commerce that it adheres to the Swiss-US Data Privacy Framework principles ("Swiss-US DPF") with regard to the processing of personal data originating from Switzerland in reliance on the Swiss-US DPF. If there is any conflict between the terms in this Privacy Notice and the Principles of the EU-US DPF and/or the UK-US Data Bridge and/or the Swiss-US DPF, the Principles of the EU-US

DPF, the UK-US Data Bridge and the Swiss-US DPF shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

The Intuitive Surgical Entities Certified under the Data Privacy Framework may be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or any other U.S. authorized statutory body.

We may be obliged to disclose personal information in response to lawful requests by US public authorities, including to meet national US security or US law enforcement requirements. In this respect, we have committed that our compliance with the Data Privacy Framework be subject to the review of the applicable EU data protection authorities. Where data transfers are not covered by the EU-US DPF, the UK-US Data Bridge or the Swiss-US DPF and where applicable, we have implemented international data transfer agreements based on standard contractual clauses covering onward transfers where applicable; a copy of these clauses can be obtained by contacting us at [data.privacy@intusurg.com](mailto:data.privacy@intusurg.com).

### 3. Security Measures for Personal Information

The Company has implemented appropriate technical, organizational, and physical safeguards to protect Personal Information. The Company stores Personal Information using industry-standard information technology and cloud services, and follows industry standard practices to maintain confidentiality, integrity and availability.

The Company stores and retains the Employee's Personal Information during and after the employment as required or permitted by applicable law.

### 4. No Automated Individual Decision-Making

The Company does not make decisions concerning the Employee based solely on automated Processing.

### 5. Requirement to Provide Data

As part of your employment, you must provide Personal Information that may be used to establish, administer or terminate the employment relationship. Without Personal Information, the Company will not be able to have an employment relationship with you. Both you and Intuitive have legal obligations described in 1.2 above. Intuitive will only request Personal Information from you for the purpose of fulfilling those obligations, and the law requires that you provide this Personal Information when requested.

### 6. Employee Rights with respect to their Personal Information

The Company will respect the rights of its Employees in accordance with applicable laws.

The rights applicable to an Employee may include:

- the right to access their Personal Information.
- the right to request that the Company rectifies, erases or restricts the Processing of their Personal Information.
- the right to object to the Processing of their Personal Information.

- the right to data portability.
- the right to give instructions on use and disclosure of their Personal Information after their death.
- the right to request compensation for alleged unlawful processing of their Personal Information.
- when Processing of Personal Information is based on the Employee's consent, the Employee may at any time withdraw their consent.

The Employee can exercise these rights by contacting the Company's Data Privacy Officer via e-mail at [data.privacy@intusurg.com](mailto:data.privacy@intusurg.com)

The Employee also has the right to lodge a complaint with any local data protection authority or with the *Commission Nationale de l'Informatique et des Libertés* ([CNIL](https://www.cnil.fr/)), the Company's lead data protection authority in the EU.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Intuitive Surgical commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship. As further explained in the DPF Principles, binding arbitration is available to address residual complaints not resolved by other means. We are obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that applicable procedures, including delivery of appropriate notice, have been followed and subject to conditions set forth in Annex I of the DPF Principles.

## California Privacy Rights

California Civil Code Section 1798.83 permits individual California residents to request certain information regarding our disclosure of certain categories of personal information to third parties for those third parties' direct marketing purposes. To make such a request, please contact us at [data.privacy@intusurg.com](mailto:data.privacy@intusurg.com). This request may be made no more than twice in a 12-month period and we reserve our right not to respond to requests submitted other than to the email or mailing addresses specified in this policy. Note that we do not currently share personal information with third parties for those third parties' direct marketing purposes.

In addition, California residents have the following privacy rights:

- **The right to know.** You have the right to request to know (i) the categories of personal information we have collected about you in the last 12 months; (ii) the specific pieces of personal information we have about you; (iii) the categories of sources from which that personal information was collected; (iv) the categories of your personal information that we sold or disclosed in the last 12 months; (v) the categories of third parties to whom your personal information was sold or disclosed in the last 12 months; and (vi) the purpose for collecting and selling your personal information.
- **Right to correct.** You have the right to obtain without undue delay the correction of inaccurate, incomplete, or outdated personal information concerning you.

- **The right to deletion.** You have the right to request that we delete the personal information that we have collected or maintain about you. We may deny your request under certain circumstances, such as if we need to comply with our legal obligations or complete a transaction for which your personal information was collected. If we deny your request for deletion, we will let you know the reason why.
- **The right to equal service.** If you choose to exercise any of these rights, Intuitive will not discriminate against you in anyway. If you exercise certain rights, understand that you may be unable to use or access certain features of our websites or services.

Intuitive does not “sell” or “share” your personal information as those terms are defined in the California Privacy Rights Act.

You may exercise your right to know twice a year. To exercise your rights, contact us via [data.privacy@intusurg.com](mailto:data.privacy@intusurg.com).

We will take steps to verify your identity before processing your request. We will not fulfill your request unless you have provided sufficient information for us to reasonably verify you are the individual about whom we collected personal information. We will only use the personal information provided in the verification process to verify your identity or authority to make a request and to track and document request responses unless you initially provided the information for another purpose.

You may use an authorized agent to submit a request. When we verify your agent’s request, we may verify your identity and request a signed document from your agent that authorizes your agent to make the request on your behalf. To protect your personal information, we reserve the right to deny a request from an agent that does not submit proof that they have been authorized by you to act on their behalf.