Intersurgical Personal Data Processing Policy

Introduction

Intersurgical is required to process personal data relating to its employees, contractors, visitors, customers and prospective customers as part of its operation. Intersurgical will take all reasonable steps to do so in accordance to this policy.

General provisions

1. The purpose of this document is to define the procedures of how Intersurgical Ltd (hereinafter referred as Intersurgical) collects, uses, discloses and/or processes personal data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC General Data Protection Regulation (hereinafter referred as GDPR). Also, how it ensures the adequate level of data protection prescribed by other data protection related national acts of United Kingdom.
2. Personal data processing shall meet the requirements of GDPR and be in accordance with the applicable national privacy laws.
3. Other terms and definitions used in this Policy have the same meaning as in GDPR and applicable national privacy laws.

Information about data controller(s) and data processor(s)

4. Intersurgical is the main data controller and processor of owned and processed personal data:
   - 4.1. Intersurgical Ltd, legal entity identifier 1488409, address – Crane House, Molly Millars Lane, Wokingham, Berkshire, United Kingdom, RG41 2RZ
5. Data processors also are other Intersurgical group companies.
6. Information about data controller and processor by different categories of personal data is provided in Annex 1.

Liability and obligations of the data controller and processor

7. Rights of the Data Controller:
   - 7.1. to proceed, review and update this procedure and other internal documents related to personal data processing;
   - 7.2. to make decisions on personal data disclosure;
   - 7.3. to approve and assign an appropriate person or department to protect the rights of Data Subjects;
   - 7.4. to subcontract processing of personal data or share personal data with third parties.
8. Responsibilities of the data controller:
   - 8.1. to ensure personal data protection is in accordance with GDPR and applicable national privacy laws;
   - 8.2. to ensure that processing meets the requirements of this procedure and guarantees the protection of the rights of the Data Subject;
   - 8.3. to implement appropriate technical and organisational measures to provide protection of the personal data;
   - 8.4. to assign the data processor who/which can ensure appropriate technical and organisational measures in such a manner that processing will meet the requirements of this procedure and ensure the protection of the rights of the Data Subject. Processing by the data processor shall be governed by a contract;
   - 8.5. to inform competent supervisory authority about processing of the personal data in accordance with GDPR and applicable national privacy laws.
9. Duties of the Data Controller:
   - 9.1. to define the purpose for which the data is processed;
   - 9.2. to organize a set-up of surveillance systems or other systems which are required for processing personal data;
   - 9.3. to provide the access rights and authorisation for processing personal data;
   - 9.4. to analyse technological, methodical and organisational problems related to processing personal data and in an effective manner, integrate the necessary safeguards into the processing in order to meet the requirements of this procedure and protect the rights of data subjects;
   - 9.5. to assist employees and provide recommendations related to processing of personal data to the data processor;
   - 9.6. to ensure that all employees involved with data processing are familiar with the current state of the legislation regarding personal data processing;
   - 9.7. other actions are taken to ensure that Data Controller's responsibilities and duties are performed.

Personal data

10. Personal data covers any information that relates to a living individual (Data Subject) who can be identified from that information. Processing is any use that is made of the data including collecting, storing, amending, disclosing or destroying it.

Basis and purposes for personal data processing

11. The following actions are taken during personal data processing: Intersurgical has identified that personal data is processed by the following:
    - 11.1. video surveillance system is used to monitor or record the activities which can ensure the protection of the company's assets, the quality of production processes and lawful procedures regarding work safety;
    - 11.2. company is administered internally while managing human resource records, administrating the orders of customers and carrying on with sales.
12. Detailed information about legal basis and purposes for personal data processing by different categories of personal data is provided in Annex 2.
13. Video surveillance system is used and covers indoor and outdoor facilities (external perimeter and territory of facility, parking lots and entrances to the premises, warehouses and manufacturing building premises, common work places in the industrial premises) of Intersurgical. Video surveillance data processing is defined in detail within UK Employee Handbook.

Data protection princliples

14. Intersurgical processes personal data in accordance with the following data protection principles:
    - 14.1. The Company processes personal data lawfully, fairly and in a transparent manner.
    - 14.2. The Company collects personal data only for specified, explicit and legitimate purposes.
    - 14.3. The Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
    - 14.4. The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
    - 14.5. The Company keeps personal data only for the period necessary for processing.
    - 14.6. The Company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Transfers of personal data and the data receivers

15. Intersurgical does not transfer personal data to third parties. Other Intersurgical group companies are not considered as third parties.
16. Any transfers of personal data shall be in accordance with GDPR and applicable national privacy laws.
17. The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by European Union or Member State law.

Technical and organisational controls

Intersurgical has put the following controls in place to ensure personal data is protected:

18. Appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data:
    - 18.1. to ensure there is protection, a process and control of access to personal data;
    - 18.2. each user shall use an account that has permissions appropriate to the job they are carrying out at the time;
    - 18.3. authorised users can perform only certain procedures or actions with personal data which they had authorisation for;
    - 18.4. the access to personal data must be protected by passwords or other security means. If the passwords are used, they must comply with the following requirements:
        - 18.4.1. must be issued, updated and protected to ensure the confidentiality;
        - 18.4.2. must be at least 8 characters long and have a combination of upper and lower-case letters, numbers and the special keyboard characters like the asterisk or currency symbols, excluding any personal information;
        - 18.4.3. passwords are changed on a regular basis (no less than once per 6 months);
        - 18.4.4. it must be changed after first log in.
    - 18.5. personal data is protected from unauthorised access to electronic communications;
    - 18.6. access to all data centres and server rooms used to host hardware and software on which personal data is stored is restricted only to those staff members that have clearance to work there;
    - 18.7. hardware where the personal data is stored is protected by antivirus software and has up-to-date operating system security patches;
19. Procedure for granting, cancelling and modifying the access rights or users to process image data:
    - 19.1. the access rights of users are granted, cancelled or modified by approval of the employee's direct manager based on internal procedures;
    - 19.2. the access rights of users to information assets are to be removed upon termination of their employment, contract or agreement, or adjusted upon change. Upon termination, the access rights of an individual to information and assets associated with data processing facilities and services are removed or suspended immediately.
20. Retention periods of different categories of personal data are defined by responsible department of Intersurgical and provided in Annex 3.
21. To ensure the access to personal data during retention period, data is backed up in accordance with timetable. The storage medium is stored in a secure environment with a log of access kept. Access is restricted to authorised personnel.

Personal data security breach management

22. If any staff member who has access rights to personal data have noticed any information/data security breach (any unintentional/for purpose release of confidential or personal information/data to unauthorised persons, either through the accidental disclosure, loss or theft of the information/data), they should immediately report to Data Protection Officer or direct manager.
23. Personal data breaches are managed in accordance with Personal Data Breach Management Plan.
24. In assessing the risk arising from the security breach in different situations, the Data Protection Officer considers what would be the potential adverse consequences for individuals. Furthermore, the degree of the impact, damage and consequences of the breach is taken into consideration which leads to decisions on the measures to be taken to contain the breach.

Rights of the data subject

25. The rights of the Data Subject (individual) are as follows:
    - 25.1. to know (be informed) about the processing of his or her personal data;
    - 25.2. to have access to his or her personal data;
    - 25.3. to object to his or her data processing;
    - 25.4. to request rectification of his or her personal data;
    - 25.5. to request erasure of his or her personal data
    - 25.6. to restrict further processing of personal data, with the exception of storage, where the data processed is in violation of the provisions of GDPR or applicable national privacy laws;
    - 25.7. to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format.
26. The general rules of implementation data subject's rights are the following:
    - 26.1. The Data Subject should send their request to the Data Controller or Processor in writing. The company electronic form may be used to make this request.
    - 26.2. an individual may be required to provide an identity document or verify his or her identity according to applicable laws, or through electronic means of communication, which provides reliable identification of the person, to verify his or her identity.
    - 26.3. if the request by the Data Subject is received by post or by courier, a notarized copy of identity document signed by a notary public must be present. If the data subject is represented by another person, the General Power of Attorney must be provided as a proof of allowing the representor to act on the Data Subject's behalf. Also, the notarized copy of representor's identity document signed by a notary public must be present.
    - 26.4. the Data Subject is provided with information or requested personal data after the request concerning the processing of personal data is received and verification of the identity of the data subject is complete;
    - 26.5. the request of the data Subject must be answered within 30 calendar days after the request was submitted;
    - 26.6. if the request from the Data Subject was received in written form, the answer must be composed in the same form.
27. A Data Subject has the right to access his or her personal data and this request is processed accordingly:
    - 27.1. An individual has the right to access his or her personal data, processed by the company and to obtain information, on the sources and the type of personal data that has been collected, the purpose of processing and the data recipients to whom the data are disclosed or have been disclosed within last year; the right to the privacy of third parties must be ensured when enforcing the right of the data subject to access her or his personal data, for example, when the Data Subject is acquainted with the video data and third parties can be identified or other information might violate their privacy (for example, registration number of the vehicle), the video must be retouched or eliminated in other ways removing the possibility of identifying third parties;
    - 27.2. in general, subject access requests from a Data Subject concerning the processing of their personal data must be responded to within 30 calendar days from the date a complete request is received. Where the request of the Data Subject is submitted in writing, the Data Controller's or Data Processor's reply must also be executed in writing. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
    - 27.3. The Data Controller or Processor shall provide a copy of the personal data undergoing processing free of charge once per year. For any further copies requested by the Data Subject, the Controller or Processor may charge a reasonable fee based on administrative costs determined by competent supervisory authority.
28. The Data Subject has the right to object personal data processing and the procedure is carried accordingly:
    - 28.1. the Data Subject has the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her;
    - 28.2. the Data Subject has the right to object to the processing of personal information before it is processed based on the grounds in GDPR Article 21or applicable national privacy laws. The Data Subject shall be informed in writing about our intentions to process this data (collection, usage, disclosure by transmission, etc.) before it is processed with the option to refuse, an explanation of legal procedures which have to be carried when processing via mail or by means of electronical communication, and the determination of a reasonable time period in which the data subject has the right to express his or her will.;
    - 28.3. where the objection of the Data Subject is legally justified, the Data Controller and Data Processor must suspend the processing of this personal data, without delay and free of charge, and duly notify the data recipients;

29. The Data Subject has the right to request erasure or restriction of the processing of the personal data (this does not apply to personal data storage):
    29.1. if the Data Subject became aware that his or her personal data is being processed illegally and not compliant with the procedures, he/she or their representative must notify the Data Controller. The following further actions should be taken: the Data Controller should check legitimacy and integrity of data processing free of charge, immediate actions to delete unauthorised and fraudulently generated personal data should be implemented, and processing of such data should be suspended with the exception of data storage;
    29.2. the Data Controller and Processor may keep personal data while the processing operations are suspended or until the data is destroyed (at the request of the data subject or after the data storage time expires). Further actions related to personal data may only be carried:
        29.2.1. for purposes to investigate circumstances of suspended data processing;
        29.2.2. if the data subject gives consent for continuing processing;
        29.2.3. to protect the rights and interests of third parties.
    29.3. the Data Controller immediately, no later than within 30 days, must inform the Data Subject or his/her representative about the actions taken in regard with the request received;
    29.4. personal data of the Data Subject is destroyed, or processing is suspended upon the request of the Data Subject or his/her authorised representative in compliance with identification of the Data Subject;
    29.5. the Data Controller immediately, no later than within 30 days, informs the data recipients about the request from the Data Subject or his/her representative regarding personal data and the implementation of the suspension of personal data process. Personal data processing suspension is not applied if it is impossible due to an enormous number of Data Subjects, data period or excessive expenditure. In this case the competent supervisory authority must be notified immediately.
30. The right of rectification is implemented accordingly:
    30.1. In order to ensure that the personal data of the data subject is being processed is inaccurate or incomplete, the Data controller may ask the data subject to provide supporting evidence;
    30.2. if the personal data of the data subject (as corrected at the request of the data subject) were passed to the data recipients, the Data controller shall inform the recipients, unless this would be impossible or demanding a disproportionate effort. The data subject has the right to request information about such recipients.
31. The right to receive personal data relating to data subject, which he or she submitted to the controller in a systematic, commonly used and computer-readable format, shall only be implemented if the data are processed by automated means on the basis of consent or contract.
32. The Data Controller has the right to refuse to implement the rights of data subject only based on GDPR requirements or applicable national laws.

Individual responsibilities

33. Individuals are responsible for helping the company keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.
34. Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.
35. Individuals who have access to personal data are required:
    35.1. to access only data that they have authority to access and only for authorised purposes;
    35.2. not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
    35.3. to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
    35.4. not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
    35.5. not to store personal data on local drives or on personal devices that are used for work purposes; and
    35.6. to report data breaches of which they become aware to [name of individual/the data protection officer] immediately.
36. Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Final provisions

37. Every employee who processes personal data while performing their duties at work, must follow this procedure, the requirements for the processing of personal data in accordance with GDPR and applicable national laws.
38. Employees are briefed on this procedure by signing it. New employee must be introduced to the procedure on the first day of employment.
39. This procedure must be reviewed at least once a year and, if necessary, amended or modified in accordance with internal processes.

Annex 1 of Personal Data Processing Procedure
Information about data controller(s) and data processor(s)

No.	Category of personal data	Data controller(s)	Data processor(s)
1.	Employees data	Intersurgical Ltd	Intersurgical Ltd
2.	Data of candidates during recruitment campaigns	Intersurgical Ltd	Intersurgical Ltd
3.	Data of clinical investigations participants (pseudonyms, no special category data)	Intersurgical Ltd	Intersurgical Ltd
4.	Customer (legal entity) data	Intersurgical Ltd	Intersurgical Ltd
5.	Post marketing surveillance and Post-market Clinical Follow-up activities	Intersurgical Ltd	Intersurgical Ltd
6.	Prospective customer (legal entity) data	Intersurgical Ltd	Intersurgical Ltd
7.	Contractor/ supplier data	Intersurgical Ltd	Intersurgical Ltd
8.	Reseller/ distributor data	Intersurgical Ltd	Intersurgical Ltd
9.	Video surveillance records	Intersurgical Ltd	Intersurgical Ltd
10.	Entry control records	Intersurgical Ltd	Intersurgical Ltd
11.	Personal information/ usage/ behaviour data	Intersurgical Ltd	Intersurgical Ltd

Annex 2 of Personal Data Processing Procedure
Legal basis and purposes for personal data processing

No.	Category of personal data	Legal basis	Business purpose
1.	Employees data	Data subject consent (point (a) of GDPR Article 6(1)) Performance of a contract or required prior to entering into a contract (point (b) of GDPR Article 6(1)) Legal obligation (point (c) of GDPR Article 6(1))	Internal administration
2.	Data of candidates during recruitment campaigns	Data subject consent (point (a) of GDPR Article 6(1)) Legitimate interests pursued by the controller or by a third party (point (f) of GDPR Article 6(1))	Internal administration
3.	Data of clinical investigations participants (pseudonyms, no special category data)	Data subject consent (point (a) of GDPR Article 6(1))	Scientific researches
4.	Customer (legal entity) data	Data subject consent (point (a) of Article 6(1)), Performance of a contract or required prior to entering into a contract (point (b) of GDPR Article 6(1))	Provision of services/products Customer service
5.	Post marketing surveillance and Post-market Clinical Follow-up activities	Legal obligation (point (c) of GDPR Article 6(1))	Product quality and safety
6.	Prospective customer (legal entity) data	Data subject consent (point (a) of GDPR Article 6(1)) Performance of a contract or required prior to entering into a contract (point (b) of GDPR Article 6(1))	Provision of services/products Direct marketing
7.	Contractor/ supplier data	Performance of a contract or required prior to entering into a contract (point (b) of GDPR Article 6(1))	Provision of services/products Customer service Internal administration
8.	Reseller/ distributor data	Performance of a contract or required prior to entering into a contract (point (b) of GDPR Article 6(1))	Provision of services/products Customer service Internal administration
9.	Video surveillance records	Legitimate interests pursued by the controller or by a third party (point (f) of GDPR Article 6(1))	Property protection, provision of services/ products (quality)
10.	Entry control records	Legitimate interests pursued by the controller or by a third party (point (f) of GDPR Article 6(1))	Property protection, employee time-keeping
11.	Personal information/ usage/ behaviour data	Data subject consent (point (a) of GDPR Article 6(1)) (personal information) Legitimate interests pursued by the controller or by a third party (point (f) of GDPR Article 6(1)) (usage, behaviour data)	There is no purpose for processing this kind of information. Intersurgical has no intentions to process such data for business process but it is aware that such information can be processed by employees themselves in computers and mobiles and by Intersurgical IT department for equipment maintenance purposes

Annex 3 of Personal Data Processing Procedure
Data retention periods for different personal data categories

No.	Category of personal data	Retention period	Comments, basis for such period
1.	Employees data	Various form 1 - 50 years – detailed confirmation outlines in the Employee Privacy Notice	Data Protection Act 1998; The National Archives Retention Scheduling: Employee Personnel Records
2.	Data of candidates during recruitment campaigns	6 months from the recruitment exercise	Due to time limits on various discrimination acts. Successful job applicant documents will be transferred to the HR file in any event
3.	Data of clinical investigations participants (pseudonyms, no special category data)	5 years after the clinical investigation	
4.	Customer (legal entity) data	1 - 10 years after last purchase	Data Protection Act 1998; The National Archives Retention Scheduling: Accounting records
5.	Post marketing surveillance and Post-market Clinical Follow-up activities	5 years	Legal acts, regarding medical equipment
6.	Prospective customer (legal entity) data	2 years after last person contact	Business needs
7.	Contractor/ supplier data	1 - 10 years after last purchase	Data Protection Act 1998; The National Archives Retention Scheduling: Accounting records
8.	Reseller/ distributor data	1 - 10 years after last purchase	Data Protection Act 1998; The National Archives Retention Scheduling: Accounting records
9.	Video surveillance records	30 days	Legitimate interest – property protection, safety accidents history
10.	Entry control records	1 year	Legitimate interest – property protection, incidents history
11.	Personal information/ usage/ behaviour data	1 year	Legitimate interest – confidential information protection, security incidents investigation