

I. INTRODUCTION

This Personal Data Processing Policy (*also referred to as “Policy” or “Rules”*) regulate Intersurgical Ltd., registered at Crane House, Molly Millars Lane, Wokingham, Berkshire United Kingdom RG41 2RZ, code 01488409 (*also referred to as “we”, “us”, “Intersurgical”, “Company”*) purposes and principles of Personal Data processing, the processed Personal Data and the terms of their storage, the procedures of implementation of the rights of Data Subjects, applicable technical and organizational measures of Personal Data security, relationship with the Supervisory authority, the transfer of Personal Data to the recipients, data processors, obligations of employees and their liability for the non-compliance with the Rules.

II. GENERAL PROVISIONS

1. The purpose of this document is to define the procedures of how 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.

III. MAIN DEFINITIONS

4. **Candidate** – a person applying for a job position in the Company.

5. **Consent of the Data subject** – any freely given, specific, informed and unambiguous indication of the Data Subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

6. **Data processor** – a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Company.

7. **Data recipient** – a natural or legal person, public authority, agency or another body, to which the Personal Data is disclosed, irrespective whether a third party or not.

8. **Data Subject** – in a context of these rules means an Employee or Applicant whose personal data is processed by the Company.

9. **Employee** – a person who has concluded an employment contract with the Company.

10. **Personal Data** – any information relating to a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

11. **Personal Data processing** – any operation or set of operations which is performed on Personal Data or on set of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

12. **Supervisory authority** – the Information Commissioner’s Office (ICO).

IV. PRINCIPLES OF PERSONAL DATA PROCESSING

13. Processing of Personal Data in the Company shall be carried out in accordance with the following main Personal Data processing principles:

13.1. Principle of legality, fairness and transparency which means that Personal Data with respect to the Data Subject is processed in a lawful, honest and transparent way;

13.2. Purpose limitation principle which means that Personal Data is collected for specified, clearly defined and legitimate purposes and shall not be further processed in a way incompatible with those purposes;

13.3. Data minimisation principle which means that Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

13.4. Accuracy principle which means that Personal Data must be accurate and, if necessary, updated; all reasonable steps must be taken to ensure that Personal Data which is not accurate in relation to the purposes for which they are processed are erased or rectified without undue delay;

13.5. The principle of limitation of the length of the storage which means that Personal Data shall be kept in such a way that the identity of the Data Subjects can be determined for no longer than is necessary for the purposes for which Personal Data is processed;

13.6. Integrity and confidentiality principle which means that Personal Data shall be managed by applying appropriate technical or organizational measures in such a way as to ensure the proper security of Personal Data, including protection from unauthorized processing or processing of unauthorized data, and against accidental loss, destruction or damage.

13.7. By processing the Personal Data, the Company implements the legal requirements of the protection of Personal Data, supervises their compliance and accumulates the data due to prove the compliance with General Data Protection Regulation. The Company implements the principle of accountability by the following measures:

13.8. The processing of Personal Data in the Company is carried out only by the Employees to the extent necessary for the performance of the work function;

13.9. The objectives of the processing of Personal Data, processed Personal Data and other circumstances are set forth, the responsible person for the processing of Personal Data is designated, including the Data protection officer;

13.10. Procedure of the implementation of Data Subjects' rights is established;

13.11. Technical and organizational measures for the security of Personal Data are applied;

13.12. Trainings for the Employees are organized and recorded.

V. PERSONAL DATA PROCESSING OF COMPANY'S CLIENTS

14. Annex No. 1 regulates Company clients' Personal Data processing purposes, legal basis, processed Personal Data (its categories), data receivers and sources of such data.

VI. PERSONAL DATA PROCESSING OF THE EMPLOYEES AND CANDIDATES TO AN EMPLOYEE POSITION

15. Annex No. 2 regulates "Intersurgical Ltd." Employees' and Candidates' Personal Data processing purposes, legal basis, processed Personal Data (its categories), data receivers and sources of such data.

VII. DATA PROCESSING OF THE PERSON WHO IS CONTACTING THE COMPANY

16. Annex No. 3 regulates persons' who is contacting the Company Personal Data processing purposes, legal basis, processed Personal Data (its categories), data receivers and sources of such data.

VIII. PERSONAL DATA PROCESSING OF THE PARTNERS OF THE COMPANY

17. Annex No. 4 regulates Company partners or Company's partners' employees / representatives Personal Data processing purposes, legal basis, processed Personal Data (its categories), data receivers and sources of such data.

IX. PERSONAL DATA PROCESSING OF THE SHAREHOLDERS' REPRESENTATIVES OF THE COMPANY

18. Annex No. 5 regulates Company shareholders' representatives Personal Data processing purposes, legal basis, processed Personal Data (its categories), data receivers and sources of such data.

X. PERSONAL DATA PROCESSING FOR DIRECT MARKETING PURPOSES

19. The direct marketing is the activity that is intended to offer the goods or services to clients by email, as well as to inquire the opinion of clients about the offered goods and services.

20. The Company may use end clients' email addresses for similar goods or services marketing when a freely given, specific and unambiguous indication of client's (as end user's) consent is given for the Company.

21. In cases when such consent is given for the Company for the use of the client's email for the marketing of similar goods and services, the client is granted with clear, free of charge and easily realizable possibility to object or withdraw from such use of client's contact details.

22. In case if client does not agree to receive these marketing messages and / or calls offered by the Company, partners of the Company or third parties, this will not have any impact on provision of the services to client.

23. The Company shall provide a clear, free-of-charge and easily realizable option for the Data Subject at any time not to give his consent or to withdraw given consent on sending of the proposals by the Company. The Company shall state in each notification sent by e-mail that the Data Subject is entitled to object to processing of Personal Data or refuse to receive notifications from the Company. The Data Subject shall be entitled to refuse to receive notifications sent by the Company by clicking on the respective link in each e-mail notification.

24. Having received a withdrawal of consent or objection to the processing of Personal Data for the before-mentioned purpose, the Company shall immediately erase the Data Subject's Personal Data processed solely for the purpose of direct marketing and shall not send email notifications any longer. In any case, withdrawal of consent and/or objection to the processing of Personal Data for the before-mentioned purpose shall not affect lawfulness of the processing of Personal Data before withdrawal.

XI. IMPLEMENTATION OF DATA SUBJECT RIGHTS

25. Following the requirements of the legal acts regulating protection of Personal Data, the Company shall guarantee the following rights for the Data Subjects:

25.1. To get familiar with Personal Data and know how it is processed;

25.2. To require rectifying false or incomplete Personal Data;

25.3. To require that the processing of Personal Data is restricted if there is a basis in the General Data Protection Regulation;

25.4. To object the processing of Personal Data if there is a basis in the General Data Protection Regulation;

25.5. To transfer Personal Data to another data controller or provide directly to the Data Subject in a convenient format (applicable to Personal Data which is provided by the Data Subject and which is processed by automated means on the basis of consent or on the basis of conclusion and performance of the contract);

25.6. To request to erase Personal Data if there is a basis in the General Data Protection Regulation;

25.7. To lodge a complaint to the Company and/or the Supervisory authority;

25.8. Other rights established in the General Data Protection Regulation and legal acts.

26. In cases where the Company received the Data Subject's request for exercise of his/her rights and acts as Data processor in respect of Personal Data and the basis indicated in the request, the Company shall transfer such request to Data controller. Further process of the examination of such requests may be fully specified in the contract between the Company and Data controller

27. The Company shall exercise rights of the Data Subjects only after receipt of a written request for execution of the particular right from the Data Subject and only after confirming the validity of Data Subject's identity.

28. The Data Subject shall submit such written request to the Company by:

28.1. Sending it by e-mail.;

28.2. Personally appearing at the registered office address of the Company;

28.3. Ordinary mail.

29. The request shall be provided in national or English language, be legible, contain information of which right referred to in clauses 32– 39 hereof and to what extent the Data Subject would like to exercise.

30. The Data Subjects' requests shall be fulfilled or fulfilment of the Data Subjects' requests shall be refused by specifying the reasons for such refusal within 30 calendar days from the date of submission of the request meeting the Rules and the General Data Protection Regulation. The aforementioned term may be extended for 30 calendar days subject to prior notice to the Data Subject if the request is related to great scope of Personal Data, other simultaneously examined requests. A response to the Data Subject shall be provided via email, unless the Data Subject indicates other preferred form.

31. The request submitted by the Data Subject shall be examined free of charge. However, if the Data Subject provides requests on a regular basis, the submitted requests are evidently unreasonable or excessive, the Company shall, taking into account the administrative costs related to provision of information or communication or performance of the requested actions, be entitled to request to pay a reasonable fee for examination of the submitted request or to refuse to fulfil the request by giving a prior notice to the Data Subject.

32. The right to get familiar with Personal Data and to know how it is processed

32.1. For the purposes of exercise of the right to access the Personal Data processed by the Company, the Data Subject shall be entitled to submit a request for access only of own Personal Data and receive information from which sources, what data and for what purpose it is collected, what data receivers will get this data and what is expected data retention period.

32.2. Upon receipt of the request for access of own Personal Data, the Data protection officer or responsible employee of the Company shall assess it, take a decision on whether to authorize or not access to Personal Data within the set time limit and inform the Data Subject. The Data Subject shall be granted access to Personal Data not later than within 30 calendar days, and in cases where the time limit for examination of the request is extended – within 60 calendar days from the date of received request of the Data Subject.

32.3. In cases where it is forbidden by the legal acts, the Company cannot provide the Data Subject with any information on processing of his/her Personal Data, e. g., where information is provided to law enforcement authorities, prosecutor's offices, courts.

33. The right to demand rectifying false or incomplete Personal Data

33.1. If, having accessed own Personal Data, the Data Subject determines that this Personal Data is false, incomplete or inaccurate, he/she shall be entitled to approach the Company with a request to rectify such Personal Data and/or, taking into account the purposes of processing of Personal Data, supplement incomplete Personal Data or erase Personal Data.

33.2. Having received a request for rectification of Personal Data, the Company shall verify the accuracy of Personal Data and, if necessary, at the request of the Data Subject, rectify any false, incomplete, inaccurate data and update processing of Personal Data or, in the cases set forth in the legal acts, restrict the actions of processing of such data.

33.3. The Company shall be entitled to request an evidence from the Data Subject supporting the need to rectify the Personal Data of the Data Subject.

33.4. Personal Data may be rectified in another manner upon receipt of information on the changes in Personal Data. Personal Data shall be rectified by the person having the authorizations to process the respective Personal Data.

33.5. The Company shall undertake to ensure that all data recipients were immediately notified of the any rectification of Personal Data of the Data Subject unless this proves impossible or involves disproportionate effort.

34. Right to request to restrict Personal Data processing if there is a basis in the General Data Protection Regulation

34.1. The Data Subject shall be entitled to request that processing of his Personal Data was restricted if:

34.1.1. the Data Subject contests the accuracy of his Personal Data; in this case, the restriction shall be valid for the period during which the Company may verify the accuracy of processed Personal Data;

34.1.2. The Data Subject believes that processing of Personal Data is unlawful and opposes the erasure of Personal Data but requests that processing of Personal Data was restricted; in this case, restriction shall be valid for the period reasonably indicated by the Data Subject;

34.1.3. The Company no longer needs the Personal Data of the Data Subject but the Personal Data is required by the Data Subject for exercise or defence of his/her rights and legitimate interests, bringing of an action etc.;

34.1.4. The Data Subject has objected to processing of his/her Personal Data carried out by the Company in order to ensure its legitimate interests but such restriction is valid only for the period pending the verification whether the legitimate grounds of the Company override those of the Data Subject.

34.2. When processing has been restricted under Clause 34 of the Policy, such Personal Data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest or in compliance with legal requirements.

34.3. The Company shall undertake to ensure that all data recipients were immediately notified of the particular restricted processing of Personal Data of the Data Subject unless this proves impossible or involves disproportionate effort.

35. Right to transfer Personal Data to another data controller or provide directly to the Data Subject in a convenient form

35.1. The Data Subject's request for transfer of Personal Data shall be fulfilled only on the basis of Personal Data processed by automated means, on the basis of the consent of performance of the contract. The Company has the right to refuse to exercise the Data Subject's right to data portability if such request cannot be fulfilled by the Company due to the lack of technical resources.

36. The right to object to processing of Personal Data

36.1. The Data Subject shall be entitled to object to processing of his Personal Data if there is a basis provided in the General Data Protection Regulation. The Company shall immediately suspend processing of the Personal Data for the period within which the Company carries out assessment whether the Data Subject's request is justified.

36.2. The Company shall no longer process the Personal Data unless the Company demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

36.3. In that case, if it is established that the Data Subject's right to object to processing of his Personal Data overrides the legitimate interests of the Company, the Company shall suspend processing of the data of the Data Subject.

36.4. Where Personal Data are processed for direct marketing purposes, the Data subject shall have the right to object at any time to processing of Personal Data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

37. The right to withdraw the consent given to the Company

37.1. Where Personal Data is processed on the basis of consent, the Data Subject shall have the right at any time to approach the Company and withdraw the earlier given consent. If the Company receives such request, it shall immediately suspend processing of Personal Data on the basis of consent. Withdrawal of the consent shall not affect lawfulness of the processing of data based on the consent before withdrawal of the consent.

38. The right to request to erase own Personal Data if a ground provided for in the Regulation exists

38.1. The Data Subject shall be entitled to request to erase his Personal Data processed by the Company if:

38.2. The Data Subject believes that the data is no longer necessary or used for the primary purposes of processing of Personal Data;

38.3. The Data Subject reasonably believes that his Personal Data is processed in an unlawful manner, e. g., for the purpose of direct marketing after the Data Subject has withdrawn his consent on the basis of which the Company processed his Personal Data and the Company has no other grounds for processing of Personal Data of the Data Subject;

38.4. The instructions on erasure of the Personal Data of the Data Subject are established in the legal acts providing for the duration of the periods of retention of data;

38.5. In other cases, provided for in the Regulation

38.6. The request for erasure of Personal Data must indicate the scope of the Personal Data asked for the erasure, if the Data Subject is aware, the basis for such request. Having received the request to erase Personal Data and having confirmed the reasonableness of the request, the Company shall be obliged to notify the recipients of such Personal Data including publication of the duty to erase the data and indicate the scope of the erased Personal Data, unless this proves impossible or involves disproportionate effort.

39. Handling of complaints from Data Subjects in the Company and lodging complaints against Company's decisions and/or actions to the Supervisory authority

39.1. The Data subject has the right to submit a complaint to the Company if the Data Subject reasonably believes that processing of Personal Data related to him/her is performed in violation of the applicable legal requirements.

39.2. The Data Subject can submit a complaint to the Company's e-mail, it must include name, surname, contact details, relevant information, which would indicate why the Data Subject reasonably believes that the processing of the data related to him/her is performed in violation of the applicable legal requirements. The Data Subject can add other available evidence that justifies the need for such a complaint.

39.3. Upon receipt of a complaint from the Data Subject, the Company confirms receipt of the complaint and indicates the time limit within which the reply will be submitted. Complaints are handled by the Data protection officer or other Employee authorized by the Company. In each case, the deadline for submitting a reply may vary as it directly depends on the extent and complexity of the complaint filed, but the Company will make the maximum effort to provide the response to the Data Subject within the shortest possible time.

39.4. The Company, after examining the complaint, reports the results and actions taken to satisfy the Complaint of the Data Subject, or provides relevant information on what further actions the Data Subject may take if the Complaint from the Data Subject was not satisfied.

39.5. The Data Subject, received Company's answer to Data Subject request or claim and who is disagreeing with the provided answer, has the right to contact the Inspectorate or to claim to the court.

XII. THE BREACHES OF PERSONAL DATA, PROCEDURE FOR DETERMINING AND INVESTIGATING THE BREACHES

40. Procedure for determining and investigating personal data breaches is established by a separate Company's procedure for determining, examining and suspension (elimination) of personal data protection breaches.

XIII. DATA PROTECTION IMPACT ASSESSMENT

41. Where a type of processing using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data.

42. A data protection impact assessment shall in particular be required in these cases of:

42.1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

42.2. processing on a large scale of special categories of data or of Personal Data relating to criminal convictions and offences or related security measures;

42.3. a systematic monitoring of a publicly accessible area on a large scale;

42.4. in other cases, specified by the Supervisory authority.

43. Where necessary, the Company shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

XIV. INTERNATIONAL TRANSFER OF PERSONAL DATA

44. In case the client's personal data is transferred outside the European Union (hereinafter – the EU) and the European Economic Area (hereinafter – the EEA), the Company will take necessary steps to ensure that the client's

data is treated securely and in accordance with this Policy and the Company will ensure that it is protected and transferred in a manner consistent with the legal requirements applicable to the personal data. This can be done in a number of different ways, for example:

44.1. the country to which the Company sends the personal data, a territory or one or more specified sectors within that third country, or the international organization is approved by the European Commission as having an adequate level of protection;

44.2. the recipient has signed or contains in its terms of the service (service agreement) standard data protection clauses which are approved by the European Commission;

44.3. special permission has been obtained from the Supervisory authority.

45. The Company may transfer personal data to a third country by taking other measures if it ensures appropriate safeguards as indicated in the GDPR.

XV. TECHNICAL AND ORGANISATIONAL CONTROLS

46. Annex No. 6 regulates the technical and organisational controls that the Company has put.

XVI. AUTOMATED DECISION MAKING

47. The Company is not using the automated decision-making tools.

XVII. DATA RETENTION

48. Annex No.7 regulates retention periods of the Personal data.

XVIII. DETAILS ABOUT THE VISITS TO THE INTERNET WEBSITE

49. The Company has its own website and during website visit, in order to provide the Data Subject with the full range of services provided by the Company, and in order to improve the quality of the services provided to the Data Subject's computer (device), cookies may be obtained.

50. The information about what kind of cookies and why are used by the Company, the information about the possibility to agree or withdraw the consent regarding the use of cookies and other information are provided in the Company's Cookies Policy, which is published in the website of Company: http://media.intersurgical.com/global/documents/support/our_privacy_and_cookie_policy_INT.pdf

XIX. DATA PROTECTION OFFICER OR PERSON RESPONSIBLE FOR DATA PROTECTION

51. The Company undertakes to appoint a Data protection officer or a person who would be responsible for compliance with Personal Data protection requirements.

XX. RELATIONSHIPS WITH THE SUPERVISORY AUTHORITY

52. The Company, by order of the manager, appoints a person who shall be responsible for the proper implementation of the cooperation with the Supervisory authority in the Company.

53. The Company ensures that when implementing the Personal Data protection policy and in accordance with the applicable regulatory requirements, it cooperates with the Supervisory authority, providing the necessary information, submitting the requested documents, arranging, if necessary, meetings of representatives to discuss cooperation and other issues.

54. Upon submission by the Supervisory authority a query or other type of request in writing or by e-mail, the Company undertakes to submit the requested replies and / or other information without unjustifiable delay. In cases where the response term to the query or other request submitted by the Supervisory authority is not sufficient for the submission of a replay, the Company shall, without unjustifiable delay, contact the Supervisory authority with the request to extend the term.

55. In the case, when the reply or other information submitted by the Company is insufficient for the Supervisory authority, then the Company undertakes to provide additional and / or clarifying information.

56. If a query or other request from the Supervisory authority is received by an Employee who is not authorized to ensure proper cooperation with the Supervisory authority, then the Employee shall inform without unjustifiable delay about that and forward the received query or other request to the responsible person.

XXI. RIGHT TO APPEAL TO THE SUPERVISORY AUTHORITY

56.1. If the Data Subject considers that the processing of his / her Personal Data is being processed in violation of his / her rights and legitimate interests established in the applicable legal acts, the Data Subject may submit a complaint to the Supervisory authority. The complaints procedure of the Supervisory authority can be found here: <https://ico.org.uk/make-a-complaint/>.

XXII. LIABILITY

57. Any breach of the obligations provided in this Policy, Regulation or other legal acts, regulating processing and protection of Personal Data will be considered a significant violation of the employment obligations and may constitute the basis for the termination of the employment agreement due to the fault of the employee.

58. For the Employees who violate the Regulation, or other legal acts, regulating the processing and protection of Personal Data, or this Policy, liability measures provided for in the relevant shall apply.

XXIII. FINAL PROVISIONS

59. These Rules come into effect on the day they are approved and are valid until they are cancelled or replaced.

60. Compliance with the Rules and, if necessary, revision, shall be trusted to the Directors Intersurgical Ltd or a person authorized by them.

61. The modification or invalidity of any of these terms due to the fact that the mandatory provisions of the law have changed or ceased to be valid shall not affect the validity of other terms of the Policy. In such a case, legal acts shall be applied directly instead of the invalid terms.

62. Company will inform Responsible Employees about the Policy by placing the Rules in the Company's electronic information system, about changes of the Rules - by sending the changes of the Rules to Employees by e-mail or by placing the changes of the Rules in the Company's electronic information system (depending on Company's preference).

63. These Rules shall be revised and updated at least once in a calendar year and / or subject to changes in imperative requirements of the law shall be reviewed and amended and / or supplemented. The amendments or supplements to the Rules shall come into effect from the day of their publication, i. e. from the day when the Rules are approved by the order of the Directors of Intersurgical Ltd.

1. This Annex regulates Personal Data processing purposes, legal basis, processed Personal Data (its categories), data receivers and sources of such data of the employees' and/or representatives' of the clients of the Company.
2. Definitions used in this Annex:
 - 2.1. **Personal identification data:** client's employee name, surname, position, signature.
 - 2.2. **Contact details:** correspondence address, telephone, e-mail address.
 - 2.3. **Data related to the performance of the contract** - letters, emails and other forms of communication.
3. Information on Personal data processing purposes, legal basis, processed Personal data categories of Company's partners (natural persons) and employees' and/or representatives' of the clients (legal persons) is listed below:

Purpose of the processing	Legal bases	Categories of personal data
Conclusion of the contract or for performance of measures at client's request prior to the conclusion of the contract	To take the necessary steps before the conclusion of the contract; Complying with obligations applicable to the Company	Basic Personal Data Identification data and other background verification Contact Data Other Personal Data needed (in order to identify the possibility of providing services)
Fulfilment of a contract concluded with client	Performance of a contract / Complying with obligations applicable to the Company	Basic Personal Data Information related to legal requirements Contact Data Other Personal Data provided to Company by or on behalf of client or generated by Company in the course of providing services.
Providing an answer when the Client contact the Company through Company's website or other communication	Consent of the Client	Basic Personal Data Contact Data Other Personal Data provided to Company by or on behalf of client

4. Personal Data of the Company's clients may be transferred to:
 - 4.1. State and municipal institutions, bodies, organizations, and other public administration entities;
 - 4.2. Pre-trial investigation bodies, courts, bailiffs, notaries
 - 4.3. Law, finance, tax, business management, personnel administration, accounting advisors, etc.;
 - 4.4. Group companies of the Company;
 - 4.5. Company's partners;
 - 4.6. Other persons with whom the Company intends to conclude or has concluded a contract(s);
 - 4.7. Other persons who are required access to the data in order to exercise their legal obligations, by a legitimate interest or with the consent of the Data Subject.
5. Personal Data of the Company's client may be collected:
 - 5.1. Directly from the client;
 - 5.2. When it is provided to the Company by a third party which is connected to the Client and/or is dealing with the Company, e.g. business partners, subcontractors, service providers, etc.;

5.3. From publicly available sources – the Company may, e.g. use sources in order to keep contact with the Client using accurate and up to date data that Company already possess for professional networking purposes or for providing our services;

5.4. From other entities in the Company Group or other entities which Company collaborates with.

Annex No. 2 To Intersurgical Personal Data Processing Policy

PERSONAL DATA PROCESSING OF INTERSURGICAL LTD. EMPLOYEES AND CANDIDATES

1. This Annex regulates Personal Data processing purposes, legal basis, processed Personal Data (its categories), data receivers and sources of such data of employees' and candidates of „Intersurgical Ltd“.
2. Definitions used in this Annex:
 - 2.1. **Personal identification data:** name, surname, national insurance number, birth date, gender.
 - 2.2. **Data on qualification and experience:** data on working experience (workplace, working period, duties, responsibilities and (or) achievements), information on Applicant's education (institution of education, period, acquired degree and (or) qualification), information on professional development courses (attended courses, obtained certificates), information on foreign language, informational technology, driving skills and other competences, as well as, other information provided by the candidate in CV, motivational letter and other documents.
 - 2.3. **Data related to the performance of work functions of the Company's employees in the Company:** details of employee's or candidate's qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Company, information about employee's or candidate's criminal record (this is specific for roles where the entry into customer locations is dependent on a clear criminal record check, for instance Sales Staff who require access into hospital departments to meet with end users), information about medical or health conditions, including whether or not an employee or a candidate have a disability for which the Company needs to make reasonable adjustments, details of periods of leave taken by the employee, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave, details of any disciplinary or grievance procedures in which an employee has been involved, including any warnings issued to an employee and related correspondence, assessments of employee's performance, including appraisals, performance reviews and ratings, training the employee have participated in, performance improvement plans and related correspondence, IT usage monitoring information (including registration of the use of internal programs and register of data entry / change);
 - 2.4. **Contact details:** permanent residence address, correspondence address (if different from the permanent place of residence), telephone, e-mail address.
 - 2.5. **Equal opportunities monitoring information:** nationality, gender.
 - 2.6. **Recommendations, employers' feedback:** person recommending or providing feedback about the applicant, his/her contacts, content of the feedback or recommendation.
 - 2.7. **Remuneration data:** information about employee's current level of remuneration, including benefit entitlements.
 - 2.8. **Special categories of personal data:** data on health.
3. Information on Personal data processing purposes, legal basis, processed Personal data categories of Company's employees and/or candidates to an employee is listed below:

Purpose of the processing	Legal bases	Categories of personal data
Execution of recruitment of the applicants	Candidate's consent Complying with obligations applicable to the Company	Personal identification data; Contact details; Data on qualification and experience; Recommendations, employers' feedback; Remuneration data; Health information; Other information.
Administration of applicants' database	Candidate's consent	Personal identification data; Contact details;

Hiring the employee, entering into an employment agreement, it's execution and accounting

Complying with regulations applicable to the Company
Ensuring the legitimate interests of the Company

Data on qualification and experience;
Recommendations, employers' feedback;
Remuneration data;
Other information
Personal identification data;
Contact details;
Data on qualification and experience;
Special categories of personal data*;
Bank account details, specifically the banking address, account name, account number and sort code, transaction data;
National insurance number;
Data related to the performance of work functions of the Company's employees in the Company;
Terms and conditions of the employment relationships;
Other provided information.
* Company collects and processes special categories of personal data only in case and to the extent when it is necessary for recruitment purposes for a particular position and how it is allowed in regard to available legal acts.

The proper fulfilment of the obligations of the Company acting as employer which are set forth by the legal acts

Complying with obligations applicable to the Company

Personal identification data;
Contact details;
Special categories of personal data;
Bank account details, specifically the banking address, account name, account number and sort code, transaction data;
National insurance number;
Emergency contacts;
Data related to the performance of work functions of the Company's employees in the Company;
Terms and conditions of the employment relationships;
Equal opportunities monitoring information;
Other provided information.
* Company collects and processes special categories of personal data only in case and to the extent when it is necessary for

<p>Maintenance of the proper communication with the employees during not working hours</p>	<p>Ensuring the legitimate interests of the Company</p> <p>Employee's consent (when providing personal contact details of the Employee)</p>	<p>recruitment purposes for a particular position and how it is allowed in regard to available legal acts.</p> <p>Name, surname, function; Contact details; Mobile apps for communication.</p>
<p>Enhancing internal communication, team building and employee relations</p>	<p>Ensuring the legitimate interests of the Company</p> <p>Employee's consent (when providing personal contact details of the Employee).</p>	<p>Name, surname, function; Contact details.</p>
<p>Internal investigation/investigation of possible violation of work discipline, violation of legal acts.</p>	<p>Ensuring the legitimate interests of the Company;</p> <p>Complying with obligations applicable to the Company.</p>	<p>Personal identification data; Contact details; Data on qualification and experience; Internet browsing history, location details; Special categories of personal data; Bank account details, specifically the banking address, account name, account number and sort code, transaction data; National insurance number; Data related to the performance of work functions of the Company's Employees in the Company; Other provided information.</p>

4. The Company will also collect personal data about candidates and employee's criminal records checks (only in cases when this data is necessary to verify whether the Employee meets the requirements established by legal acts for the performance of duties or performance of work functions).

5. Personal Data of the Candidates and Company's Employees may be transferred to:

- 5.1. State and municipal institutions, bodies, organizations, and other public administration entities;
- 5.2. Pre-trial investigation bodies, courts, bailiffs, notaries;
- 5.3. Law, finance, tax, business management, personnel administration, accounting advisors, etc.;
- 5.4. Groups companies of the Company;
- 5.5. Other persons with whom the Company intends to conclude or has concluded a contract (s);
- 5.6. Other persons who are required access to the data in order to exercise their legal obligations, by a legitimate interest or with the consent of the applicants to the Company job position and employees.

6. Personal Data of the Candidates and Company's Employees may be received:

- 6.1. Directly from the Candidates or Employees;
- 6.2. Recruitment agencies, employment websites, career-oriented social media websites and (or) other entities providing job search, selection and / or mediation services;
- 6.3. From registers, databases and other sources;

6.4. Former employers of the Candidates or Employees.

Annex No. 3 To Intersurgical Personal Data Processing Policy

DATA PROCESSING OF THE PERSON WHO IS CONTACTING THE COMPANY

1. This Annex regulates Personal Data processing purposes, legal basis, processed Personal Data (its categories), data receivers and sources of such data of person who is contacting the Company.

2. Definitions used in this Annex:

2.1. **Basic personal data** - name, surname, job title.

2.2. **Contact data** - correspondence address, phone number, e-mail address etc.

3. Information on Personal data processing purposes, legal basis, processed Personal data categories of person who is contacting the Company:

Purpose of the processing	Legal bases	Categories of Personal data
Submit a response, to the person who is contacting the Company by submitting a request in the website or other means of communication	Person who is contacting the Company has given a consent; Ensuring the legitimate interests of the Company.	Basic personal data; IP address; Contact data; Another provided information.

4. The Personal Data of the person who is contacting the Company may be transferred to:

4.1. State and municipal institutions, bodies, organizations, and other public administration entities;

4.2. Pre-trial investigation bodies, courts, bailiffs, notaries;

4.3. Group companies of the Company.

5. The Personal Data of the person who is contacting the Company may be collected:

5.1. Directly from of the person who is contacting the Company.

Annex No. 4 To Intersurgical Personal Data Processing Policy

**PERSONAL DATA PROCESSING OF THE PARTNERS AND/OR EMPLOYEES',
 REPRESENTATIVES' OF THE PARTNER OF THE COMPANY**

1. This Annex regulates Personal data processing purposes, legal basis, processed personal data (its categories), data receivers and sources of such data of Company's partners (natural persons) and employees' and/or representatives' of the partners (legal persons).

2. Definitions used in this Annex:

2.1. **Personal identification data:** partner's, employees' and/or representatives' of the partner name, surname, date of birth (age), personal identification code, position, signature.

2.2. **Contact details:** correspondence address, telephone, e-mail address.

2.3. **Data related to the performance of the contract:** letters, emails and other forms of communication, data created using Company's internal IT systems, specifically designed computer programs, data, information, correspondence, media, signed documents contained in such programs related to the Partners or Partners employees', representatives', log of Partner or Partners employees', representatives' actions taken in various applications to which access has been granted by the Company, any other communication of the Employee.

3. Information on Personal data processing purposes, legal basis, processed Personal data categories of Company's partners (natural persons) and employees' and/or representatives' of the partners (legal persons) is listed below:

Purpose of the processing	Legal base	Categories of personal data
Conclusion and execution of the agreements made with partners	Performance of a contract to which partner is a party or in order to take steps at the request of the partner prior to entering into a contract Ensuring the legitimate interests of the Company	Personal identification data; Contact data; Financial data: financial institution account number, transaction data; Data related to the performance of the contract; Other provided information.

4. Personal Data of partners and/or employees', representatives' of the partner of the Company may be transferred to:

- 4.1. State and municipal institutions, bodies, organizations and other public administration entities;
- 4.2. Pre-trial investigation bodies, courts, bailiffs, notaries;
- 4.3. Commercial banks, other financial institutions;
- 4.4. Law, finance, tax, business management, personnel administration, accounting advisors, etc;
- 4.5. Groups companies of the Company;
- 4.6. Other persons with whom the Company intends to conclude or has concluded a contract (s).

5. Personal Data of the Company's partners and/or employees', representatives' of the partner may be collected:

- 5.1. Directly form the partners;
- 5.2. From registers, databases and other sources.

Annex No. 5 To Intersurgical Personal Data Processing Policy

PERSONAL DATA PROCESSING OF COMPANY'S SHAREHOLDERS REPRESENTATIVES

1. This Annex regulates Personal data processing purposes, legal basis, processed personal data (its categories), data receivers and sources of such data of Company's shareholders representatives.
2. Definitions used in this Annex:
 - 2.1. **Personal identification data:** name, surname, former name (if different), personal identification code (where available), date and place of birth, citizenship (s).
 - 2.2. **Contact details:** correspondence address (if different from the permanent place of residence), telephone, e-mail address.
3. Information on Personal data processing purposes, legal basis, processed Personal data categories of Company's shareholders:

Purpose of the processing	Legal basis	Categories of personal data
Proper fulfilment of the Company's duties set out in the legal acts and proper management of the Company	Complying with obligations applicable to the Company	Personal identification data; Contact details; Other provided information.

4. Personal Data of Company's shareholders representatives may be transferred to:
 - 4.1. State and municipal institutions, bodies, organizations and other public administration entities;
 - 4.2. Pre-trial investigation bodies, courts, bailiffs, notaries;
 - 4.3. Commercial banks, other financial institutions;
 - 4.4. Law, finance, tax, business management, personnel administration, accounting advisors, etc;
 - 4.5. Groups companies of the Company;
 - 4.6. Other persons with whom the Company intends to conclude or has concluded a contract (s).
5. Personal Data of the Company's shareholders representatives may be collected:
 - 5.1. Directly form the shareholders;
 - 5.2. From other sources.

Annex No. 6 To Intersurgical Personal Data Processing Policy

TECHNICAL AND ORGANISATIONAL CONTROLS

1. The Company has put the following controls in place to ensure personal data is protected:

1.1. 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:

1.1.1. to ensure there is protection, a process and control of access to personal data;

1.1.2. each user shall use an account that has permissions appropriate to the job they are carrying out at the time;

1.1.3. authorised users can perform only certain procedures or actions with personal data which they had authorisation for;

1.1.4. 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:

1.1.5. must be issued, updated and protected to ensure the confidentiality;

1.1.6. 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;

1.1.7. passwords are changed on a regular basis (no less than once per 6 months);

1.1.8. it must be changed after first log in.

1.2. personal data is protected from unauthorised access to electronic communications;

1.3. 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;

1.4. hardware where the personal data is stored is protected by antivirus software and has up-to-date operating system security patches;

1.5. personal data is pseudonymised as soon as possible.

2. Procedure for granting, cancelling and modifying the access rights or users to process image data:

2.1. the access rights of users are granted, cancelled or modified by approval of the employee's direct manager based on internal procedures;

2.2. 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.

3. 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.

Annex No. 7 To Intersurgical Personal Data Processing Policy

DATA RETENTION PERIODS FOR DIFFERENT PERSONAL DATA CATEGORIES IN INTERSURGICAL LTD.

1. This Annex determines periods for which the personal data that the Company process shall be stored.
2. When determining retention period of personal data, the COMPANY takes into account the purposes of processing personal data and retention periods of personal data which are laid down by legal acts of the United Kingdom. In cases when retention periods of personal data are not laid down by legal acts of the United Kingdom, retention periods are determined by the COMPANY taking into account purposes of processing personal data and following the principle of storage limitation.
3. Data not indicated in this Annex are retained in accordance with legal acts of the United Kingdom.
4. The information on personal data retention periods used by the Company is listed below.

Data retention periods for different personal data categories in the Company:

Category of personal data	Retention period
Data retention period of Intersurgical Ltd. employees and candidates:	
Data of candidates during recruitment campaigns	6 months from the recruitment exercise
Start/Finish Date	50 years after employment ceases
Health and Safety - Risk Assessments	
Accident at work forms	
Name	
Training Records and Certificates	
Appraisal Forms and salary review	6 years after employment ceases
Contract of Employment	
Disciplinary - details and warnings	
Doctors Certificates/Fitness for Work Certificates	
Exit Interview	
File Notes	
Finish Reason	
Flexible Working Requests	
Gender	
Grievance Details	
Job Descriptions	
Maternity/Paternity/Shared Paternity details including MATBI	
Offer Letters	
Recruitment Documents, Application Forms, CV's	
Working days and hours	
Training Agreements	Deleted immediately when employment ceases
Contact Number	
Date of Birth	
Emergency Contact Details	
Medical Questionnaire	

Nationality	
New Employee Form (including bank details and NI)	
References	
Staff Photo	
Right to Work	2 years
Home address	30 days
Nomination Form	
Medical Reports / Assessments	Dependant on circumstances
Video records	30 days
Entry control records	1 year
IT usage, monitoring data	
Data retention periods of Intersurgical Ltd. clients	
Customer (legal entity) data	1 - 10 years after last purchase
Post marketing surveillance and Post-market Clinical Follow-up activities	5 years
Prospective customer (legal entity) data	2 years after last person contact
Data retention periods of Intersurgical Ltd. partners, clients	
Contractor/ supplier data	1 - 10 years after last purchase
Reseller/ distributor data	1 - 10 years after last purchase
Contracts with the partners, clients	6 years after the relationship between you and "Intersurgical Ltd." has ended
Data retention periods of persons contacting Intersurgical Ltd.	
Personal data of persons contacting the Company is processed in order to manage the request received by the Company	6 months after the last day of the communication, if there are no legal requirements to keep them longer
Video surveillance records	30 days
Other data retention periods Intersurgical Ltd.	
Video surveillance records (Intersurgical Ltd.)	30 days
Entry control records	1 year
Registration of the use of internal programs and register of data entry / change	1 year

5. In the cases when the terms of data keeping are indicated in the legislative regulations, the legislative regulations are applied.
6. Personal Data might be stored longer if:
 - 6.1. it is necessary in order for us to defend ourselves against claims, demands or action and exercise our rights;
 - 6.2. there is a reasonable suspicion of an unlawful act that is being investigated;
 - 6.3. Personal Data is necessary for the proper resolution of a dispute/ complaint;
 - 6.4. under another statutory basis.