



SURKOVSKY CENTRE LTD

PRIVACY POLICY

Personal Data Protection Policy

Document Number: POL-001
Document Title: Privacy Policy
Document Classification: Internal Governance Document
Company: Surkovsky Centre Ltd
Registered Office: London, United Kingdom
Version: 1.0
Effective Date: 1 August 2026
Review Date: 1 August 2027
Document Owner: Director
Approved By: Board of Directors
Document Status: Approved

Document Control

Document No.	Version	Issue Date	Review Date
POL-001	1.0	1 August 2026	1 August 2027

Contents

1. Introduction
2. Purpose
3. Scope
4. Definitions
5. Data Protection Principles
6. Lawful Basis for Processing
7. Personal Data Collected
8. Special Category Data
9. Collection of Personal Data
10. Use of Personal Data
11. Disclosure of Personal Data
12. International Data Transfers
13. Data Security



14. Data Retention
 15. Individual Rights
 16. Cookies and Website Technologies
 17. Marketing Communications
 18. Personal Data Breaches
 19. Responsibilities
 20. Monitoring and Review
 21. Related Company Documents
 22. Approval
-

1. Introduction

Surkovsky Centre Ltd is committed to protecting the privacy, confidentiality and security of personal data entrusted to the Company by its students, researchers, employees, clients, partners, contractors, suppliers and other individuals.

The Company recognises that the protection of personal information is fundamental to maintaining trust, safeguarding individual rights and ensuring responsible organisational governance.

This Privacy Policy establishes the principles and organisational framework governing the collection, use, storage, disclosure, retention and protection of personal data processed by Surkovsky Centre Ltd.

The Company is committed to processing personal data fairly, lawfully and transparently while respecting the rights and freedoms of every individual.

All processing activities shall be conducted in accordance with applicable legislation, recognised professional standards and the Company's internal policies.

2. Purpose

The purpose of this Privacy Policy is to establish a comprehensive framework for the lawful and responsible processing of personal data throughout all activities undertaken by Surkovsky Centre Ltd.

This Policy aims to:

- protect the privacy of individuals;
- ensure compliance with UK data protection legislation;
- establish consistent standards for processing personal data;
- promote transparency regarding the Company's data processing activities;



- safeguard confidentiality and information security;
- define organisational responsibilities;
- support accountability;
- reduce data protection risks;
- strengthen stakeholder confidence;
- promote continual improvement in data protection practices.

Personal data protection shall form an integral part of the Company's governance, quality management and information security arrangements.

3. Scope

This Privacy Policy applies to every activity involving the processing of personal data undertaken by Surkovsky Centre Ltd.

It applies to personal data processed in connection with:

- education and training;
- scientific research;
- academic publications;
- consultancy services;
- conferences and seminars;
- professional development programmes;
- recruitment;
- employment;
- supplier relationships;
- contractual management;
- marketing and communications;
- website services;
- administrative activities;
- corporate governance.

This Policy applies to:

- the Director;
- employees;
- researchers;



- lecturers;
- consultants;
- contractors;
- volunteers;
- visiting academics;
- students participating in Company programmes;
- partner organisations where applicable.

This Policy applies irrespective of whether personal data are processed:

- electronically;
- in paper records;
- through online platforms;
- during international activities;
- on Company premises;
- at partner institutions.

Every individual acting on behalf of Surkovsky Centre Ltd shares responsibility for protecting personal data.

4. Definitions

For the purposes of this Policy, the following definitions apply.

Personal Data

Any information relating to an identified or identifiable natural person.

An identifiable person is one who can be identified directly or indirectly, particularly by reference to an identifier such as:

- name;
- identification number;
- location data;
- online identifier;
- or one or more factors specific to the individual's identity.

Processing

Any operation performed on personal data, whether by automated means or otherwise.



Processing includes:

- collection;
- recording;
- organisation;
- storage;
- adaptation;
- retrieval;
- consultation;
- use;
- disclosure;
- transmission;
- restriction;
- erasure;
- destruction.

Data Subject

The individual whose personal data are processed.

Controller

The organisation that determines the purposes and means of processing personal data.

For the purposes of this Policy, Surkovsky Centre Ltd acts as the Data Controller unless otherwise specified.

Processor

A natural or legal person who processes personal data on behalf of the Data Controller.

Personal Data Breach

A security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Special Category Data



Personal data requiring additional protection under applicable legislation, including information concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data;
- health;
- sex life;
- sexual orientation.

5. Data Protection Principles

5.1 General Principle

Surkovsky Centre Ltd shall process all personal data in accordance with the principles established by UK data protection legislation.

The Company shall ensure that personal data are processed responsibly, securely and transparently throughout their entire lifecycle.

5.2 Lawfulness, Fairness and Transparency

Personal data shall be processed:

- lawfully;
- fairly;
- transparently.

Individuals shall receive clear information regarding how their personal data are collected, used and protected.

5.3 Purpose Limitation

Personal data shall be collected only for specified, explicit and legitimate purposes.

Data shall not subsequently be processed in a manner incompatible with those original purposes.



5.4 Data Minimisation

The Company shall collect only personal data that are adequate, relevant and limited to what is necessary for the intended purposes.

Excessive or unnecessary collection of personal information shall be avoided.

5.5 Accuracy

Reasonable steps shall be taken to ensure that personal data remain accurate, complete and up to date.

Inaccurate personal data shall be corrected or erased without undue delay.

5.6 Storage Limitation

Personal data shall be retained only for as long as necessary to fulfil the purposes for which they were collected or as required by applicable legislation.

Secure disposal procedures shall apply following expiry of retention periods.

5.7 Integrity and Confidentiality

Personal data shall be protected against:

- unauthorised access;
- accidental loss;
- unlawful disclosure;
- alteration;
- destruction;
- misuse.

Appropriate technical and organisational measures shall be implemented to maintain confidentiality, integrity and availability of personal information.

5.8 Accountability

Surkovsky Centre Ltd shall be able to demonstrate compliance with all applicable data protection requirements.

The Company shall maintain appropriate records, policies, procedures and governance arrangements supporting accountability in personal data processing.

6. Lawful Basis for Processing



6.1 General Principle

Surkovsky Centre Ltd shall process personal data only where a valid lawful basis exists under applicable UK data protection legislation.

Before commencing any processing activity, the Company shall identify and document the appropriate lawful basis for processing.

The lawful basis shall be proportionate to the nature, purpose and scope of the processing activity.

6.2 Consent

Where processing is based upon consent, the Company shall ensure that consent is:

- freely given;
- specific;
- informed;
- unambiguous;
- capable of being withdrawn at any time.

Individuals shall be informed that withdrawal of consent does not affect the lawfulness of processing undertaken prior to its withdrawal.

6.3 Performance of a Contract

Personal data may be processed where such processing is necessary for the performance of a contract to which the individual is a party or in order to take steps at the request of the individual prior to entering into a contract.

This may include processing relating to:

- educational services;
 - consultancy agreements;
 - research collaboration;
 - employment;
 - supplier contracts;
 - conference registration.
-

6.4 Legal Obligation

The Company may process personal data where processing is necessary for compliance with a legal obligation.



Such obligations may arise under:

- employment legislation;
- taxation legislation;
- company law;
- safeguarding obligations;
- regulatory requirements;
- judicial or law enforcement requests.

6.5 Legitimate Interests

The Company may process personal data where processing is necessary for its legitimate interests, provided that such interests are not overridden by the rights and freedoms of the individual.

Legitimate interests may include:

- organisational administration;
- quality assurance;
- fraud prevention;
- information security;
- risk management;
- business development;
- service improvement;
- protection of Company assets.

Legitimate interests shall be assessed before processing begins.

6.6 Vital Interests

Personal data may be processed where necessary to protect the vital interests of an individual or another person.

Such processing shall normally occur only in exceptional circumstances involving risks to life or serious harm.

6.7 Public Task

Where applicable, personal data may be processed where necessary for the performance of a task carried out in the public interest or in the exercise of official authority.



7. Personal Data Collected

7.1 General Principle

Surkovsky Centre Ltd shall collect only personal data that are necessary, relevant and proportionate for legitimate organisational purposes.

The Company shall avoid collecting excessive or unnecessary personal information.

7.2 Categories of Personal Data

The Company may process the following categories of personal data:

- full name;
- title;
- date of birth;
- postal address;
- email address;
- telephone number;
- nationality;
- educational qualifications;
- employment history;
- professional experience;
- photographs where appropriate;
- identification information;
- correspondence;
- payment information;
- attendance records;
- learning records;
- research participation records.

Processing shall always remain proportionate to the intended purpose.

7.3 Online Information

Where individuals use the Company's website or online services, the Company may collect:

- IP addresses;



- browser information;
- device information;
- website usage information;
- cookies and similar technologies;
- log files;
- online communication records.

Such information shall be collected only where necessary for legitimate organisational purposes.

7.4 Business Information

The Company may process personal data obtained during professional relationships, including information relating to:

- clients;
- suppliers;
- partner organisations;
- contractors;
- consultants;
- conference participants;
- authors;
- reviewers.

Business information shall be processed in accordance with this Policy.

8. Special Category Data

8.1 General Principle

Special Category Data require enhanced protection due to their sensitive nature.

The Company shall process such data only where permitted by applicable legislation and where an appropriate lawful basis and additional processing condition have been identified.

8.2 Types of Special Category Data

Special Category Data may include information concerning:

- racial or ethnic origin;
- religious or philosophical beliefs;



- political opinions;
- trade union membership;
- genetic data;
- biometric data;
- health;
- sex life;
- sexual orientation.

The Company does not routinely collect such information unless it is necessary for legitimate organisational purposes.

8.3 Additional Safeguards

Where Special Category Data are processed, the Company shall implement enhanced safeguards, including:

- restricted access;
- enhanced confidentiality;
- additional security controls;
- staff awareness;
- secure storage;
- appropriate retention arrangements.

Access shall be limited to authorised individuals with a legitimate business need.

8.4 Research Activities

Where research activities involve Special Category Data, processing shall comply with:

- applicable legislation;
- the Research Ethics Policy;
- the Academic Integrity Policy;
- recognised research ethics standards.

Appropriate ethical approval shall be obtained where required.

9. Collection of Personal Data

9.1 General Principle



Personal data shall normally be collected directly from the individual concerned whenever reasonably practicable.

The Company shall collect personal information fairly, transparently and for specified purposes.

9.2 Methods of Collection

Personal data may be collected through:

- application forms;
- registration forms;
- employment processes;
- contractual documentation;
- research participation;
- educational activities;
- conferences;
- correspondence;
- online forms;
- website services;
- telephone communications;
- face-to-face meetings.

The collection method shall remain appropriate to the intended purpose.

9.3 Information Provided to Individuals

When collecting personal data, the Company shall normally provide individuals with information regarding:

- the identity of the Company;
- the purposes of processing;
- the lawful basis for processing;
- data retention;
- individual rights;
- contact details;
- complaint mechanisms.

Information shall be presented in a clear, concise and understandable manner.



9.4 Data Obtained from Third Parties

Where personal data are obtained from third parties, the Company shall ensure that:

- collection is lawful;
- the source is legitimate;
- individuals are informed where required by law;
- processing remains fair and transparent.

Appropriate records shall be maintained regarding the source of the information.

10. Use of Personal Data

10.1 General Principle

Personal data shall be used only for legitimate organisational purposes consistent with the purposes for which they were collected.

Processing shall remain proportionate, lawful and transparent.

10.2 Organisational Purposes

The Company may process personal data for purposes including:

- delivery of educational services;
- scientific research;
- professional training;
- conference administration;
- publication activities;
- consultancy services;
- contractual management;
- recruitment;
- employment administration;
- financial management;
- customer support;
- quality assurance;
- legal compliance;
- organisational governance.



Processing shall remain limited to what is necessary for each purpose.

10.3 Automated Decision-Making

The Company does not normally make decisions based solely upon automated processing that produce legal or similarly significant effects on individuals.

Where such processing becomes necessary, appropriate safeguards shall be implemented in accordance with applicable legislation.

10.4 Accuracy and Updating

The Company shall take reasonable steps to ensure that personal data remain accurate and up to date throughout their lifecycle.

Individuals are encouraged to notify the Company of changes affecting their personal information without undue delay.

11. Disclosure of Personal Data

11.1 General Principle

Surkovsky Centre Ltd shall not disclose personal data to third parties unless such disclosure is lawful, necessary and consistent with the purposes for which the data were originally collected.

Any disclosure of personal data shall be limited to the minimum information necessary and shall be carried out in accordance with applicable legislation and this Policy.

11.2 Disclosure to Service Providers

The Company may disclose personal data to carefully selected service providers where necessary for the delivery of its activities.

Such service providers may include:

- information technology providers;
- website hosting providers;
- cloud service providers;
- payment service providers;
- legal advisers;
- professional consultants;
- auditors;
- training providers.



All service providers processing personal data on behalf of the Company shall be required to implement appropriate technical and organisational measures to protect personal information.

11.3 Disclosure to Partner Organisations

Where necessary, personal data may be shared with partner organisations involved in:

- educational programmes;
- scientific research;
- conferences;
- professional training;
- joint projects;
- contractual cooperation.

Such disclosure shall occur only where an appropriate legal basis exists and suitable safeguards have been implemented.

11.4 Legal Disclosure

The Company may disclose personal data where required by:

- applicable legislation;
- court orders;
- regulatory authorities;
- law enforcement agencies;
- statutory reporting obligations.

Any disclosure shall be limited to information required by law.

11.5 Protection During Disclosure

Whenever personal data are disclosed, the Company shall take reasonable steps to ensure that:

- appropriate confidentiality is maintained;
 - information is transmitted securely;
 - only authorised recipients receive the information;
 - unnecessary personal data are not disclosed.
-

12. International Data Transfers



12.1 General Principle

Personal data may occasionally be transferred outside the United Kingdom where necessary for the Company's educational, research or professional activities.

International transfers shall only take place where appropriate safeguards exist in accordance with applicable data protection legislation.

12.2 Appropriate Safeguards

Safeguards may include:

- adequacy regulations;
- International Data Transfer Agreements (IDTA);
- recognised contractual safeguards;
- approved certification mechanisms;
- other legally recognised transfer mechanisms.

The Company shall ensure that transferred personal data receive an equivalent level of protection.

12.3 International Research Collaboration

International research collaboration may involve the lawful exchange of personal data with partner institutions.

Such transfers shall:

- support legitimate research objectives;
 - comply with applicable legislation;
 - protect the rights of research participants;
 - respect research ethics requirements.
-

12.4 International Conferences and Education

Where educational programmes, conferences or professional activities involve international participants, personal data shall be processed only to the extent necessary for organising and delivering those activities.

13. Data Security

13.1 General Principle



Surkovsky Centre Ltd is committed to protecting personal data against unauthorised access, loss, destruction, alteration or disclosure.

Appropriate technical and organisational measures shall be implemented to maintain the confidentiality, integrity and availability of personal information.

13.2 Technical Security Measures

Security measures may include:

- secure authentication procedures;
- access controls;
- password protection;
- encryption where appropriate;
- secure network infrastructure;
- malware protection;
- system monitoring;
- regular software updates.

Security measures shall be proportionate to identified risks.

13.3 Organisational Security Measures

Organisational measures may include:

- staff training;
- confidentiality obligations;
- restricted access to personal data;
- documented procedures;
- information security policies;
- incident reporting arrangements;
- internal monitoring.

Every individual handling personal data shares responsibility for maintaining information security.

13.4 Access Control

Access to personal data shall be restricted to individuals who require such access for legitimate organisational purposes.



Access rights shall be:

- appropriate;
 - proportionate;
 - regularly reviewed;
 - removed when no longer required.
-

13.5 Physical Security

Where personal data are held in physical form, appropriate safeguards shall be implemented, including:

- secure storage;
 - controlled access;
 - secure disposal;
 - protection against theft or damage.
-

14. Data Retention

14.1 General Principle

Personal data shall not be retained longer than necessary for the purposes for which they were collected.

Retention periods shall reflect:

- legal requirements;
 - regulatory obligations;
 - contractual commitments;
 - operational needs;
 - research requirements where applicable.
-

14.2 Retention Periods

The Company shall establish documented retention periods for different categories of personal data.

Retention schedules shall be reviewed periodically to ensure continuing compliance with applicable legislation.

14.3 Secure Disposal



When personal data are no longer required, they shall be securely disposed of.

Disposal methods may include:

- secure deletion;
- permanent destruction;
- anonymisation where appropriate;
- confidential shredding of paper records.

The Company shall take reasonable steps to prevent unauthorised recovery of disposed information.

15. Individual Rights

15.1 General Principle

Surkovsky Centre Ltd respects and supports the rights of individuals under applicable UK data protection legislation.

Requests relating to individual rights shall be handled promptly, fairly and in accordance with legal requirements.

15.2 Rights of Individuals

Individuals may have the right to:

- access their personal data;
- request correction of inaccurate information;
- request erasure of personal data;
- request restriction of processing;
- object to processing;
- request data portability where applicable;
- withdraw consent where processing is based upon consent;
- lodge a complaint with the relevant supervisory authority.

The exercise of these rights may be subject to legal limitations provided by applicable legislation.

15.3 Requests from Individuals

Requests concerning personal data should normally be submitted in writing.



The Company may request reasonable evidence of identity before responding to protect personal information against unauthorised disclosure.

Requests shall be handled within the timescales established by applicable legislation.

15.4 Complaints

Individuals who believe that their personal data have been processed unlawfully are encouraged to contact the Company in the first instance.

Where appropriate, individuals may also submit complaints to the Information Commissioner's Office (ICO) or another competent supervisory authority.

16. Cookies and Website Technologies

16.1 General Principle

Surkovsky Centre Ltd may use cookies and similar technologies to improve the functionality, security and performance of its website and online services.

Cookies shall be used in a transparent manner and in accordance with applicable legislation, including the Privacy and Electronic Communications Regulations (PECR).

Where required by law, the Company shall obtain the user's consent before placing non-essential cookies on their device.

16.2 Types of Cookies

The Company may use the following categories of cookies:

- strictly necessary cookies;
- functional cookies;
- analytical cookies;
- performance cookies;
- security cookies;
- preference cookies.

Each category of cookies shall be used only for legitimate and specified purposes.

16.3 Cookie Preferences

Website users shall be provided with appropriate mechanisms to manage their cookie preferences.

Users may:



- accept cookies;
- reject non-essential cookies;
- modify previously selected preferences;
- delete cookies through their browser settings.

Changes to cookie preferences may affect the functionality of certain website features.

16.4 Website Analytics

The Company may use website analytics tools to better understand how visitors use its online services.

Analytics information may include:

- pages visited;
- duration of visits;
- navigation behaviour;
- device information;
- browser information;
- general geographic location.

Analytics data shall be used only for improving website performance and user experience.

17. Marketing Communications

17.1 General Principle

Surkovsky Centre Ltd shall conduct marketing communications responsibly, transparently and in accordance with applicable legislation.

Marketing activities shall respect the privacy and communication preferences of individuals.

17.2 Consent for Marketing

Where required by law, marketing communications shall only be sent after obtaining appropriate consent.

Individuals shall have the opportunity to:

- provide consent;
- refuse consent;
- withdraw consent at any time;
- update communication preferences.



Withdrawal of consent shall be respected without unnecessary delay.

17.3 Types of Marketing Communications

Marketing communications may include information regarding:

- educational programmes;
- conferences;
- seminars;
- publications;
- research activities;
- professional development opportunities;
- Company news;
- events.

Marketing communications shall be relevant, accurate and proportionate.

17.4 Opt-Out

Every marketing communication sent electronically shall include a clear mechanism enabling recipients to unsubscribe or opt out from future communications.

Opt-out requests shall be processed promptly.

18. Personal Data Breaches

18.1 General Principle

Surkovsky Centre Ltd is committed to preventing, identifying, reporting and managing personal data breaches in a timely and effective manner.

Every suspected personal data breach shall be treated seriously and investigated without unnecessary delay.

18.2 Identification of Data Breaches

Personal data breaches may include:

- unauthorised disclosure of personal data;
- unauthorised access;
- accidental loss;
- destruction of information;



- alteration of personal data;
- theft of records;
- cyber security incidents;
- accidental transmission to an incorrect recipient.

Every individual acting on behalf of the Company shall report suspected personal data breaches immediately.

18.3 Incident Response

Upon becoming aware of a suspected personal data breach, the Company shall:

- assess the nature of the incident;
- identify affected information;
- contain the incident where possible;
- evaluate potential risks;
- document the incident;
- implement corrective measures;
- notify relevant authorities where required by law;
- communicate with affected individuals where appropriate.

Incident response activities shall be proportionate to the seriousness of the breach.

18.4 Breach Records

The Company shall maintain records of all personal data breaches, including:

- the nature of the breach;
- date of occurrence;
- affected information;
- actions taken;
- lessons learned;
- preventive measures implemented.

Breach records shall support continual improvement of information security and data protection practices.

19. Responsibilities



19.1 Responsibility of the Company

Surkovsky Centre Ltd is responsible for establishing, implementing and maintaining effective arrangements for the protection of personal data.

The Company shall:

- implement this Privacy Policy;
 - promote awareness of data protection requirements;
 - provide appropriate training;
 - establish suitable security measures;
 - monitor compliance;
 - respond appropriately to data protection incidents;
 - promote continual improvement.
-

19.2 Responsibilities of the Director

The Director has overall responsibility for ensuring that personal data are processed lawfully, fairly and securely.

The Director shall:

- oversee implementation of this Policy;
 - promote compliance with applicable legislation;
 - allocate appropriate resources;
 - monitor organisational performance;
 - approve significant data protection improvements;
 - support continual improvement.
-

19.3 Responsibilities of Employees

Every employee shall:

- comply with this Privacy Policy;
- protect personal data;
- maintain confidentiality;
- report suspected data breaches;
- complete relevant training;
- cooperate during investigations;



- support secure information handling.

Employees shall never knowingly misuse personal data.

19.4 Responsibilities of Third Parties

Third parties processing personal data on behalf of the Company shall:

- comply with contractual obligations;
 - implement appropriate security measures;
 - process personal data only as instructed;
 - maintain confidentiality;
 - notify the Company of relevant incidents without undue delay.
-

20. Monitoring and Review

20.1 Monitoring

The effectiveness of this Privacy Policy shall be monitored on a continuing basis.

Monitoring activities may include:

- internal audits;
- compliance reviews;
- security assessments;
- incident reviews;
- management reviews;
- stakeholder feedback.

Monitoring shall support continual improvement of personal data protection.

20.2 Review of this Policy

This Privacy Policy shall normally be reviewed:

- annually;
- following significant legislative changes;
- following major organisational changes;
- following significant data protection incidents;
- following internal audit recommendations;



- where opportunities for improvement are identified.

Revised versions shall replace previous editions upon approval.

21. Related Company Documents

This Privacy Policy shall be read together with:

- GOV-001 Code of Conduct
- GOV-002 Equality, Diversity and Inclusion
- GOV-003 Governance Structure
- QUA-001 Quality Assurance Policy
- EDU-001 Academic Integrity Policy
- RES-001 Research Ethics Policy
- PRO-001 Complaints Procedure
- Information Security Policy
- Records Management Policy
- Data Protection Policy
- Risk Management Policy
- Business Continuity Policy
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy

Where another Company Policy establishes more specific requirements regarding the protection or processing of personal data, that Policy shall take precedence over this Privacy Policy where appropriate.

22. Approval

This Privacy Policy has been approved by the Director of Surkovsky Centre Ltd and shall take effect from the Effective Date specified in this document.

All individuals acting on behalf of the Company are expected to comply with the principles, responsibilities and requirements established within this Policy.

This document shall remain subject to periodic review to ensure its continuing effectiveness, legal compliance and alignment with the Company's strategic objectives.

Document Title: Privacy Policy

Document Number: POL-001

Company: Surkovsky Centre Ltd

Version: 1.0



Approved by: Board of Directors
Authorised by: Director
Surkovsky Centre Ltd

Signature:

Name: Jozef SURKOVSKY

Date: 1 August 2026

Document History

Version	Date	Description	Approved By
1.0	1 August 2026	Initial issue	Director

End of Document