SURKOVSKY CENTRE LTD

DATA PROTECTION POLICY
Personal Data Governance and Protection Framework

Document Number:	POL-002
Document Title:	Data Protection 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-002	1.0	1 August 2026	1 August 2027

Contents

---

1. Introduction

Surkovsky Centre Ltd is committed to protecting personal data and respecting the privacy, rights and freedoms of every individual whose personal information is processed by or on behalf of the Company.

The Company recognises that responsible data protection is an essential element of good corporate governance, organisational integrity, information security and public confidence.

Surkovsky Centre Ltd processes personal data in connection with its educational, scientific, research, professional, administrative and corporate activities.

This Data Protection Policy establishes the organisational framework, principles, responsibilities and controls governing the processing and protection of personal data throughout the Company.

All personal data shall be processed lawfully, fairly, transparently and securely and shall be protected throughout their entire lifecycle.

Data protection shall be integrated into organisational governance, operational management, information security, research, education and decision-making.

---

2. Purpose

The purpose of this Policy is to establish a comprehensive framework for the lawful, responsible and secure processing of personal data by Surkovsky Centre Ltd.

This Policy aims to:

- ensure compliance with applicable data protection legislation;
- protect the rights and freedoms of individuals;
- establish clear responsibilities for personal data processing;
- promote lawful, fair and transparent processing;
- ensure appropriate information security;
- minimise data protection risks;
- establish effective accountability arrangements;
- support responsible data sharing;
- ensure appropriate management of personal data breaches;
- promote data protection by design and by default;
- establish appropriate retention and disposal arrangements;
- strengthen stakeholder confidence;
- support continual improvement in data protection governance.

Protection of personal data shall be regarded as a shared organisational responsibility.

---

3. Scope

This Policy applies to all personal data processed by or on behalf of Surkovsky Centre Ltd.

It applies to personal data processed in connection with:

- education and training;
- scientific research;

- academic activities;
- publications;
- conferences and seminars;
- consultancy services;
- professional development programmes;
- recruitment;
- employment;
- contractual relationships;
- supplier management;
- partnerships;
- marketing and communications;
- website and online services;
- financial administration;
- corporate governance;
- quality assurance;
- complaints and investigations.

This Policy applies to:

- the Director;
- employees;
- researchers;
- lecturers;
- consultants;
- contractors;
- volunteers;
- visiting academics;
- students and programme participants where applicable;
- authorised representatives;
- third parties processing personal data on behalf of the Company.

This Policy applies to personal data regardless of the format or system in which they are processed, including:

- electronic records;

- paper records;
- databases;
- email communications;
- cloud systems;
- online platforms;
- portable devices;
- research records;
- archived records.

Every individual processing personal data on behalf of Surkovsky Centre Ltd shall comply with this Policy.

---

4. Legal and Regulatory Framework

4.1 General Principle

Surkovsky Centre Ltd shall process personal data in accordance with applicable data protection and privacy legislation.

The Company's data protection arrangements shall reflect relevant legal, regulatory and contractual requirements.

4.2 Principal Legislation

This Policy shall be implemented with regard to applicable legislation, including:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018;
- the Privacy and Electronic Communications Regulations (PECR), where applicable;
- other applicable UK legislation relating to privacy, confidentiality and information governance.

The Company shall monitor relevant legislative developments and amend its practices where necessary.

4.3 Regulatory Authority

The Information Commissioner's Office (ICO) is the independent supervisory authority responsible for data protection regulation in the United Kingdom.

Surkovsky Centre Ltd shall cooperate with the ICO where required by applicable legislation.

4.4 Relationship with Other Requirements

Data protection obligations shall be considered together with:

- contractual obligations;
- duties of confidentiality;
- information security requirements;
- research ethics requirements;
- employment obligations;
- corporate governance requirements;
- records management requirements.

Where several requirements apply simultaneously, the Company shall ensure that personal data remain appropriately protected.

---

5. Definitions

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

Personal Data

Any information relating to an identified or identifiable natural person.

An individual may be identifiable directly or indirectly through information such as:

- name;
- identification number;
- contact information;
- location information;
- online identifier;
- professional information;
- other information relating to the individual's identity.

Processing

Any operation or set of operations performed on personal data.

Processing may include:

- collection;
- recording;
- organisation;

- structuring;
- storage;
- adaptation;
- alteration;
- retrieval;
- consultation;
- use;
- disclosure;
- transmission;
- restriction;
- erasure;
- destruction.

Data Subject

An identified or identifiable natural person to whom personal data relate.

Data Controller

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

Surkovsky Centre Ltd may act as a Data Controller where it determines why and how personal data are processed.

Data Processor

A person or organisation processing personal data on behalf of a Data Controller.

Processors shall process personal data only in accordance with applicable legal and contractual requirements.

Joint Controllers

Two or more controllers that jointly determine the purposes and means of processing personal data.

Where Surkovsky Centre Ltd acts as a Joint Controller, appropriate arrangements shall be established to define respective responsibilities.

Special Category Data

Personal data subject to additional legal protection because of their sensitive nature.

Such data may include information relating to:

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

Personal Data Breach

A breach of security leading to accidental or unlawful:

- destruction;
- loss;
- alteration;
- unauthorised disclosure of;
- unauthorised access to personal data.

---

6. Data Protection Principles

6.1 General Principle

Surkovsky Centre Ltd shall ensure that personal data are processed in accordance with the fundamental principles of data protection.

These principles shall apply throughout the complete lifecycle of personal data.

6.2 Lawfulness, Fairness and Transparency

Personal data shall be processed:

- lawfully;
- fairly;

- transparently.

The Company shall identify an appropriate lawful basis for processing and shall provide individuals with appropriate information concerning the use of their personal data.

6.3 Purpose Limitation

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

Personal data shall not be further processed in a manner incompatible with those purposes unless such processing is permitted by applicable legislation.

6.4 Data Minimisation

Personal data shall be:

- adequate;
- relevant;
- limited to what is necessary for the purposes of processing.

The Company shall avoid collecting or retaining unnecessary personal information.

6.5 Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

Reasonable steps shall be taken to correct or erase inaccurate personal data without unnecessary delay.

6.6 Storage Limitation

Personal data shall not be retained in identifiable form for longer than necessary for the purposes for which they are processed, subject to applicable legal, regulatory, contractual, archival or research requirements.

6.7 Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security.

The Company shall implement appropriate technical and organisational measures to protect personal data against:

- unauthorised processing;
- unlawful processing;
- accidental loss;

- destruction;
- damage;
- unauthorised disclosure;
- unauthorised access.

6.8 Accountability

Surkovsky Centre Ltd shall be responsible for compliance with applicable data protection requirements and shall be able to demonstrate such compliance.

Accountability measures may include:

- documented Policies and Procedures;
- records of processing activities where required;
- risk assessments;
- Data Protection Impact Assessments where required;
- staff training;
- security controls;
- contractual safeguards;
- internal reviews;
- incident records;
- appropriate governance arrangements.

Data protection accountability shall form an integral part of the Company's Corporate Governance Framework.

---

7. Roles and Responsibilities in Data Processing

7.1 General Principle

Surkovsky Centre Ltd shall ensure that responsibilities relating to the processing and protection of personal data are clearly defined throughout the organisation.

Every individual who processes personal data on behalf of the Company shall understand their responsibilities and shall process personal data only within the scope of their authorised duties.

7.2 Data Controller

Where Surkovsky Centre Ltd determines the purposes and means of processing personal data, the Company shall act as the Data Controller.

As Data Controller, the Company shall be responsible for:

- identifying appropriate purposes for processing;
- establishing an appropriate lawful basis;
- ensuring transparency;
- protecting individual rights;
- implementing appropriate technical and organisational measures;
- maintaining appropriate documentation;
- selecting appropriate Data Processors;
- managing personal data breaches;
- demonstrating compliance with applicable legislation.

7.3 Data Processor

Where Surkovsky Centre Ltd processes personal data on behalf of another Data Controller, the Company may act as a Data Processor.

In such circumstances, the Company shall:

- process personal data only in accordance with documented instructions;
- maintain confidentiality;
- implement appropriate security measures;
- assist the Data Controller where legally required;
- notify the Data Controller of relevant personal data breaches;
- comply with applicable contractual and legal obligations.

7.4 Joint Controllers

Where Surkovsky Centre Ltd jointly determines the purposes and means of processing with another organisation, the parties may act as Joint Controllers.

Appropriate arrangements shall define their respective responsibilities regarding:

- transparency;
- individual rights;
- information security;
- personal data breaches;
- regulatory compliance;

- communication with Data Subjects.

7.5 Authorised Personnel

Employees, researchers, lecturers, consultants, contractors and other authorised persons shall process personal data only:

- for legitimate organisational purposes;
- within the scope of their responsibilities;
- in accordance with Company Policies and Procedures;
- using approved systems and methods;
- subject to appropriate confidentiality obligations.

Unauthorised access to or use of personal data is prohibited.

---

8. Lawful Basis for Processing

8.1 General Principle

Surkovsky Centre Ltd shall identify an appropriate lawful basis before commencing the processing of personal data.

The lawful basis shall be determined according to the purpose and circumstances of the processing.

The Company shall document the lawful basis where required and provide appropriate information to Data Subjects.

8.2 Lawful Bases

Depending upon the circumstances, processing may be based upon:

- consent;
- performance of a contract;
- compliance with a legal obligation;
- protection of vital interests;
- performance of a task in the public interest or exercise of official authority, where applicable;
- recognised legitimate interests, where applicable;
- legitimate interests pursued by the Company or a third party, where appropriate.

No lawful basis shall automatically take precedence over another. The appropriate basis shall be determined according to the particular processing activity.

8.3 Consent

Where processing is based upon consent, consent shall be:

- freely given;
- specific;
- informed;
- unambiguous;
- demonstrated through a clear affirmative action.

The Company shall maintain appropriate evidence of consent where necessary.

Individuals shall be able to withdraw consent at any time, and withdrawal shall be as straightforward as providing consent.

Withdrawal shall not affect the lawfulness of processing carried out before consent was withdrawn.

8.4 Contract

Personal data may be processed where processing is necessary:

- for the performance of a contract with the Data Subject; or
- to take steps at the request of the Data Subject before entering into a contract.

Contractual processing shall be limited to information genuinely necessary for the relevant contractual purpose.

8.5 Legal Obligation

Personal data may be processed where necessary for compliance with a legal obligation applicable to the Company.

The Company shall identify the relevant legal obligation where appropriate and shall not rely upon this basis for purely contractual obligations.

8.6 Vital Interests

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

This lawful basis shall normally apply only where processing is necessary to protect life or prevent serious harm.

8.7 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.

The Company shall rely upon this basis only where the processing is supported by an appropriate basis in law.

8.8 Recognised Legitimate Interests

Where permitted by applicable legislation, the Company may rely upon a recognised legitimate interest where the processing is necessary for a purpose specifically recognised by law.

The Company shall ensure that the statutory conditions applicable to the relevant recognised legitimate interest are satisfied.

8.9 Legitimate Interests

The Company may process personal data where:

- a legitimate interest exists;
- processing is necessary to achieve that interest; and
- the interests, rights and freedoms of the Data Subject do not override that interest.

Where appropriate, the Company shall undertake and document a Legitimate Interests Assessment.

---

9. Special Category Data and Criminal Offence Data

9.1 General Principle

Surkovsky Centre Ltd recognises that Special Category Data and Criminal Offence Data require additional safeguards.

Such information shall be processed only where the applicable legal requirements are satisfied and appropriate organisational and technical safeguards are implemented.

9.2 Special Category Data

Special Category Data may include personal data revealing or concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;

- genetic data;
- biometric data used for identification;
- health;
- sex life;
- sexual orientation.

The Company shall not process Special Category Data unless an appropriate lawful basis and an applicable additional condition for processing have been identified.

9.3 Conditions for Processing Special Category Data

Depending upon the circumstances, processing may be permitted on grounds including:

- explicit consent;
- employment, social security and social protection obligations;
- vital interests;
- information manifestly made public by the Data Subject;
- establishment, exercise or defence of legal claims;
- substantial public interest;
- health or social care;
- public health;
- archiving, scientific or historical research or statistical purposes.

Where required, the Company shall also satisfy applicable conditions under the Data Protection Act 2018.

9.4 Appropriate Policy Document

Where required by applicable legislation, Surkovsky Centre Ltd shall maintain an Appropriate Policy Document supporting the processing of Special Category Data or Criminal Offence Data.

Such documentation shall describe relevant safeguards, retention arrangements and compliance with data protection principles.

9.5 Criminal Offence Data

Personal data relating to criminal convictions, offences, allegations, investigations or related security measures shall receive additional protection.

The Company shall process Criminal Offence Data only where:

- an appropriate lawful basis has been identified; and
- the processing is under official authority or an applicable condition under UK law has been satisfied.

The Company shall not maintain a comprehensive register of criminal convictions unless legally authorised to do so.

9.6 Additional Safeguards

Where Special Category Data or Criminal Offence Data are processed, additional safeguards may include:

- restricted access;
- enhanced confidentiality controls;
- encryption;
- secure storage;
- documented authorisation;
- additional staff training;
- Data Protection Impact Assessments;
- defined retention periods;
- secure disposal.

The level of protection shall reflect the risks associated with the processing.

---

10. Collection and Use of Personal Data

10.1 General Principle

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

The Company shall collect only information that is adequate, relevant and necessary for those purposes.

10.2 Collection of Personal Data

Personal data may be collected:

- directly from Data Subjects;
- through application and registration forms;
- through contractual relationships;

- through employment and recruitment processes;
- through educational activities;
- through research activities;
- through conferences and events;
- through the Company's website and online services;
- from partner organisations;
- from publicly available sources;
- from other lawful third-party sources.

Collection methods shall be fair, lawful and transparent.

10.3 Use of Personal Data

Personal data may be used for legitimate purposes including:

- providing educational services;
- conducting scientific research;
- administering academic activities;
- managing publications;
- organising conferences and events;
- providing consultancy services;
- managing contracts;
- recruitment and employment administration;
- financial administration;
- communicating with stakeholders;
- quality assurance;
- risk management;
- information security;
- legal and regulatory compliance;
- corporate governance.

Personal data shall not be used for incompatible purposes unless such further processing is permitted by applicable legislation.

10.4 Data Minimisation

Before collecting personal data, the Company shall consider whether each category of information is genuinely necessary.

Where possible, unnecessary personal identifiers shall be avoided or removed.

10.5 Accuracy

Reasonable steps shall be taken to ensure that personal data are accurate and, where necessary, kept up to date.

Individuals shall be encouraged to inform the Company where information requires correction or updating.

---

11. Transparency and Privacy Information

11.1 General Principle

Surkovsky Centre Ltd shall provide individuals with clear and accessible information regarding the processing of their personal data.

Transparency shall form an essential element of fair and lawful processing.

11.2 Privacy Information

Where required, individuals shall be informed about matters including:

- the identity and contact details of the Data Controller;
- purposes of processing;
- lawful bases for processing;
- categories of personal data where appropriate;
- recipients or categories of recipients;
- international transfers where applicable;
- retention periods or criteria used to determine them;
- individual rights;
- the right to withdraw consent where applicable;
- the right to complain to the supervisory authority;
- automated decision-making where applicable.

11.3 Method of Providing Information

Privacy information may be provided through:

- the Company's Privacy Policy;
- specific privacy notices;
- application forms;
- research participant information;
- employment documentation;
- contractual documentation;
- website notices;
- electronic communications.

Information shall be concise, transparent, intelligible and accessible.

11.4 Changes to Processing

Where the purpose or nature of processing changes materially, the Company shall consider whether updated privacy information is required.

Individuals shall be informed of relevant changes where required by applicable legislation.

---

12. Data Subject Rights

12.1 General Principle

Surkovsky Centre Ltd shall respect and facilitate the rights of Data Subjects under applicable data protection legislation.

Requests shall be handled fairly, securely and within applicable statutory timescales.

12.2 Right to be Informed

Individuals have the right to receive appropriate information about how their personal data are processed.

The Company shall provide such information in accordance with applicable transparency requirements.

12.3 Right of Access

Individuals may request confirmation as to whether their personal data are being processed and may request access to their personal data and associated information.

The Company shall verify identity where reasonably necessary before disclosing personal information.

12.4 Right to Rectification

Individuals may request correction of inaccurate personal data and completion of incomplete personal data where appropriate.

The Company shall take reasonable steps to ensure that corrections are implemented without undue delay.

12.5 Right to Erasure

Individuals may request erasure of personal data in circumstances provided by applicable legislation.

The right to erasure is not absolute and may be restricted where continued processing is legally permitted or required.

12.6 Right to Restriction of Processing

Individuals may request restriction of processing in circumstances provided by applicable legislation.

Where processing is restricted, personal data shall normally remain stored but shall not otherwise be processed except where legally permitted.

12.7 Right to Data Portability

Where applicable, individuals may have the right to receive personal data they have provided to the Company in a structured, commonly used and machine-readable format.

They may also have the right to request transmission of such data to another controller where technically feasible and legally applicable.

12.8 Right to Object

Individuals may have the right to object to processing based upon particular lawful bases or purposes.

The Company shall assess objections in accordance with applicable legislation and shall cease processing where legally required.

12.9 Rights Relating to Automated Decision-Making

Where applicable, individuals shall be protected against certain decisions based solely upon automated processing, including profiling, that produce legal or similarly significant effects.

Where such processing is permitted, appropriate safeguards shall be implemented.

12.10 Withdrawal of Consent

Where processing is based upon consent, individuals may withdraw their consent at any time.

Withdrawal shall not affect the lawfulness of processing undertaken before withdrawal.

12.11 Complaints

Individuals who believe that their personal data have been processed in breach of applicable data protection requirements may raise the matter with Surkovsky Centre Ltd.

Individuals also have the right to lodge a complaint with the competent supervisory authority.

The Company shall cooperate appropriately with the Information Commissioner's Office where required.

---

13. Data Protection by Design and by Default

13.1 General Principle

Surkovsky Centre Ltd shall integrate data protection considerations into the design, development and implementation of organisational processes, systems, services, projects and activities involving personal data.

Data protection shall be considered from the earliest stages of planning and throughout the entire lifecycle of processing.

13.2 Data Protection by Design

When designing or introducing new processing activities, the Company shall consider:

- the nature of the personal data;
- the purposes of processing;
- the volume of personal data involved;
- the categories of Data Subjects;
- potential risks to individuals;
- appropriate technical and organisational safeguards;
- data minimisation;
- access controls;
- retention requirements;
- information security;

- individual rights.

Appropriate safeguards shall be incorporated into relevant processes wherever practicable.

13.3 Data Protection by Default

The Company shall ensure that, by default, only personal data necessary for each specific purpose are processed.

Default arrangements shall take account of:

- the amount of personal data collected;
- the extent of processing;
- the period of storage;
- accessibility of information;
- authorised access.

Personal data shall not be made accessible to an indefinite number of persons without appropriate justification.

13.4 New Systems and Projects

Data protection requirements shall be considered when:

- introducing new information systems;
- developing online services;
- establishing new research projects;
- introducing educational platforms;
- procuring software or cloud services;
- developing databases;
- establishing new partnerships;
- changing existing processing activities.

Where appropriate, privacy and security requirements shall form part of project planning and procurement.

---

14. Data Protection Impact Assessments

14.1 General Principle

Surkovsky Centre Ltd shall conduct a Data Protection Impact Assessment (DPIA) where processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA shall be undertaken before the relevant high-risk processing begins.

14.2 Circumstances Requiring Assessment

A DPIA may be required where processing involves:

- new technologies;
- systematic and extensive evaluation of individuals;
- large-scale processing of Special Category Data;
- large-scale processing of Criminal Offence Data;
- systematic monitoring;
- innovative processing techniques;
- significant profiling;
- combining data from multiple sources;
- processing involving vulnerable individuals;
- other activities presenting potentially high risks.

The need for a DPIA shall be assessed according to the nature, scope, context and purposes of processing.

14.3 DPIA Process

A DPIA should, where appropriate:

- describe the proposed processing;
- identify the purposes of processing;
- assess necessity and proportionality;
- identify risks to individuals;
- assess the likelihood and severity of identified risks;
- identify measures to reduce or manage risks;
- document decisions and safeguards;
- establish responsibilities for implementation.

14.4 Review of DPIAs

DPIAs shall be reviewed where:

- the nature of processing changes;

- new technologies are introduced;
- significant new risks are identified;
- the purpose or scope of processing changes;
- an incident indicates that existing safeguards may be insufficient.

Where high residual risk cannot be appropriately mitigated, the Company shall take any further steps required under applicable legislation before commencing the processing.

---

15. Data Sharing and Disclosure

15.1 General Principle

Personal data shall be shared or disclosed only where there is a legitimate and lawful reason for doing so.

The Company shall ensure that data sharing is:

- lawful;
- fair;
- transparent;
- necessary;
- proportionate;
- secure.

Only the minimum personal data necessary for the relevant purpose shall be disclosed.

15.2 Internal Data Sharing

Personal data may be shared internally where necessary for legitimate organisational activities.

Internal access shall be limited according to:

- organisational responsibilities;
- operational requirements;
- authorised access rights;
- confidentiality requirements;
- the principle of least privilege.

15.3 External Data Sharing

Personal data may be shared with external organisations where necessary, including:

- educational partners;
- research institutions;
- professional advisers;
- contractors;
- service providers;
- suppliers;
- regulatory authorities;
- public authorities;
- law enforcement authorities where legally required.

The Company shall establish an appropriate lawful basis before disclosure.

15.4 Data Sharing Agreements

Where appropriate, formal Data Sharing Agreements shall be established.

Such agreements may define:

- the purpose of sharing;
- categories of personal data;
- responsibilities of the parties;
- lawful bases;
- security requirements;
- retention arrangements;
- procedures for individual rights;
- breach management arrangements;
- restrictions on further disclosure.

15.5 Disclosure Required by Law

Personal data may be disclosed where required by:

- legislation;
- court order;
- regulatory requirement;
- lawful request from a competent authority;

- other binding legal obligation.

The Company shall verify the legitimacy and scope of such requests where appropriate.

---

16. Data Processors and Third Parties

16.1 General Principle

Where Surkovsky Centre Ltd appoints another organisation to process personal data on its behalf, appropriate safeguards shall be established before processing begins.

Processors shall provide sufficient guarantees regarding the implementation of appropriate technical and organisational measures.

16.2 Selection of Processors

When selecting a Data Processor, the Company may consider:

- information security arrangements;
- data protection compliance;
- technical capabilities;
- confidentiality arrangements;
- incident management procedures;
- business continuity arrangements;
- location of processing;
- use of sub-processors;
- ability to support individual rights.

16.3 Processor Contracts

Processing by a Data Processor shall be governed by an appropriate written contract or other legally binding arrangement where required.

Such arrangements shall address applicable requirements concerning:

- subject matter and duration of processing;
- nature and purpose of processing;
- categories of personal data;
- categories of Data Subjects;
- confidentiality;
- security;

- sub-processors;
- assistance with individual rights;
- personal data breaches;
- deletion or return of personal data;
- audits and compliance information.

16.4 Sub-Processors

A Processor shall not appoint a Sub-Processor contrary to applicable contractual or legal requirements.

Appropriate data protection obligations shall apply throughout the processing chain.

16.5 Monitoring Third Parties

The Company may periodically review third-party processing arrangements to ensure continuing compliance with contractual, security and data protection requirements.

---

17. International Data Transfers

17.1 General Principle

Surkovsky Centre Ltd may engage in international educational, scientific, research, professional and commercial activities that require personal data to be transferred outside the United Kingdom.

International transfers shall take place only where permitted under applicable UK data protection legislation.

17.2 Adequacy

Personal data may be transferred to a country, territory, sector or organisation covered by applicable UK adequacy regulations where the relevant legal requirements are satisfied.

17.3 Appropriate Safeguards

Where an applicable adequacy arrangement is not available, the Company shall consider whether an appropriate lawful safeguard can be used.

Such safeguards may include:

- the UK International Data Transfer Agreement;
- an applicable UK Addendum to recognised contractual clauses;

- binding corporate rules where applicable;
- legally recognised certification mechanisms;
- legally recognised codes of conduct;
- other safeguards permitted under applicable legislation.

17.4 Assessment of International Transfers

Where required, the Company shall assess the circumstances and risks associated with an international transfer and determine whether the proposed safeguards provide appropriate protection.

Additional technical, contractual or organisational safeguards shall be implemented where necessary.

17.5 Exceptional Transfers

In limited circumstances, international transfers may take place under an applicable legal exception or derogation.

Such exceptions shall not be used routinely where a more appropriate transfer mechanism is available.

17.6 International Research and Education

International research collaborations, educational programmes, conferences and professional partnerships may involve transfers of personal data.

Such transfers shall be appropriately documented and shall respect:

- applicable data protection legislation;
- confidentiality obligations;
- research ethics;
- contractual requirements;
- individual rights;
- information security requirements.

---

18. Data Security

18.1 General Principle

Surkovsky Centre Ltd shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Security measures shall reflect:

- the nature of personal data;
- the scope and context of processing;
- the purposes of processing;
- available technology;
- implementation considerations;
- the likelihood and severity of risks to individuals.

18.2 Technical Measures

Appropriate technical measures may include:

- access controls;
- secure authentication;
- password protection;
- encryption;
- pseudonymisation;
- network security;
- malware protection;
- software updates;
- secure backups;
- logging and monitoring;
- secure configuration of systems.

18.3 Organisational Measures

Appropriate organisational measures may include:

- defined responsibilities;
- confidentiality obligations;
- staff training;
- access management;

- documented security procedures;
- incident reporting;
- supplier management;
- secure records management;
- periodic security reviews.

18.4 Access to Personal Data

Access to personal data shall be granted only to authorised individuals who require such access for legitimate purposes.

Access permissions shall be:

- proportionate to responsibilities;
- appropriately authorised;
- periodically reviewed;
- amended when responsibilities change;
- withdrawn when no longer required.

18.5 Confidentiality

Individuals authorised to process personal data shall maintain appropriate confidentiality.

Personal data shall not be disclosed or discussed with unauthorised persons.

Confidentiality obligations may continue after employment, contractual engagement or other association with the Company has ended.

18.6 Remote Working and Portable Devices

Where personal data are processed remotely or using portable devices, appropriate safeguards shall be applied.

These may include:

- secure connections;
- device authentication;
- encryption;
- physical protection of devices;
- restrictions on local storage;
- secure disposal of temporary records;

- protection against unauthorised observation or access.

---

19. Data Retention and Disposal

19.1 General Principle

Personal data shall be retained only for as long as necessary for the purposes for which they are processed, subject to applicable legal, regulatory, contractual, research or archival requirements.

The Company shall avoid indefinite retention without legitimate justification.

19.2 Retention Criteria

Retention periods may be determined according to:

- the purpose of processing;
- applicable legal requirements;
- contractual requirements;
- limitation periods;
- regulatory obligations;
- research requirements;
- operational requirements;
- potential legal claims;
- legitimate archival requirements.

19.3 Retention Schedule

Where appropriate, the Company shall maintain a Data Retention Schedule identifying retention periods for relevant categories of records and personal data.

Retention arrangements shall be periodically reviewed.

19.4 Research Data

Personal data associated with scientific or academic research may require specific retention arrangements.

Research records shall be retained in accordance with:

- applicable legislation;
- research ethics requirements;

- contractual commitments;
- funding requirements where applicable;
- scientific integrity requirements;
- the Company's Research Ethics Policy.

Where identifiable personal data are no longer necessary, anonymisation should be considered where appropriate.

19.5 Secure Disposal

Personal data that are no longer required shall be securely:

- deleted;
- destroyed;
- anonymised;
- otherwise rendered inaccessible or irrecoverable.

Paper records containing personal data shall be destroyed using appropriate confidential disposal methods.

Electronic records shall be deleted using methods appropriate to the sensitivity of the information and the relevant technology.

---

20. Personal Data Breaches

20.1 General Principle

Surkovsky Centre Ltd shall maintain arrangements for the prompt identification, assessment, containment, documentation and management of Personal Data Breaches.

All suspected or confirmed breaches shall be treated seriously.

20.2 Reporting of Suspected Breaches

Employees, researchers, contractors and other authorised persons shall report suspected Personal Data Breaches immediately through the appropriate internal reporting arrangements.

Individuals shall not conceal, ignore or independently investigate significant incidents without appropriate authorisation.

20.3 Initial Response

Following notification of a suspected breach, the Company shall take appropriate steps to:

- contain the incident;

- prevent further unauthorised access or disclosure;
- identify affected systems and information;
- preserve relevant evidence;
- determine the circumstances of the incident;
- assess potential consequences.

20.4 Risk Assessment

The Company shall assess the potential risk to the rights and freedoms of affected individuals.

The assessment may consider:

- the type of personal data involved;
- the sensitivity of the information;
- the number of individuals affected;
- potential consequences;
- whether information was encrypted or otherwise protected;
- the likelihood of misuse;
- measures available to reduce harm.

20.5 Regulatory Notification

Where a Personal Data Breach is notifiable under applicable legislation, Surkovsky Centre Ltd shall notify the Information Commissioner's Office without undue delay and, where feasible, within the applicable statutory period.

The Company shall document the reasons for its notification decision.

20.6 Communication with Affected Individuals

Where a Personal Data Breach is likely to result in a high risk to the rights and freedoms of individuals, affected Data Subjects shall be informed where required by applicable legislation.

Communications shall provide appropriate information concerning:

- the nature of the breach;
- potential consequences;
- measures taken or proposed;
- steps individuals may take to protect themselves;
- relevant contact information.

20.7 Breach Records

The Company shall maintain appropriate records of Personal Data Breaches.

Records may include:

- circumstances of the breach;
- affected data;
- consequences;
- risk assessment;
- containment measures;
- notification decisions;
- remedial actions;
- lessons learned.

Breach information shall be used to strengthen future data protection and information security arrangements.

---

21. Records of Processing and Accountability

21.1 General Principle

Surkovsky Centre Ltd shall maintain appropriate documentation to demonstrate compliance with applicable data protection requirements.

The Company recognises accountability as a fundamental element of responsible data governance.

21.2 Records of Processing Activities

Where required by applicable legislation, the Company shall maintain appropriate Records of Processing Activities.

Such records may include:

- purposes of processing;
- categories of Data Subjects;
- categories of personal data;
- categories of recipients;
- international transfers;
- applicable safeguards;

- retention arrangements;
- general descriptions of technical and organisational security measures.

Records shall be maintained in an appropriate and accessible form.

21.3 Documentation

Data protection documentation may include:

- Policies and Procedures;
- privacy notices;
- Records of Processing Activities;
- Data Protection Impact Assessments;
- Legitimate Interests Assessments;
- consent records;
- Data Sharing Agreements;
- Processor agreements;
- international transfer documentation;
- personal data breach records;
- individual rights request records;
- training records;
- audit and review records.

Documentation shall be proportionate to the nature, scale and risks of the Company's processing activities.

21.4 Demonstrating Compliance

The Company shall be able to demonstrate that appropriate measures have been implemented to support compliance with data protection requirements.

Evidence of compliance may include:

- approved Policies;
- documented decisions;
- risk assessments;
- security controls;
- contractual arrangements;

- training records;
- internal reviews;
- corrective actions;
- management oversight.

21.5 Review of Processing Activities

Processing activities shall be reviewed where appropriate to ensure that:

- purposes remain legitimate;
- lawful bases remain appropriate;
- personal data remain necessary;
- retention periods remain justified;
- security measures remain effective;
- privacy information remains accurate;
- risks remain appropriately controlled.

---

22. Training and Awareness

22.1 General Principle

Surkovsky Centre Ltd shall promote an organisational culture in which personal data are handled responsibly and securely.

Individuals whose roles involve access to personal data shall receive appropriate information, guidance or training according to their responsibilities.

22.2 Data Protection Awareness

Relevant personnel shall be made aware of:

- fundamental data protection principles;
- confidentiality requirements;
- secure handling of personal data;
- individual rights;
- information security responsibilities;
- personal data breach reporting;
- appropriate use of Company systems;

- consequences of non-compliance.

22.3 Role-Specific Training

Additional training may be provided where responsibilities involve:

- significant volumes of personal data;
- Special Category Data;
- Criminal Offence Data;
- research participant information;
- recruitment or employment records;
- information technology administration;
- handling individual rights requests;
- management of Personal Data Breaches;
- international transfers;
- high-risk processing.

22.4 Training Records

Where appropriate, the Company shall maintain records of data protection training and awareness activities.

Training requirements shall be reviewed periodically and updated in response to:

- legislative developments;
- organisational changes;
- new technologies;
- identified risks;
- security incidents;
- audit findings;
- changes in processing activities.

---

23. Responsibilities

23.1 Overall Responsibility

Surkovsky Centre Ltd has overall responsibility for ensuring that personal data processed by or on behalf of the Company are handled in accordance with applicable data protection requirements.

Responsibility for data protection shall form part of the Company's governance and management framework.

23.2 Responsibilities of the Director

The Director has overall responsibility for oversight of the Company's data protection arrangements.

The Director shall, as appropriate:

- approve Data Protection Policies;
- oversee implementation of data protection requirements;
- promote a culture of responsible information handling;
- ensure appropriate organisational measures are established;
- oversee significant data protection risks;
- consider significant Personal Data Breaches;
- support appropriate training and awareness;
- ensure that material compliance issues are addressed;
- approve significant corrective actions;
- support continual improvement.

23.3 Data Protection Officer

Surkovsky Centre Ltd shall appoint a Data Protection Officer where such appointment is required by applicable legislation.

Where a statutory Data Protection Officer is not required, the Company may assign appropriate data protection responsibilities to a designated individual or function without representing that role as a statutory Data Protection Officer.

23.4 Employees and Other Authorised Persons

Every employee, researcher, lecturer, consultant, contractor and other authorised person processing personal data on behalf of the Company shall:

- comply with this Policy;
- process personal data only for authorised purposes;
- maintain confidentiality;
- use appropriate security measures;
- follow relevant Procedures;

- report suspected Personal Data Breaches;
- cooperate with compliance reviews and investigations;
- complete relevant training where required;
- protect personal data from unauthorised access, disclosure, alteration or loss.

23.5 Managers and Project Leaders

Individuals responsible for projects, programmes or organisational activities involving personal data shall ensure that data protection requirements are considered throughout those activities.

Responsibilities may include:

- identifying relevant processing activities;
- ensuring appropriate lawful bases;
- considering data minimisation;
- identifying potential risks;
- ensuring appropriate access controls;
- supporting DPIAs where required;
- ensuring appropriate third-party arrangements;
- monitoring compliance within their area of responsibility.

23.6 Third Parties

Third parties processing personal data for or in cooperation with the Company shall comply with applicable:

- legal requirements;
- contractual obligations;
- confidentiality requirements;
- security requirements;
- data protection instructions.

Failure to meet required standards may result in review, restriction or termination of the relevant relationship.

---

24. Monitoring and Compliance

24.1 General Principle

Compliance with this Data Protection Policy shall be monitored on an ongoing and proportionate basis.

Monitoring shall support the identification of risks, weaknesses, non-compliance and opportunities for improvement.

24.2 Monitoring Activities

Monitoring may include:

- internal reviews;
- audits;
- security assessments;
- review of processing records;
- review of Data Protection Impact Assessments;
- review of Personal Data Breaches;
- review of individual rights requests;
- review of third-party arrangements;
- examination of complaints;
- management review.

The extent and frequency of monitoring shall reflect the nature and risks of relevant processing activities.

24.3 Non-Compliance

Suspected or identified non-compliance shall be assessed and addressed appropriately.

Corrective measures may include:

- clarification of responsibilities;
- additional training;
- amendment of procedures;
- improvement of security controls;
- restriction of access;
- review of processing activities;
- revision of contractual arrangements;
- disciplinary action where appropriate;
- other proportionate remedial measures.

24.4 Reporting Significant Issues

Significant data protection risks, incidents or compliance failures shall be reported to the Director.

Where required by law, relevant matters shall also be reported to the Information Commissioner's Office or another competent authority.

24.5 Continual Improvement

The Company shall use information obtained through:

- audits;
- incidents;
- complaints;
- risk assessments;
- regulatory developments;
- staff feedback;
- operational experience;

to improve its data protection arrangements.

Data protection shall be treated as an evolving governance responsibility rather than a one-time compliance exercise.

---

25. Policy Review

25.1 Regular Review

This Data Protection Policy shall normally be reviewed at least annually.

The scheduled Review Date is specified in the document control information.

25.2 Additional Review

An additional review may be undertaken following:

- significant changes in data protection legislation;
- regulatory guidance or enforcement developments;
- significant organisational changes;
- introduction of new technologies;
- commencement of significant new processing activities;

- significant Personal Data Breaches;
- audit findings;
- material changes in organisational risk;
- identified opportunities for improvement.

25.3 Amendments

Amendments to this Policy shall be appropriately documented and approved.

Where material amendments affect organisational responsibilities or processing practices, relevant individuals shall be informed.

Previous versions shall be managed in accordance with the Company's document control arrangements.

---

26. Related Company Documents

This Data Protection Policy shall be read together with relevant Company documents, including:

- POL-001 Privacy Policy;
- 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 Retention Policy;
- Cookie Policy;
- Data Breach Response Procedure;
- Subject Access Request Procedure;
- Risk Management Policy;
- Business Continuity Policy;
- Whistleblowing Policy;

- Anti-Bribery and Corruption Policy.

Where another Company document establishes more specific requirements for a particular processing activity, those requirements shall be applied together with this Policy.

---

27. Approval

This Data Protection 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 Policy shall remain subject to periodic review to ensure its continuing effectiveness, legal compliance and alignment with the Company's governance, educational, research and organisational objectives.

Document Title: Data Protection Policy
Document Number: POL-002
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