UK Society for Behaviour Analysis

UK-SBA

DATA PROTECTION

POLICY & PROCEDURES

Committee responsible:	GDPR Group/DPO	**Date approved:**	April 2024
Approved by:	UK-SBA Board	**Date of last review:**	March 2026
Version Number:	2	**Date of next review:**	March 2028

TABLE OF CONTENTS

1. Purpose....3
2. Definitions....3
3. Scope....4
4. The Policy....4
5. Complaints....6
6. Integrated Procedures....7
   - 6.1 Fair, Lawful and Transparent Processing....7
   - 6.2 Consent....9
   - 6.3 Data Collection....9
   - 6.4 Individual Rights of Data Subjects....9
   - 6.5 Subject Access Requests....9
   - 6.6 Data Accuracy....10
   - 6.7 Retention of Data....10
   - 6.8 Data Storage and Security....10
   - 6.9 Data Sharing....11
   - 6.10 Data Breach....11
   - 6.11 Data Protection Impact Assessments....11
7. Implementation....12
   - 7.1 Distribution....12
   - 7.2 Training....12
   - 7.3 Records & Confidentiality....12
   - 7.4 Roles & Responsibilities....12
8. Review....14
9. Contact....14

1. Purpose

1.1 This policy and related procedures outline how the UK-SBA meets its obligation to comply with UK GDPR.

1.2 The policy ensures that UK-SBA:

Complies with UK GDPR and follows good practice

Protects the rights of employees, directors, business contacts, members, customers, and partners

Is open about how it stores and processes individuals' data

Protects itself from the risks of a data breach

2. Definitions

2.1 'UK-SBA' is an acronym for UK Society for Behaviour Analysis

2.2 'personal data', means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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, physiological, genetic, mental, economic, cultural or social identity of that natural person; is any information relating to an identified or identifiable natural person (data subject)

2.3 'special categories of personal data' (Sensitive personal data) refers to information that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life and sexual orientation

2.4 'data processing', means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

2.5 'data subject', refers to an individual who is the subject of the personal data

2.6 'data controller', means the natural or legal person, public authority, agency, or other body which alone or jointly with others, determines the purposes and means of processing the personal data

2.7 'data processor' means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller

2.8 'recipient' means a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not

2.9 'consent' of the data subject means 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

2.10 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed

2.11 ‘third party’ means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

2.12 ‘third country’ means any country recognised as not having an adequate level of legal protection for the rights of freedoms of data subjects in relation to processing personal data

2.13 ‘Data Protection Authority’, refers to an independent Public Authority responsible for monitoring the application of the relevant Data Protection legislation

2.14 ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future

2.15 ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

2.16 ‘encryption’ means the process of converting information or data into code, to prevent unauthorised access

2.17 ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

3. Scope

3.1 This policy applies to:

- All staff, directors, and volunteers of UK-SBA
- All members of UK-SBA
- All contractors, suppliers and other people working on behalf of UK-SBA
- All visitors, consultants, professionals, professional bodies associated with UK-SBA
- All data that UK-SBA processes relating to identifiable individuals, including names, postal addresses, email addresses, telephone numbers plus any other information relating to individuals in accordance with the Data Protection Act 2018
- To be read in conjunction with UK-SBA privacy notices

4. The Policy

4.1 UK-SBA collects and uses personal information (referred to as personal data in the UK General Data Protection Regulation) about members and individuals who come into contact with UK-SBA. This information is gathered in order to enable the regulation of certified practitioners and other activities undertaken to protect the consumers. In addition, UK-SBA may be required by law to collect, use and share certain information.

4.2 UK-SBA fulfils the role of the data controller for individuals, organisations employed or contracted by UK-SBA fulfil the role of the processor. Data protection is the

responsibility of everyone, the data controller and data processor, however overall responsibility lies with UK-SBA as the data controller.

4.3 UK-SBA has a designated person responsible for data protection, known as the Data Protection Officer (DPO). This person is **Kate Grant (Treasurer)**

4.4 UK-SBA issues privacy notices to members and individuals coming into contact with UK-SBA. These can be found on UK-SBA's website and summarise the personal information held, the purpose for which it is held and who it may be shared with. Information is also provided about an individual's rights in respect of their personal data.

4.5 The UK GDPR establishes six principles that UK-SBA must adhere to at all times

- Personal data shall be processed fairly, lawfully and in a transparent manner.
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Personal data shall be adequate, relevant, and limited to what is necessary to the purposes for which they are processed and not excessive.
- Personal data shall be accurate and where necessary, kept up to date.
- Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

4.6 UK-SBA is committed to maintaining the principles and duties in the UK GDPR at all times. Therefore, UK-SBA will:

- inform individuals of the identity and contact details of the data controller
- inform individuals of the contact details of the person responsible for data protection
- inform individuals of the purposes that personal information is being collected and the basis for this
- inform individuals when their information is shared, and why and with whom unless the UK GDPR provides a reason not to do this
- inform individuals and provide details of where safeguards can be obtained if information is transferred outside of the European Economic Area
- inform individuals of their data subjects rights
- inform individuals that they can withdraw consent (where relevant) and if that consent is withdrawn UK-SBA will cease processing their data although that will not affect the legality of data processed up until that point
- provide details of the length of time an individual's data will be kept
- inform and seek consent from individuals when personal data collected is used for different purposes for which it was originally intended
- check the accuracy of the information it holds and review it at regular intervals

- ensure that only authorised personnel have access to personal information whatever medium (paper or electronic) it is stored in
- ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect information from loss, theft, and unauthorised disclosure, irrespective of the format in which it is recorded
- ensure that personal information is not retained longer than it is needed
- ensure that when information is destroyed that it is done so appropriately and securely
- share information with others only when it is legally appropriate to do so
- comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- ensure that personal information is not transferred outside the EEA without appropriate safeguards
- ensure that all staff, consultants, and Directors are aware of and understand this policy and integrated procedures.

5. Complaints

5.1 If an individual has a complaint about UK-SBA has handled their personal information, this should be raised with UK-SBA's Data Protection Team either electronically or in writing - email Treasurer@UK-SBA.org. The complaint should set out the concern in detail and the outcome that the complainant is seeking

5.2 UK-SBA will carry out appropriate verification checks to confirm the identity of the complainant and that the requestor is the data subject or has the right to raise a complaint on behalf of the data subject.

5.3 All complaints will be acknowledged within 30 days of receipt.

5.4 UK-SBA will ask for further information from the complainant as is deemed necessary to support the investigation of the complaint.

5.5 In investigating any complaint, UK-SBA will:

- Look at relevant facts thoroughly, fairly and accurately
- Speak to relevant staff
- Compare information held with the information from the complainant

5.6 It is expected that any complaints investigation will be completed within 4 weeks of receipt. If an investigation is likely to take longer than this the complainant will be notified of how long it is expected to take.

5.7 Once the investigation is completed UK-SBA will provide an outcome to the complainant as soon as possible, including a clear explanation of what has been done to resolve the complaint and any actions taken (where appropriate).

5.8 If the complainant is not satisfied with the outcome, they have the right to complaint to the ICO:

ICO Helpline: 0303 123 1113

Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

www.ico.gov.uk

5.9 A record of all complaints received will be kept, in line with UK-SBA's Data Protection and retention processes and practices.

6. Integrated Procedures

6.1 Fair, Lawful and Transparent Processing

6.1.1 UK-SBA only collects, processes and shares personal data fairly and lawfully and for specified purposes. The Society must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.. These lawful processing grounds include:

- Consent: the individual has given clear consent for UK-SBA to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract UK-SBA has entered with an individual, or because the individual has asked UK-SBA to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for UK-SBA to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for UK-SBA to perform a task in the public interest or for UK-SBA's official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for UK-SBA's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

6.1.2 UK-SBA only processes special categories of personal data if one of the following applies:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of UK-SBA or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of UK-SBA's legitimate activities with appropriate safeguards to the data subject;

- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6.1.3 UK-SBA ensures that data subjects are informed of data collection and processing practices. Data subjects are informed via privacy notices. Privacy notices are communicated via UK-SBA website, email, in writing (printed copies) and in person (where applicable) to all data subjects.

6.1.4 Where personal data were collected by UK-SBA, information provided to data subjects will include:

- contact details for UK-SBA and the nominated person responsible for data protection;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the legitimate interests pursued by UK-SBA or by a third party where processing is carried out on this ground;
- the recipients or categories of recipients of the personal data, if any;
- the period for which the personal data will be stored;
- the existence of the right to request from UK-SBA access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with Information Commissioner's Office (ICO);
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

6.1.5 UK-SBA will provide the above information within a reasonable period after obtaining the personal data, but at the latest within one month.

6.2 Consent

6.2.1 Where processing personal data is based on consent, UK-SBA will ensure that there is a written record of the data subject's consent. The consent will be presented in a manner that is clearly distinguishable from other matters, it is easily accessible and in an intelligible form using clear and plain language.

6.2.2 The data subject has the right to withdraw consent at any time. UK-SBA will ensure that withdrawing consent will be as easy as giving consent.

6.3 Data Collection

6.3.1 Some of the personal data UK-SBA collects and processes are required by law. Therefore, it is mandatory for data subjects to provide information. In some cases, however, data subjects provide the information voluntarily. When collecting personal data, UK-SBA will inform data subjects whether the information is mandatory or voluntary.

6.4 Individual Rights of Data Subjects

6.4.1 According to data protection law and regulations individuals have the right to:

- be informed about their personal data (purpose of processing, who information is shared with, how long it is retained)
- access their personal data UK-SBA collects, holds and processes (by means of a Subject Access Request)
- have their personal data rectified if inaccurate;
- have personal data and information to be erased in certain circumstances (right to be forgotten);
- restrict personal data processing in certain circumstances;
- data portability;
- object to processing where processing is carried on the grounds of public interest or legitimate interests of UK-SBA, including direct marketing and profiling;
- have decisions made with an element of human intervention, rather than be made on the basis of automated decision-making, including profiling.

6.5 Subject Access Requests

6.5.1 Under data protection legislation, an individual has the right, subject to certain exemptions, to access the personal information that an organisation holds about them. Accessing personal data in this way is known as making a Subject Access Request or SAR (Refer to the Subject Access Request Policy for more information).

6.5.2 Anyone wishing to make a request under any of the above rights, can do so by contacting the Data Protection Officer via our Admin office admin@uk-sba.org UK-SBA will confirm the receipt of the request in writing and electronically (email). A response to each request will be provided within 30 days.

6.5.3 UK-SBA will carry out appropriate verification checks to confirm the identity of the requestor and that the requestor is the data subject.

6.5.4 UK-SBA will keep a log of all requests. Any member of staff, who receives a subject access request, must inform the Data Protection Officer without delay.

6.6 Data Accuracy

6.6.1 The law requires UK-SBA to take reasonable steps to ensure data is kept accurate and up to date.

6.6.2 To ensure data accuracy UK-SBA will hold personal data in as few places as necessary, staff will not create any unnecessary additional data sets and will take reasonable steps to ensure personal data is up to date. Any inaccuracies in personal data will be rectified and previous information deleted.

6.7 Retention of Data

6.7.1 To ensure fair processing, personal data will not be retained for longer than necessary in relation to the purposes for which was originally collected.

6.7.2 UK-SBA may retain data for differing periods of time for different purposes as required by statute and best practice. The data retention schedule is also available on request.

6.8 Data Storage and Security

6.8.1 UK-SBA will ensure that personal data are kept securely by implementing appropriate technical and operational measures.

6.8.2 To ensure security of personal data on paper UK-SBA will:

- keep personal data in locked cabinets, drawers when not required;
- follow a 'clear desk' policy;
- ensure printouts with personal information are not left on printers;
- shred and securely dispose of any documents, printouts once they are no longer required.

6.8.3 Where data are stored electronically, UK-SBA will ensure that personal information is protected from unauthorised access, accidental deletion and malicious hacking attempts by:

- protecting data stored on ICT devices by appropriate security software and a firewall;
- backing up data at least daily;
- testing of back-up procedures and security of systems are undertaken from time to time;

- use of strong passwords that should be updated regularly. Passwords should never be shared between employees;
- using password protection for accessing ICT devices;
- locking screens on devices when devices are unattended.
- storing data on designated UK-SBA drives and secure dropbox.
- encrypting USB devices;
- encrypting personal data when it is transferred from UK-SBA to a third party;
- not saving or downloading personal data directly to laptops, mobile devices (e.g. tablets, smartphones), desktops.

6.9 Data Sharing

6.9.1 UK-SBA will ensure that personal data are not disclosed to third parties without the consent of the data subject.

6.9.2 In certain circumstances, the data protection legislation allows personal data to be disclosed to official bodies such as law enforcement agencies, without the consent of the data subject.

6.9.3 In some cases, in order to perform a task or meet the needs of a contract, personal data may be shared with third parties without the consent of the data subject. In these cases, UK-SBA will inform the data subject of the personal data shared.

6.9.4 Where consent is given by the data subject for personal data to be shared with third parties, UK-SBA will keep a written record of this consent and data subject informed of their right to withdraw consent at any time. In cases where consent is withdrawn, UK-SBA will make reasonable steps to inform the third party for the personal data to be deleted.

6.9.5 Before sharing personal data with third parties, UK-SBA will conduct due diligence checks to ensure that the third party the data are shared with meets data protection legislation requirements.

6.10 Data Breach

6.10.1 UK-SBA is committed to keeping and processing personal data securely and implements appropriate organisational and technical measures to minimise risks to the accidental or unlawful destruction, loss, alteration, transmission, storage, unauthorised disclosure of, or access to personal data.

6.10.2 Any employee becoming aware of a suspected or substantiated personal data breach must report it to the Data Protection Officer without undue delay.

6.10.3 Refer to the Data Breach Policy for more information. This can be requested from UK-SBA Administrator admin@uk-sba.org

6.11 Data Protection Impact Assessments

6.11.1 Where a type of processing in particular 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 data subjects, UK-SBA will, prior to the processing,

carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

6.11.2 UK-SBA will also undertake Data Protection Impact Assessments on existing processing operations to review and inform protection of personal data.

7. Implementation

7.1 Distribution

7.1.1 This policy and integrated procedures are available online on the UK-SBA's website alongside with privacy notices. Printed copy can be requested from the administrator.

7.2 Training

7.2.1 All new Directors, employees and consultants joining UK-SBA receive training on this policy and integrated procedures during their induction.

7.3 Records & Confidentiality

7.3.1 UK-SBA will keep a record of processing activities under its responsibility. That record is kept as an electronic data audit and contains all of the following information:

- contact details for UK-SBA as the controller and processor, any joint controllers and the person responsible for data protection within UK-SBA;
- the purposes of processing;
- the categories of processing carried out on behalf of UK-SBA description of categories of the data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
- time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures applied by UK-SBA.

7.3.2 UK-SBA will also keep records on staff training linked to data protection, subject access requests and retention procedures for personal data. These records will be kept in an electronic format as part of UK-SBA's central data protection compliance record.

7.4 Roles & Responsibilities

7.4.1 Everyone who works for or with UK-SBA has some responsibility for ensuring data is collected, stored and handled appropriately and securely. Each team that handles personal data must ensure that it is handled and processed in line with this policy and procedures and data protection principles.

7.4.2 Board of Directors are responsible for:

- ensuring that UK-SBA complies with data protection law and regulation;

- implementing appropriate policies and procedures;
- ensuring privacy notices are accessible to data subjects;
- having a data protection officer in place.

7.4.3 Data Protection Officer is responsible for:

- keeping the board of directors updated about data protection responsibilities, risks and issues;
- reviewing all data protection procedures and related policies, in line with an agreed schedule;
- arranging and providing data protection training and advice for the people covered by this policy;
- responding to data protection questions from staff and anyone else covered by this policy;
- dealing with requests from individuals to see the data UK-SBA holds about them (also called 'Subject Access Requests');
- informing ICO of any personal data breach and acting as point of contact until the matter is resolved;
- checking and approving any contracts or agreements with third parties that may handle the company's sensitive data;
- keeping up to date records on processing activities and training within the organisation.

7.4.4 Board will ensure the IT/Website consultants support the business operations:

- ensuring all systems, services and equipment used for storing data meet acceptable security standards;
- performing regular checks, tests and scans to ensure security hardware and software is functioning properly;
- evaluating any third-party services that the company is considering using to store or process data. For instance, cloud computing services.

7.4.5 All staff and Board Directors are responsible for:

- complying with this policy and integrated procedures;
- keeping personal information and other records accurate and up to date;
- using and keeping personal data securely;
- deleting personal information that is no longer required in line with retention schedules;
- informing the data protection officer of any requests of access to personal data;

- informing the data protection officer of any data protection issues, personal data breaches.

8. Review

8.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the person responsible for data protection alongside senior managers within UK-SBA.

8.2 This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

8.3 This policy was last reviewed in March 2024

9. Contact

9.1 Any enquiries in relation to this policy should be directed to UK-SBA Administrator admin@uk-sba.org