The British Association of Prosthetics and Orthotics

Data Protection & Privacy Policy

Effective date: December 5th 2025 Review date: December 5th 2026

Contents

Data Protection & Privacy Policy

1 Introduction

BAPO is committed to protecting the personal data of its members, staff, contractors and other individuals with whom it interacts. This policy sets out how BAPO collects, uses, stores, shares and disposes of personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2 Scope

This policy applies to all personal data processed by BAPO in connection with members, staff, contractors and other individuals. It covers all formats: digital, paper, audio/visual or other.

3 Definitions

Personal data, Processing, Controller, Processor, Special category data — as defined by the UK GDPR.

4 Data Protection Principles

BAPO ensures all personal data meets the following principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.

5 Legal Basis for Processing

Processing is based on one or more lawful grounds including contractual necessity, legal obligation, legitimate interest, or consent. Special category data requires additional Article 9 conditions.

6 Data Subject Rights

Individuals have rights to be informed, access, rectify, erase, restrict processing, object, data portability, and to not be subject to automated decision-making.

7 Privacy Notices

BAPO maintains clear privacy notices explaining who we are, what we collect, why, lawful basis, recipients, retention, and rights.

8 Data Collection, Storage, and Access

BAPO collects only necessary data, stores securely, restricts access, maintains records, and reviews regularly.

9 Retention and Disposal

Retention schedules specify how long data is kept. When no longer required, data is securely deleted or anonymised.

10 Data Security and Breach Management

Appropriate measures are implemented to protect data. In case of a breach, BAPO assesses impact, notifies ICO if required, and documents the response.

11 International Data Transfers

Transfers outside the UK/EEA occur only with appropriate safeguards such as adequacy decisions or standard contractual clauses.

12 Data Protection Officer and Governance

BAPO Secretary or designated person oversees compliance, supported by the BAPO Chair and training programmes.

13 Data Protection by Design and Default

Privacy is built into all systems and projects. Data Protection Impact Assessments (DPIAs) are used for high-risk processing.

14 Monitoring and Audits

Regular compliance checks and audits are conducted, with corrective action where needed.

15 Third-party Processors and Contractors

All third-party processors are reviewed, contracted under Article 28 GDPR, and monitored for compliance.

16 Policy Changes

This policy may be updated as required. Significant changes will be communicated to stakeholders.

17 Contact and Complaints

For questions, data requests, or complaints contact: BAPO Secretary, Dr Sophie Hill (sophie.hill@bapo.com) Complaints can also be made to the ICO at https://ico.org.uk.

Appendix A: Retention Schedule Template

This schedule defines how long personal and organisational data should be retained and the method of secure disposal once it is no longer needed. Retention periods are determined by statutory requirements, operational needs, and data protection principles under the UK GDPR.

Data Category	Description	Retention Period	Legal/Business Basis	Responsible Department	Disposal Method
Membership Records	Member details, registration forms, communications	6 years after membership ends	Contractual necessity / Legitimate interest	Membership Administration	Secure deletion / shredding
Staff Employment Records	Contracts, payroll, appraisals, disciplinary actions	6 years after employment ends	Employment law / HMRC	HR Department	Secure deletion / destruction
Financial Records	Invoices, receipts, bank details	7 years	HMRC regulations	Finance	Secure deletion / shredding
Meeting Minutes and Governance Records	Board, committee, and working group minutes	Permanent archive	Legal / Historical record	Secretariat	Secure storage / archival
Training and CPD Records	Certificates, attendance, CPD logs	6 years	Professional standards	Education / CPD	Secure deletion
Contractor Details	Agreements, contact data, correspondence	6 years after contract end	Contractual necessity	Operations	Secure deletion
Event Registrations	Attendee lists, contact details, accessibility info	1 year after event	Legitimate interest / Consent	Events	Secure deletion
Health & Safety Records	Accident reports, risk assessments	3 years (adults) / until age 21 + 3 years (minors)	Legal requirement	Health & Safety	Secure deletion / destruction
Marketing and Communications Data	Mailing lists, consent records, analytics	Until withdrawal of consent or 2 years	Consent	Communications	Secure deletion
Supplier and Partner Agreements	Contracts and service agreements	6 years after expiry	Contractual / Legal	Procurement	Secure deletion

Review and Updates:
This schedule should be reviewed annually to ensure retention periods remain appropriate and compliant with current legislation.

Notes:
- Data no longer required must be securely deleted or destroyed.
- Where legal or regulatory requirements dictate longer retention, this must be documented.
- All destruction must be logged in the Data Disposal Register.

Appendix B: Data Protection Impact Assessment (DPIA) Template

This template is designed to assist in evaluating and documenting potential privacy and data protection risks arising from new or existing projects that involve personal data. Completing a DPIA ensures compliance with the UK GDPR and demonstrates accountability for data protection by design and default.

1 Project Name and Purpose

Provide the project title and a summary of its objectives. Describe why personal data will be processed and the intended outcomes.

2 Description of Data Processing

Detail how personal data will be collected, used, stored, shared, and disposed of. Include information on:

- Systems and processes used
- Who will access the data
- Any third-party involvement

3 Legal Basis

Specify the lawful basis under Article 6 of the UK GDPR. If special category data is processed, include the appropriate Article 9 condition.

4 Data Categories and Subjects

List the types of data (e.g., names, contact details, health information) and the groups of individuals affected (e.g., members, staff, contractors).

5 Risks Identified

Identify and assess potential risks to individuals' rights and freedoms. Consider confidentiality, integrity, and availability of data.

6 Mitigation Actions

Describe measures implemented to address and reduce identified risks. Examples include encryption, limited access, anonymisation, and secure storage protocols.

7 Residual Risk

Outline any remaining risk after mitigation and evaluate whether it is acceptable. Consider whether additional measures are required.

8 DPO Review and Approval

The Data Protection Officer (BAPO Secretary) should review and confirm the adequacy of this DPIA before implementation.

DPO Name: **Date:**

Signature:

Appendix C: Third-party Processors Template

This template is to record and monitor all third-party organisations (processors) that process personal data on behalf of the British Association of Prosthetics and Orthotics (BAPO). Maintaining this register ensures accountability and compliance with Article 28 of the UK GDPR.

Processor	Service Provided	Location	Safeguards	Contract Reference
Cloudhost Ltd.	Cloud Storage	UK	UK GDPR compliant	Contract Ref: 2025/01

Ensure that all third-party processors listed have written contracts in place, outlining responsibilities, security obligations, and breach reporting procedures. This table should be reviewed and updated regularly.

Appendix D: Data Subject Request Procedure Template

This template outlines the procedure for handling data subject requests in accordance with the UK GDPR. It ensures that all requests are managed transparently, securely, and within statutory timeframes.

1 Receive Request (Verify Identity)

- Acknowledge the request and verify the requester's identity before processing.
- Acceptable verification may include official ID or confirmation through existing contact information.
- Requests may include rights of access, rectification, erasure, restriction, objection, or data portability.

2 Log Request Date and Details

- Record the date of receipt, the requester's name, contact details, request type, verification outcome, and staff responsible.
- Maintain a Data Subject Request Log for accountability.

3 Assess and Locate Data

- Identify where the personal data is stored and who controls it.
- Coordinate with relevant staff and third-party processors if necessary to locate all relevant data.

4 Respond Within One Month (Extensions Must Be Justified)

- Respond to the request within one calendar month.
- Extensions of up to two months are permissible for complex requests, but justification must be documented and communicated to the requester.

5 Record Completion and Archive Securely

- Document the final response, including whether data was disclosed, corrected, or deleted.
- Record the date of completion and securely store all related records for auditing and compliance purposes.

All personnel involved in processing data subject requests must be trained on this procedure and aware of their responsibilities under the UK GDPR.

Appendix E: Data Breach and Incident Response Template

This template provides a structured approach for managing data breaches and security incidents to ensure swift action, regulatory compliance, and mitigation of harm to individuals and the organisation.

1 Identify and Contain the Incident

- Immediately identify the nature and scope of the breach.
- Take steps to contain it and prevent further unauthorised access, disclosure, or damage.
- Examples include isolating affected systems, suspending user accounts, or securing physical files.

2 Assess Risk to Individuals

- Evaluate the potential impact on individuals' rights and freedoms.
- Consider the type of data involved, sensitivity, volume, and likelihood of misuse.
- Determine whether the breach is likely to result in a risk or high risk to individuals.

3 Notify DPO and Management

- Report the incident immediately to the BAPO Secretary and Chair.
- The Secretary will coordinate the response, assess reporting obligations, and document the incident.

4 Report to ICO within 72 Hours if Required

- If the breach is likely to result in a risk to individuals, report it to the Information Commissioner's Office (ICO) within 72 hours of becoming aware.
- The report must include the nature of the breach, data categories, number of data subjects affected, likely consequences, and mitigation steps taken.

5 Notify Affected Individuals if High Risk

- If the breach is likely to result in a high risk to individuals, notify those affected without undue delay.
- Provide clear information about what happened, potential impacts, and actions they can take to protect themselves.

6 Record, Review and Improve Controls

- Record the breach in the organisation's Incident Log, detailing cause, response, and corrective actions.
- Conduct a post-incident review to identify lessons learned and strengthen future controls to prevent recurrence.

All breaches, regardless of severity, must be logged and reviewed to ensure continuous improvement in data protection practices.

Appendix F: Data Subject Access Request (DSAR) Log

This log should be maintained to record all data subject access requests (DSARs) received by the British Association of Prosthetics and Orthotics (BAPO). It ensures transparency, accountability, and compliance with the UK GDPR's requirement to document and evidence how data rights requests are handled.

Request ID	Date Received	Requester Name	Verification Completed	Type of Request	Responsible Staff Member	Response Date	Extension Applied	Outcome / Notes
ID number	dd/mm/yyyy	Name	Yes ☐ No ☐	Request	Name	dd/mm/yyyy	Yes ☐ No ☐	Outcome/Notes
ID number	dd/mm/yyyy	Name	Yes ☐ No ☐	Request	Name	dd/mm/yyyy	Yes ☐ No ☐	Outcome/Notes
ID number	dd/mm/yyyy	Name	Yes ☐ No ☐	Request	Name	dd/mm/yyyy	Yes ☐ No ☐	Outcome/Notes
ID number	dd/mm/yyyy	Name	Yes ☐ No ☐	Request	Name	dd/mm/yyyy	Yes ☐ No ☐	Outcome/Notes
ID number	dd/mm/yyyy	Name	Yes ☐ No ☐	Request	Name	dd/mm/yyyy	Yes ☐ No ☐	Outcome/Notes
ID number	dd/mm/yyyy	Name	Yes ☐ No ☐	Request	Name	dd/mm/yyyy	Yes ☐ No ☐	Outcome/Notes
ID number	dd/mm/yyyy	Name	Yes ☐ No ☐	Request	Name	dd/mm/yyyy	Yes ☐ No ☐	Outcome/Notes

Notes:

- Each request should be assigned a unique Request ID for tracking.
- Keep completed logs securely for audit purposes.
- Ensure any extension to the one-month timeframe is justified and documented.

Registered address:
Clyde Offices, 2/3 48 West George Street, Glasgow G2 1BP
Tel: 0141 561 7217 E-mail: enquiries@bapo.com
www.bapo.com