Data Protection Policy

Current version:	v3
Business Area:	Business Management
Owner:	Head of Business Management
Author:	Policy and Information Officer
Date effective from:	09/05/2023
Date of last review:	01/09/2022
Date of next review:	09/05/2026

Record of changes

Version	Date	Changes
v2	01/09/2022	Policy rewrite, changes to all sections.
v3	09/05/2023	Policy reviewed; no changes required.

Contents

Introduction

Key definitions

Personal data: Information that relates to an identifiable living person.

Data subject: This is the technical term for the individual whom particular personal data is about. We often use the term 'individuals' instead.

Processing: Almost anything we do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing, or deleting it.

Data controller: The organisation that decides how and why to collect and use the data.

Data processor: A separate organisation who processes data on behalf of the controller.

Information Commissioner's Office (ICO): The ICO regulates data protection in the UK. They offer advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance, and take enforcement action where appropriate.

Context

Data protection is about ensuring people can trust The Outdoors Group (TOG) to use their data fairly and responsibly. UK data protection law is mainly set out in the Data Protection Act 2018 (DPA 2018), along with the UK General Data Protection Regulation (UK GDPR). It takes a flexible, risk-based approach which puts the onus on TOG to think about and justify how and why we use data.

Associated legislation & guidance

- Data Protection Act 2018
- UK GDPR
- ICO Guide to the UK GDPR

Associated Outdoors Group documents

- Records Retention Schedule

Aims

The aim of this policy is to set out the governing principles that ensure TOG meets its obligations under the law and adopts good practice when processing personal data. It ensures that TOG will keep the UK GDPR principles at the heart of its approach to

processing data. It also ensures that TOG upholds the rights of the individuals whose data it processes.

Scope

This policy applies to:

- all TOG employees, volunteers and freelancers (staff); and
- all activities that operate under TOG.

This is not a legal document. It does not confer rights nor override any legal or statutory obligations.

Roles and Responsibilities

All staff

Data protection is the responsibility of all staff at TOG. We must all:

- apply the principles and best practice set out in this policy and in associated policies, standard operating procedures (SOPs) and guidance; and
- engage with training to embed data protection into our daily work.

Data Protection Lead

The role of the Data Protection Lead is to:

- assist TOG to monitor internal compliance;
- inform and advise on its data protection obligations;
- provide advice regarding Data Protection Impact Assessments (DPIAs); and
- act as a contact point for data subjects and the supervisory authority.

TOG does not currently have a Data Protection Officer (DPO). This is a specific role set out in the UK GDPR. Once an organisation reaches a certain threshold, it is required to have one.

Business Area Administrators

It is usually the responsibility of the Administrators to coordinate responses to data subject requests on behalf of their business areas.

Heads of Business Areas

Heads must make sure policies and SOPs for their business area are in line with this data protection policy.

Training

TOG will provide general data protection training for all staff, which must be completed as part of induction or onboarding. More detailed training will be provided for staff for whom processing personal data is a significant part of their role.

Principles

1. Lawfulness, fairness and transparency

TOG will identify valid grounds under the UK GDPR, known as “lawful basis”, for collecting and using personal data. We will only use personal data in a way that is fair; not unduly detrimental, unexpected or misleading to the individuals concerned. We will be clear, open and honest with people from the start about how we will use their data. TOG’s privacy notice is one of the main ways in which we demonstrate transparency.

2. Purpose limitation

TOG will be clear about what our purposes for processing are from the start. We will record our purposes as part of our documentation obligations and specify them in our privacy information for individuals. We will only use the personal data for a new purpose if either this is compatible with our original purpose, we get consent, or we have a clear obligation or function set out in law.

3. Data minimisation

TOG will ensure the personal data we are processing is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. We will identify the minimum amount of personal data we need to fulfil our purpose and will hold that much information, but no more.

4. Accuracy

Tog will take all reasonable steps to ensure the personal data we hold is not incorrect or misleading as to any matter of fact. Where necessary, we will keep the personal data updated. If we discover that personal data is incorrect or misleading, we will take reasonable steps to correct or erase it as soon as possible.

5. Storage limitation

TOG will not keep personal data for longer than we need it. Our Records Retention Schedule sets standard retention periods where possible. When deciding how long to keep data, we will take into account the purpose for processing that data; whether we

need to keep information to defend possible future legal claims; any legal or regulatory requirements; and industry standards or guidelines.

6. Integrity and confidentiality (security)

TOG will process personal data in a manner that ensures appropriate security, ensuring the confidentiality, integrity or availability of the data. This includes preventing data from being accidentally or unlawfully lost or destroyed; made unavailable; altered; disclosed to or accessed by an unauthorised individual; made available where it should not have been; stolen; or fraudulently used.

7. Accountability principle

TOG takes responsibility for complying with data protection laws and has in place appropriate measures to demonstrate compliance.

Lawful Basis for Processing

In accordance with the lawfulness, fairness and transparency principle, TOG must have a valid lawful basis in order to process personal data. There are six available lawful bases. Which basis is most appropriate to use will depend on the purpose for processing and relationship with the individual.

Consent

TOG will normally rely on consent when we can offer people real choice and control over how we use their data and want to build their trust and engagement. Genuine consent must be freely given and should put individuals in charge. This requires:

- a positive opt-in, rather than pre-ticked boxes or any other method of default consent;
- distinct, granular options for consenting to different types of processing; and
- the right to withdraw consent to be clear and easy for individuals to choose at any time.

TOG will keep clear records to demonstrate consent.

Contract

TOG will normally rely on this lawful basis if we need to process someone's personal data:

- to deliver a contractual service to them; or
- because they have asked us to do something before entering into a contract.

Legal obligation

TOG will normally rely on this lawful basis if we need to process the personal data to comply with a common law or statutory obligation, other than contractual obligations. We should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out our obligation.

Vital interests

It is unlikely that TOG will need to rely on this lawful basis but we will if we need to process personal data to protect someone's life and the individual is unable to give their consent.

Public task

It is unlikely that TOG will need to rely on this lawful basis because we are not a public authority. However, we may if we exercise official authority or carry out tasks in the public interest and our underlying task, function or power has a clear basis in law.

Legitimate interests

TOG relies on this basis when processing is necessary for pursuing the company's legitimate interests. It is most appropriate where we use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. When we do so, we balance our interests with the individual's interests, rights and freedoms.

Special category data

This is data that needs more protection because it is sensitive. It includes information about:

- Racial or ethnic origin
- Beliefs (religious, political, etc.)
- Health
- Sex life or sexual orientation

To lawfully process special category data, TOG will identify a lawful basis and a separate condition for processing under Article 9 of the UK GDPR.

Criminal offence data

The UK GDPR gives extra protection to the personal data of offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings. TOG does not have official authority, so we will only process criminal offence data when relying on a specific condition for processing in Schedule 1 of the DPA 2018.

Individual Rights

The UK GDPR provides certain rights for individuals. Individuals can make requests relating these rights in writing or verbally. There are exemptions that may apply and some rights only apply in certain circumstances. TOG will assess requests on a case-by-case basis and, in most cases, will respond within one calendar month. We can also refuse to comply with a request if it is manifestly unfounded or excessive.

Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This includes the purposes for processing, retention periods for that personal data and who it will be shared with. This is a key transparency requirement under the UK GDPR. At the time of collection, TOG will provide individuals with this information, normally in the form of a privacy notice.

Right of access

Individuals have the right to access and receive from TOG a copy of their personal data, and other supplementary information. This is commonly referred to as a data subject access request (DSAR) or sometimes, just 'SAR'.

Right to rectification

Individuals have the right to have inaccurate personal data that TOG processes rectified or completed if it is incomplete. This may involve providing a supplementary statement to the incomplete data, rather than overwriting it.

Right to erasure

Individuals have the right to have personal data erased by TOG, also known as 'the right to be forgotten'.

Right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. This means TOG will store the personal data, but not use it.

Right to data portability

Individuals have the right to receive personal data they have provided to TOG in a structured, commonly used and machine readable format. It also gives them the right to request that TOG transmits this data directly to another controller.

Right to object

Individuals have the right to object to TOG processing their personal data at any time. This effectively allows individuals to stop or prevent TOG from processing their personal data. In some cases, we may be able to continue processing if we can show that we have a compelling reason for doing so.

Rights related to automated decision making including profiling

Where TOG identifies data processing that involves automated decision making or profiling that falls under Article 22 of the UK GDPR, we will introduce simple ways for individuals to request human intervention or challenge a decision.

Accountability and Governance

For reference, see Appendix A – Accountability and Governance Diagram.

TOG will be proactive and organised about our approach to data protection and be able to evidence the steps we take to comply with data protection laws. We will embed data protection into everything we do. Our approach includes:

- ensuring a good level of understanding and awareness of data protection amongst our staff;
- implementing comprehensive but proportionate policies and procedures for handling personal data; and
- keeping records of what we do and why in the form of our record of processing activities (RoPA) and data protection impact assessments (DPIAs).

Record of processing activities (RoPA)

In accordance with Article 30 of the UK GDPR, TOG will maintain a record of our data processing activities. This is important, not only because it is itself a legal requirement, but also because it can support good data governance and help demonstrate our compliance with other aspects of the UK GDPR. The RoPA includes:

- the purposes of processing;
- categories of individuals;
- categories of personal data;
- categories of other organisations we share data with;
- international transfers and safeguards;
- retention schedules; and
- security measures.

Data protection impact assessments (DPIAs)

TOG will carry out DPIAs for processing that is likely to result in a high risk to individuals. We will also carry out DPIAs at other times, where it is deemed to be good practice to do so. A template will be used to make sure DPIAs:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Data Sharing

TOG shares personal data with various other organisations. The nature of the relationship and location of the transferred data affect what safeguards TOG will use. The following table is a summary:

TOG's role	Other organisation's role	Safeguard
Data controller	Data processor	Contract
Data controller	Data controller	Data sharing agreement
Data processor	Data controller	Contract

International transfers

In addition to the safeguards in the table above, if data is being transferred outside of the UK, the transfer will be covered by:

- an adequacy decision – the location the data is being transferred to has adequate data protection laws;
- appropriate safeguards – currently, TOG uses Standard contractual clauses (SCCs); or
- an exemption.

Personal Data Breaches

A personal data breach is a security risk that affects the confidentiality, integrity or availability of personal data. This could happen when personal data is accidentally or unlawfully:

- Lost or destroyed
- Made unavailable
- Altered
- Disclosed to or accessed by an unauthorised individual
- Made available where it should not have been
- Stolen
- Fraudulently used

A breach can have a range of adverse effects on individuals, which include emotional distress and physical and material damage.

On becoming aware of a breach, TOG will take reasonable steps to contain it and assess the potential adverse consequences for individuals, based on how serious these are and how likely they are to happen.

If a breach is likely to result in a risk to the rights and freedoms of individuals, TOG will notify the ICO without undue delay, but not later than 72 hours after becoming aware of it.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, TOG will inform those concerned directly without undue delay.

Appendix A – Accountability and Governance Diagram