The Global Biodiversity Standard

# Data Protection Policy

October 2026

| | |
|---|---|
| **Status** | Approved and in force |
| **Version** | 1.1 |
| **Policy owner** | CEO, with Board oversight |
| **Approved by** | TGBS Ltd Board of Directors |
| **Approval date** | 27 October 2026 |
| **Effective date** | 27 October 2026 |
| **Next review** | October 2027: Annually, and after any material incident or legal change |

**The Global Biodiversity Standard (TGBS Ltd)**

# Data Protection Policy

TGBS Ltd company policy

**This is TGBS's internal data-protection policy. It is distinct from audience-specific privacy notices, which explain to staff, directors, website users, applicants, clients and other individuals how their information is used.**

## 1. Purpose and document architecture

TGBS Ltd is a UK company limited by guarantee and acts as controller for personal data when it determines why and how that data is used. This policy establishes internal governance under the UK GDPR, Data Protection Act 2018 and the Data (Use and Access) Act 2025 amendments.

- This policy tells covered persons how to handle personal data.
- Separate privacy notices must be maintained for relevant audiences, including staff/workers, directors, website and mailing-list users, applicants/certificate holders/clients, event or training participants, and job applicants.
- Cookie information and consent controls must be addressed through a website cookie notice or tool.
- Contracts and data-sharing agreements must define controller/processor roles; a privacy notice does not replace them.

## 2. Scope and key definitions

This policy applies to TGBS Ltd directors, officers, employees, workers, consultants, contractors, volunteers and interns. It also applies, to the extent stated in contract or appointment terms, to TGBS hubs, certified assessors, technical reviewers, committee members, delivery partners and any other person acting for or representing TGBS.

- **Personal data:** information relating to an identified or identifiable living person, including online identifiers and location data.
- **Special-category data:** data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric identifiers, health, sex life or sexual orientation.
- **Criminal-offence data** requires additional legal safeguards.
- **Processing** includes collecting, recording, organising, storing, viewing, sharing, analysing, altering, deleting or destroying data.
- **Data breach:** accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

Biodiversity and project data may become personal data when linked to landholders, community members, Indigenous knowledge holders, assessors or precise locations. Confidential ecological data can also require security even when it is not personal data.

# 3. Roles and responsibilities

- The Board approves the policy, oversees material risks and ensures that allegations involving senior leadership are handled independently.
- The CEO implements the policy, assigns proportionate controls and reports material matters to the Board. A responsibility may be delegated, but accountability remains with the role that delegated it.
- Directors and managers model the required conduct, act on concerns promptly, protect reporters from retaliation and identify conflicts before taking part in a decision.
- All covered persons must understand the policy, complete required training, keep accurate records and raise concerns without delay.
- Each hub must nominate a responsible lead, cascade relevant requirements to assessors and subcontractors, maintain suitable local controls, comply with applicable local law, and report material concerns to TGBS. A hub remains responsible for its own legal duties and personnel.
- Assessors and reviewers must act impartially, declare conflicts, protect evidence and information, and never allow commercial or relationship pressures to affect their professional judgement.
- TGBS is not currently required to appoint a statutory Data Protection Officer. The Board will designate a Data Protection Lead with responsibility for coordinating compliance with this policy. TGBS will document and periodically review whether its processing activities meet the statutory criteria requiring appointment of a Data Protection Officer, including following any material change in the nature or scale of its activities.
- System and process owners must document purposes, lawful bases, access, retention, sharing and security and complete a data-protection impact assessment for likely high-risk processing.
- Hubs must identify whether they act as independent controller, joint controller or processor and must not transfer TGBS personal data without the required written terms and safeguards.

# 4. Data protection principles

- **Lawfulness, fairness and transparency:** identify and document a lawful basis and give clear privacy information.
- **Purpose limitation:** use data only for specified, explicit and legitimate purposes unless further use is lawful and compatible.
- **Data minimisation:** collect only what is adequate, relevant and necessary.
- **Accuracy:** take reasonable steps to keep data accurate and correct or delete inaccurate data.
- **Storage limitation:** follow the retention schedule and securely delete or anonymise data when no longer needed.
- **Integrity and confidentiality:** protect data through appropriate technical and organisational measures.
- **Accountability:** be able to demonstrate compliance through records, contracts, assessments, training and review.

# 5. Lawful processing and individual rights

## 5.1. Lawful bases and sensitive data

Before processing personal data, TGBS must identify and document the applicable lawful basis under Article 6 of the UK GDPR. The basis must reflect the specific purpose and circumstances of the processing and must be

reviewed if that purpose changes. Consent will be used only when freely given, specific, informed, unambiguous and as easy to withdraw as to give. Special-category and criminal-offence data require an additional lawful condition and any required policy documentation.

Children's data requires particular care, age-appropriate information and a safeguarding assessment. Personal data must not be collected merely because it may be useful later.

### 5.2. Rights requests and complaints

Individuals may have rights of access, information, rectification, erasure, restriction, objection, portability and safeguards relating to automated decisions. Any covered person receiving a request must send it immediately to the Data Protection Lead. Identity will be checked proportionately, and TGBS will respond within the applicable statutory period, explaining any lawful extension, pause, exemption or refusal.

TGBS will maintain a data-protection complaints process in line with the Data (Use and Access) Act 2025. Individuals may also complain to the Information Commissioner's Office.

## 6. Information governance and security

- Maintain a record of processing activities or proportionate data inventory, privacy notices, retention schedule and authorised systems list.
- Apply least-privilege access, strong authentication, secure configuration, supported software, backups, encryption where appropriate and secure deletion.
- Use approved devices, storage and communication channels; do not move personal data to personal accounts or unapproved tools.
- Complete due diligence and written processor terms before a supplier processes personal data.
- Use data-protection impact assessments for new technology or processing likely to create high risk, including systematic monitoring, large-scale sensitive data, biometric tools or significant automated decisions.
- Consider confidentiality, intellectual property, Indigenous data governance and harm from disclosure alongside legal data-protection duties.

### International transfers

A transfer outside the UK requires an applicable adequacy regulation, appropriate safeguards such as the UK International Data Transfer Agreement/Addendum, or a lawful exception. A transfer-risk assessment and contractual/technical measures must be used where required. Access by an overseas hub or cloud provider may constitute a transfer.

## 7. Personal data breaches

Any suspected loss, misdirection, unauthorised access, phishing compromise or disclosure must be reported to the Data Protection Lead immediately and no later than 24 hours after discovery. Preserve evidence and do not delete or conceal the incident.

The Data Protection Lead will contain and assess the breach, document the decision and notify the ICO without undue delay and, where feasible, within 72 hours after TGBS becomes aware if the breach is likely to risk

individuals' rights and freedoms. Affected individuals will be informed without undue delay where high risk is likely. Hubs and processors must notify TGBS promptly enough to meet these deadlines.

## 8. Reporting and escalation of data-protection concerns or breaches

A person may raise a concern orally or in writing and may be accompanied or supported where appropriate. Anonymous reports will be considered as far as the available information allows. Reports should include the facts known, relevant dates, people involved and any evidence that can be preserved safely.

| Situation | Route |
|---|---|
| Ordinary route | Report to the CEO and copy the Board Chair or another non-conflicted director. |
| Concern involves the CEO | Report to the Board Chair and at least one other non-conflicted director. The CEO must not receive, direct or decide the matter. |
| Concern involves the Board Chair | Report to the CEO and at least one other non-conflicted director. The Chair must not receive, direct or decide the matter. |
| Concern involves both the CEO and Chair, several directors, or internal independence is reasonably in doubt | Report to any non-conflicted director or to the Governance Contact, who must notify at least one other non-conflicted director and arrange an independent response. External professional advice or an external investigator must be used where necessary. |
| Immediate danger or suspected crime/regulatory breach | Contact emergency services, law enforcement or the relevant regulator where appropriate. Internal reporting is not a precondition. |

The Board will maintain a current Policy Contact Register containing direct contact details for the CEO, Chair, Governance Contact and at least two other directors. The Governance Contact means the Company Secretary, if appointed, or a non-conflicted director designated by the Board.

No person may investigate, influence, decide or hear a review of a matter in which they are implicated or have an actual, potential or perceived conflict of interest. A report received by an implicated person must be forwarded immediately to a non-conflicted route without screening or alteration.

Retaliation, victimisation, obstruction, concealment, destruction of evidence and knowingly false or malicious allegations are prohibited. A report made honestly will not attract action merely because it is unsubstantiated.

## 9. Confidentiality, records and non-retaliation

Information will be shared only with those who need it to protect people, assess the matter, comply with law, obtain advice or take action. Absolute confidentiality cannot be promised where disclosure is necessary for a fair process or legal duty.

Retention periods will be defined by category in the TGBS retention schedule and reflect purpose, legal obligations, limitation periods, funder or certification requirements and individual rights. Data must not be kept indefinitely by default.

Personal data will be handled under the TGBS Data Protection Policy. Records must be factual, access-controlled and kept separately from general personnel or project files where sensitivity requires it.

## 10. Breaches and corrective action

TGBS may restrict access, require remedial training, correct or delete data, notify individuals or authorities, suspend a system or transfer, and take disciplinary or contractual action. Deliberate misuse, concealment or unlawful disclosure is serious misconduct.

## 11. Monitoring and review

The Data Protection Lead will review the data inventory, rights requests, complaints, breaches, high-risk processing, supplier arrangements, international transfers and privacy notices at least annually and report material matters to the Board.

## 12. Related documents and legal framework

- Audience-specific TGBS privacy notices; Safeguarding Policy; Whistleblowing Policy; Complaints Policy.
- UK GDPR; Data Protection Act 2018; Data (Use and Access) Act 2025; Privacy and Electronic Communications Regulations 2003; Data Protection (Charges and Information) Regulations 2018; applicable local data-protection law.