Personal Data Protection Policy

At St1 Biokraft, protecting personal data is part of how we keep people safe, maintain trust, comply with the law and run a resilient business. Data protection sits alongside our Safety First mindset and our Cornerstones: Be Collaborative, Be the Expert, Be Commercial and Be Open, and forms part of our responsible business governance under ESRS G1. This Policy outlines our approach to protecting personal data in a way that is practical, clear and aligned with our governance across our operations and value chain.

Purpose and Scope

This Policy sets expectations for how St1 Biokraft collects, uses, stores, shares and protects personal data. It applies across all St1 Biokraft group companies to employees, contractors, consultants, board members, and third parties who handle personal data on our behalf. It covers automated and non-automated processing that forms part of a filing system.

Principles of Personal Data Protection

We apply the GDPR principles throughout the data lifecycle:

- Lawfulness, fairness, transparency: clear purpose, lawful basis, understandable notices.
- Purpose limitation: process only for specified, legitimate purposes.
- Data minimisation: adequate, relevant, necessary.
- Accuracy: keep data accurate and up to date.
- Storage limitation: retain only as long as needed for the specified legitimate purposes.
- Integrity and confidentiality: protect via appropriate technical and organisational measures (CIA triad).

Security and Incident Management

Data security follows our Cyber Security Policy and NIS2-aligned governance. We maintain proportionate controls (access management, encryption, logging/monitoring, resilience and backup) and escalate incidents per our cyber incident plan. Personal data breaches are assessed without delay and, where required, notified within 72 hours per GDPR.

Transparency and Data Subject Rights

We provide employees and other data subjects with clear and accessible privacy information, including a dedicated privacy notice or equivalent communication that explains how their data is collected, used, stored and protected. We also handle requests to exercise rights such as access, correction or deletion in line with GDPR timeframes.

Legal Bases for Processing

Under GDPR, all processing must have a valid legal basis. These fall into two categories: bases for regular personal data and stricter conditions for special categories of personal data.

Regular Personal Data (GDPR Article 6)

We only process personal data when there is a clear legal basis. This may include situations where:

- the law requires it (for example, payroll or basic health and safety compliance records)
- it is necessary to fulfil an employment contract or another agreement
- St1 Biokraft has a legitimate business interest that does not override the rights of the individual
- it is needed to protect someone's vital interests in an emergency
- the processing is carried out in the public interest
- the individual has given consent, which must be freely given, specific, informed, unambiguous and documented, and can be withdrawn at any time.

Special Categories of Personal Data (GDPR Article 9)

These are sensitive types of data such as health information. We only process them when there is a specific legal ground, for example:

- to meet obligations in employment or social security law
- to manage or defend legal claims
- to protect vital interests where the person cannot give consent
- where the individual has made the data public themselves
- for reasons of substantial public interest permitted by law
- with the individual's explicit consent.

Processors and Third-Party Oversight

We use a four-step approach for processors: first we determine their role, then vet their privacy standards, conclude a Data Processing Agreement (DPA), and finally carry out audits or reviews to ensure compliance. Critical vendors, including cloud and HR platforms, must demonstrate adequate security and data protection, verified proportionally to risk.

Records, Retention and Risk Assessments

St1 Biokraft maintains a GDPR-compliant Record of Processing Activities (RoPA). Retention periods follow applicable legal, regulatory and business requirements. Where backups technically persist, they remain restricted and are not used operationally; deletion follows standard cycles.

We assess privacy risks periodically and conduct Data Protection Impact Assessments (DPIAs) for high-risk processing such as new technology, large-scale sensitive data or automated decisions. Where new technologies including AI or advanced analytics involve personal data, St1 Biokraft will apply GDPR principles and consider a DPIA if risks are high.

International Data Transfers

For transfers of personal data outside the EU/EEA, St1 Biokraft relies on lawful safeguards such as Standard Contractual Clauses (SCCs) or the EU-US Data Privacy Framework where applicable. We assess transfer risks and apply supplementary measures if required to ensure adequate protection.

Training and Awareness

All employees complete periodic personal data protection and cyber awareness training, with additional modules for roles that handle sensitive data.

Policy Governance, Monitoring and Oversight

We track training completion, incident response times and internal/external audit findings to measure programme effectiveness and drive improvement.

This Policy has shared ownership by the Head of IT overseeing systems and process security and HR overseeing employee data. Managers are accountable for compliance in their respective areas.

The Policy will be reviewed annually, or sooner if required by legal or regulatory changes, and reported to the Board.

***

This Personal Data Protection Policy was last approved on the 27th of November 2025 by the board of St1Biokraft AB.

St1 Biokraft AB, Board of Directors