TRICEL
GENERATIONS OF INNOVATION

Data Protection

Policy Statement

Purpose of policy

The primary objective of Tricel's GDPR Personal Data Protection Policy is to ensure compliance with the General Data Protection Regulation (GDPR) and relevant legislation, protecting personal data across its operations. The policy focuses on safeguarding data subjects' rights, ensuring data security, and implementing privacy by design. It aims to maintain data accuracy, minimize processing, secure personal data, and ensure transparency, fostering trust in Tricel's data management practices.

Name of Policy	Data Protection Policy
Tricel Site	Tricel Group
Applicable Policies	Data Subject Request Procedure. Data Protection Impact Assessment Process Document. Personal Data Breach Notification Procedure.

1. Introduction

The primary objective of Tricel's GDPR Personal Data Protection Policy is to ensure full compliance with the General Data Protection Regulation (GDPR) and other pertinent legislation, thereby safeguarding personal data within its operations. The policy aims to establish clear and verifiable compliance practices across all systems, personnel, and processes involved in data handling. This includes protecting the rights of data subjects, ensuring data security, and implementing privacy by design. The goals are to maintain data accuracy, minimise data processing, secure personal data, and guarantee transparency in data handling practices, ultimately fostering trust and reliability in Tricel's data management.

2. Scope

The GDPR Personal Data Protection Policy of Tricel is applicable across all systems, processes, and personnel involved in handling personal data. This includes board members, directors, employees, suppliers, and other third parties with access to Tricel's information systems. The policy governs data collection, storage, and processing activities, ensuring compliance with GDPR and other relevant legislation. Specific areas covered include obtaining and processing personal data, data subject rights, breach notifications, and data transfers outside the EU.

3. Out of Scope

The GDPR Personal Data Protection Policy for Tricel does not cover certain items that fall outside its boundaries and applicability. These out-of-scope items include data processing activities not related to personal data of EU citizens, non-compliance with GDPR by third-party entities not engaged with Tricel's systems, and internal processes unrelated to data protection such as non-IT operational workflows. Departments or areas not specifically mentioned within the policy, such as general business strategies and non-personal data analytics, are also not covered under this policy. Additionally, any non-compliant actions by stakeholders that fall outside the outlined procedures and safeguards are considered beyond the scope of this document.

4. Responsibilities

Roles	**Responsibilities**
Senior Management/ Executive Team	• Provide leadership and strategic direction for data protection initiatives. • Ensure adequate resources and support for data protection activities. • Approve and periodically review the Data Protection Policy. • Ensure that data protection practices are integrated into business operations.
Data Controllers/ Department Heads & Managers	• Define the purposes and means of processing personal data. • Ensure that personal data is processed in compliance with GDPR principles. • Monitor and enforce data protection measures within their teams or departments. • Ensure proper data subject consent, where applicable. • Coordinate with the DPO and respond to data subject requests (e.g., access, rectification, erasure).

IT & Security Teams	• Implement technical and organizational measures to safeguard personal data. • Ensure the security of data storage, transmission, and access. • Regularly test and update data security systems to prevent breaches. • Assist with incident management and breach response plans.
Employees & Contractors	• Handle personal data in compliance with the company's Data Protection Policy. • Report any data protection concerns, breaches, or risks to the relevant manager. • Complete mandatory data protection training. • Follow security protocols, including data encryption, access control, and secure disposal of data. • to obtain and process personal data fairly. • Keep such data only for explicit and lawful purposes. • Only disclose such data only in ways compatible with these purposes • Keep such data accurate, complete and up-to-date. • Ensure that such data is adequate, relevant and not excessive. • Retain such data for no longer than is necessary for the explicit purpose.
Data Subjects	The data subject has rights under the GDPR. These consist of: • The right to be informed • The right of access • The right to rectification • The right to erasure • The right to restrict processing • The right to data portability • The right to object • Rights in relation to automated decision making and profiling.

Any data access requests received should be forwarded immediately to the Manager, Compliance & Information Management. Each of these rights must be supported by appropriate procedures within Tricel that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown below:

Data Subject Request	**Deadline**
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

5. Policy

As per GDPR regulation, 2016 version, there are 7 principles involving personal data and how companies should treat these aspects. These are as follows, as per Chapter II, Article 5.1

5.1. Data Processing

Personal data shall be:

5.1.1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

5.1.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further

processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

5.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

5.1.4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5.1.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

5.1.6. 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, using appropriate technical or organisational measures ('integrity and confidentiality').

5.2. Data Controller

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Tricel complies with these principles by using business workflows based on technology that use metadata in order to search, discover, classify, label, protect and apply actions at all levels of personal data. Also, Operational Security

Procedures defined support and provide the specific guidelines for all teams involved including IT Support, Customer Support or Line of Business .

6. MONITORING AND REVIEW

Monitoring and periodically reviewing the effectiveness of the GDPR Personal Data Protection Policy at Tricel involves a structured process to ensure continuous compliance and improvement. The process includes regular audits, employee training sessions, and periodic data protection impact assessments. Key performance indicators (KPIs) related to data protection are tracked and reported to senior management. Triggers for updates or revisions to the policy include significant changes in legislation, the identification of new risks or vulnerabilities, data breaches, and feedback from internal audits or external regulatory bodies. Any changes in business operations or IT infrastructure that impact data processing activities also prompt a policy review to maintain alignment with GDPR requirements.

7. SUPPORTING DOCUMENTATION

https://gdpr-info.eu/

- Data Subject Request Procedure.
- Data Protection Impact Assessment Process Document.
- Personal Data Breach Notification Procedure.

8. ACKNOWLEDGMENT AND COMPLIANCE

Tricel ensures compliance with its GDPR Personal Data Protection Policy through several actionable steps and measures. Every staff member involved in handling personal data is responsible for understanding and adhering to good data protection practices. The company provides comprehensive training to all employees on data protection principles. Our team oversees compliance efforts, ensuring all legal bases for data processing are clear and unambiguous. Tricel follows strict rules regarding obtaining consent and processes data in line with

GDPR requirements. Regular reviews and audits of data processing activities are conducted to maintain adherence to the policy, incorporating privacy by design in all new or significantly altered systems. Additionally, clear documentation of processing activities and established procedures for responding to data subject inquiries further support compliance.