



Data Protection and Privacy Policy

1. Purpose

The purpose of this Data Protection and Privacy Policy is to establish the principles and practices for the protection of personal and sensitive data collected and processed by Toros Consulting. This Policy ensures compliance with GDPR data protection laws and regulations and outlines our commitment to safeguarding the privacy and confidentiality of individuals' data.

2. Scope

This Policy applies to all employees, contractors, vendors, and authorised users who handle or have access to personal and sensitive data within Toros Consulting. It encompasses data collected from customers, employees, partners, and other stakeholders.

3. Policy Statements

3.1 Data Protection Principles:

- **Lawful Processing:**
Toros Consulting will only collect, process, and use personal and sensitive data when there is a lawful basis for doing so, such as consent, contract necessity, legal obligation, legitimate interests, or the protection of vital interests.
- **Transparency:**
Individuals will be informed about the purpose, use, and processing of their data at the time of collection or as soon as practicable thereafter.
- **Data Minimisation:**
Toros Consulting will only collect data that is necessary for the specified purpose and will retain it only for as long as required.
- **Data Accuracy:**
Reasonable efforts will be made to ensure the accuracy of data, and individuals have the right to request correction of inaccuracies.
- **Security:**
Appropriate security measures, including encryption, access controls, and data breach response plans, will be implemented to protect data from unauthorised access, disclosure,



3.2. Data Collection and Consent

- **Consent:**

Wherever required by law, Toros Consulting will obtain clear and unambiguous consent from individuals before collecting or processing their personal data.

3.3. Data Subject Rights

- **Access and Rectification:**

Data subjects have the right to access their data and request corrections, updates, or deletions.

- **Data Portability:**

Data subjects may request their data in a structured, commonly used, and machine-readable format for portability.

- **Objection and Restriction:**

Data subjects have the right to object to the processing of their data and request restriction under certain circumstances.

- **Withdrawal of Consent:**

Data subjects have the right to withdraw their consent at any time where processing is based on consent.

3.4. Data Breach Response

- **Notification:**

Toros Consulting will promptly investigate and report data breaches to the appropriate regulatory authorities and affected individuals, as required by law.

- **Mitigation:**

Steps will be taken to mitigate the impact of data breaches, prevent recurrence, and address vulnerabilities.

3.5. Third-Party Data Processors

- **Third-Party Contracts:**

When Toros Consulting engages third-party data processors, contracts will be established to ensure they comply with data protection regulations and safeguard the data in their custody.

4. Training and Awareness

- **Training:**

Employees, contractors, and authorised users will receive regular training and awareness programs on data protection and privacy to ensure compliance and awareness of data protection principles.



4.1 Responsibilities

- **Data Protection Officer:**
Responsible for overseeing data protection compliance, monitoring data security, and acting as the point of contact for data subjects and regulatory authorities.
- **Employees and Users:**
Responsible for adhering to this Policy, understanding data protection principles, and reporting any data protection concerns or breaches.

5. Compliance and Consequences

Non-compliance with this Data Protection and Privacy Policy may result in disciplinary actions in accordance with Toros Consulting's policies and procedures. Violations may also lead to legal and regulatory penalties.

6. Policy Review

This Data Protection and Privacy Policy will be reviewed annually or more frequently if necessary. Updates or changes to the Policy will be communicated to all relevant personnel to ensure continued adherence to data protection and privacy guidelines.