Data Protection Policy

Recover is committed to ensuring the protection, confidentiality, and integrity of personal data entrusted to us by our clients, customers, employees, and other stakeholders. This Data Protection Policy outlines our commitment to compliance with data protection laws and regulations, including but not limited to the General Data Protection Regulation (GDPR).

Scope

This policy applies to all personal data processed by Recover, whether held electronically or in paper format. It covers all employees, contractors, third-party service providers, and other individuals who may process personal data on behalf of Recover.

Principles of Data Protection

Recover adheres to the following principles when processing personal data:

a. Lawfulness, Fairness, and Transparency: Personal data is processed lawfully, fairly, and transparently, ensuring that individuals are informed about the processing of their data.

b. Purpose Limitation: Personal data is collected and processed only for specified, explicit, and legitimate purposes.

c. Data Minimization: Recover collects and processes only the personal data that is necessary for the intended purpose.

d. Accuracy: Recover takes reasonable steps to ensure the accuracy of personal data and update it as necessary.

e. Storage Limitation: Personal data is kept for no longer than necessary for the purposes for which it is processed.

f. Integrity and Confidentiality: Appropriate security measures are in place to protect personal data from unauthorized access, disclosure, alteration, and destruction.

g. Accountability: Recover is accountable for its compliance with data protection laws and regulations.

Data Collection and Processing

Recover collects and processes personal data for the following purposes:

a. Customer and Client Services: To provide information, products, and services to our customers and clients.

b. Employee Management: To manage and administer the employment relationship with our staff.

c. Marketing and Communication: To send promotional materials and communicate with stakeholders about relevant products and services.

5. Data Security

Recover employs technical and organizational measures to ensure the security of personal data. This includes encryption, access controls, regular security assessments, and employee training on data protection.

6. Data Subject Rights

Recover respects the rights of data subjects, including the right to access, rectify, erase, and object to the processing of their personal data. Data subjects can exercise their rights by contacting Recover's Data Protection Officer (DPO) at [DPO contact details].

7. Data Breach Notification

In the event of a data breach that poses a risk to the rights and freedoms of individuals, Recover will promptly notify the relevant supervisory authority and affected data subjects as required by applicable data protection laws.

8. Policy Review and Updates

This Data Protection Policy will be regularly reviewed and updated to ensure its continued relevance and effectiveness. Any updates will be communicated to relevant stakeholders.

10. Compliance with Laws and Regulations

Recover is committed to complying with all applicable data protection laws and regulations, and this policy is designed to meet the requirements of the GDPR and other relevant legislation.