



Itus Protection Limited

Data Protection Policy

Our contact details

Name: Itus Protection Limited
Address: 167–169
Great Portland Street
London
W1W 5PF

Phone Number: 0330 043 7133
E-mail: Enquires-itusprotection@outlook.com

Data Protection Policy

1. Introduction

Itus Protection Limited is committed to protecting the privacy and security of personal and sensitive data in compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018, and other relevant legislation. This Data Protection Policy outlines our approach to data protection and the measures we have implemented to ensure the confidentiality, integrity, and availability of personal data.

2. Scope

This policy applies to all personal and sensitive data processed by [Security Company Name], including data relating to employees, clients, suppliers, and other individuals.

3. Principles of Data Protection

Lawfulness, Fairness, and Transparency: We will process personal data lawfully, fairly, and transparently, ensuring that individuals are informed about how their data is being used and their rights in relation to that data.

Purpose Limitation: We will only collect and process personal data for specified, explicit, and legitimate purposes, and we will not use the data for any other purposes without obtaining consent or another lawful basis for processing.

Data Minimization: We will only collect and process personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.

Accuracy: We will take reasonable steps to ensure that personal data is accurate, kept up to date, and corrected without delay if inaccuracies are identified.

Storage Limitation: We will not keep personal data in a form that permits identification of individuals for longer than is necessary for the purposes for which it is processed.

Integrity and Confidentiality: We will implement appropriate technical and organizational measures to ensure the security of personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage.

Accountability: We will be able to demonstrate compliance with data protection principles and obligations, including maintaining records of processing activities, conducting data protection impact assessments (DPIAs) where necessary, and cooperating with supervisory authorities.

4. Data Protection Responsibilities

Management: The management team is responsible for ensuring that data protection policies and procedures are implemented and adhered to throughout the organization. They will appoint a Data Protection Officer (DPO) to oversee data protection compliance.

Employees: All employees have a responsibility to comply with data protection policies and procedures, including handling personal data securely, reporting any breaches or concerns, and cooperating with data protection audits and investigations.

Data Protection Officer (DPO): The DPO is responsible for advising the organization on data protection matters, monitoring compliance with data protection laws and policies, and acting as a point of contact for data subjects and supervisory authorities.

5. Data Processing Activities

We will only process personal data where we have a lawful basis for doing so, such as:

Consent: where the individual has given explicit consent for the processing of their personal data for specific purposes.

Contractual necessity: where the processing is necessary for the performance of a contract with the individual or to take steps at the request of the individual prior to entering into a contract.

Legal obligation:

where the processing is necessary for compliance with a legal obligation to which we are subject.

Legitimate interests:

where the processing is necessary for our legitimate interests or the legitimate interests of a third party, provided that such interests are not overridden by the rights and freedoms of the individual.

6. Data Security Measures

We will implement appropriate technical and organizational measures to ensure the security of personal data, including:

Encryption of personal data in transit and at rest.

Access controls to restrict access to personal data to authorized personnel only.

Regular security assessments and audits to identify and address vulnerabilities.

Training and awareness programs to educate employees about data protection best practices.

7. Data Subject Rights

We will respect the rights of data subjects under data protection laws, including the right to:

Access their personal data and obtain information about how it is processed.
Rectify inaccurate or incomplete personal data.
Erase personal data in certain circumstances, such as where it is no longer necessary for the purposes for which it was collected.
Restrict the processing of their personal data under certain conditions.
Object to the processing of their personal data in certain circumstances, such as for direct marketing purposes.
Data portability, where applicable.

8. Data Breach Management

We will implement procedures to detect, report, and investigate data breaches promptly. In the event of a data breach, we will assess the risk to individuals' rights and freedoms and notify the relevant supervisory authority and affected individuals as required by law.

9. International Data Transfers

We will ensure that personal data is only transferred to countries or organizations outside the European Economic Area (EEA) that provide an adequate level of data protection or where appropriate safeguards are in place to protect the data, such as standard contractual clauses or binding corporate rules.

10. Review and Update

This Data Protection Policy will be reviewed and updated regularly to ensure it remains accurate, relevant, and effective. Changes may be made in response to changes in legislation, technology, business operations, or other factors affecting data protection compliance.

Conclusion

This Data Protection Policy reflects our commitment to protecting the privacy and security of personal data and ensuring compliance with data protection laws and regulations. By adhering to the principles and procedures outlined in this policy, we can maintain the trust and confidence of our employees, clients, and other stakeholders.

