Tiny Air Limited Data Security and Data Management Policy

Introduction

Tiny Air Limited is committed to safeguarding the personal data it handles, ensuring its confidentiality, integrity, and availability in line with UK GDPR and the Data Protection Act 2018. This policy outlines our approach to data security and management to prevent unauthorized access, disclosure, alteration, and destruction of data.

Scope

This policy applies to all data processed by Tiny Air Limited, including digital and physical records of personal data of our employees, customers, and partners, irrespective of where the data is stored.

Data Security Measures

Access Control: Only authorised personnel have access to personal data, based on their role and necessity. Access is controlled through secure authentication mechanisms.

Data Encryption: Personal data stored and transmitted is encrypted using industry-standard encryption methods to protect data in transit and at rest.

Network Security: We employ firewall and intrusion detection systems to protect against unauthorized access and cyber threats.

Regular Security Assessments: Conduct regular security assessments and audits to identify vulnerabilities and implement corrective measures.

Data Minimization: Collect and process only the data necessary for the specified purposes, minimizing the amount of personal data held.

Data Management Practices

Data Accuracy: Implement procedures to ensure that personal data is accurate, up to date, and corrected or deleted without delay when inaccurate.

Data Retention: Retain personal data no longer than necessary for the purposes for which it is processed, with clear retention periods and deletion procedures.

Data Protection by Design and by Default: Integrate data protection into processing activities and business practices, from the design stage of any system, service, or process.

Data Transfer Security: Ensure secure data transfers, especially when transferring data outside the UK, complying with UK GDPR requirements for international data transfers.

Incident Response and Data Breach Notification

Implement an incident response plan to address data breaches or security incidents promptly.

Notify the UK Information Commissioner's Office (ICO) within 72 hours of becoming aware of a data breach, where feasible, if it is likely to result in a risk to the rights and freedoms of individuals.

Inform affected individuals without undue delay if the breach could result in a high risk to their rights and freedoms.

Training and Awareness

Provide regular data protection and security training to all employees to ensure they understand their responsibilities.

Update training materials to reflect changes in law, regulations, and internal policies.

Roles and Responsibilities

Assign a Data Protection Officer (DPO) to oversee compliance with this policy, the UK GDPR, and the Data Protection Act 2018.

Ensure all employees and contractors understand their roles and responsibilities in protecting personal data.

Review and Updates

Review this policy annually or following significant changes to processing activities or applicable laws.

Update the policy as necessary to maintain compliance with the UK GDPR and other relevant regulations.

Contact Information

For any inquiries related to this policy or data protection practices, please contact our Data Protection Officer at ute@tinyair.co.uk

This policy is effective as of 15/11/2022 and must be followed by all Tiny Air Limited employees, contractors, and third parties engaged in processing activities on behalf of the company.