07876761713
info@alphait.uk
www.alphait.uk
60 Sandringham Street,
HU3 6EB

GDPR Compliance Policy for IT Support Services

1. Introduction

Purpose: This policy outlines our commitment to GDPR compliance, ensuring the protection of personal data handled by our IT support services.

Scope: This policy applies to all employees, contractors, and third-party service providers involved in IT support services.

2. Key Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person.
- **Data Subject**: The individual whose personal data is being processed.
- **Processing**: Any operation performed on personal data, such as collection, storage, use, and deletion.
- **Data Controller**: The entity that determines the purposes and means of processing personal data.
- **Data Processor**: The entity that processes personal data on behalf of the data controller.

3. Principles of Data Protection

- **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully, fairly, and in a transparent manner.
- **Purpose Limitation**: Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimisation**: Data collected must be adequate, relevant, and limited to what is necessary.
- **Accuracy**: Personal data must be accurate and kept up to date.
- **Storage Limitation**: Data must be kept in a form that permits identification of data subjects for no longer than necessary.
- **Integrity and Confidentiality**: Personal data must be processed in a manner that ensures appropriate security.
- **Accountability**: The data controller is responsible for, and must be able to demonstrate, compliance with these principles.

4. Lawful Basis for Processing

- **Consent**: Obtained from the data subject.
- **Contract**: Processing is necessary for the performance of a contract.
- **Legal Obligation**: Processing is necessary for compliance with a legal obligation.
- **Vital Interests**: Processing is necessary to protect the vital interests of the data subject or another person.
- **Public Task**: Processing is necessary for the performance of a task carried out in the public interest.

07876761713
info@alphait.uk
www.alphait.uk
60 Sandringham Street,
HU3 6EB

- **Legitimate Interests**: Processing is necessary for the purposes of legitimate interests pursued by the data controller or a third party.

5. Data Subject Rights

- **Right to be Informed**: Data subjects must be informed about the collection and use of their personal data.
- **Right of Access**: Data subjects have the right to access their personal data.
- **Right to Rectification**: Data subjects can request the correction of inaccurate data.
- **Right to Erasure**: Data subjects can request the deletion of their data.
- **Right to Restrict Processing**: Data subjects can request the restriction of processing.
- **Right to Data Portability**: Data subjects can request their data in a structured, commonly used, and machine-readable format.
- **Right to Object**: Data subjects can object to the processing of their data.
- **Rights Related to Automated Decision-Making**: Data subjects have rights concerning automated decision-making and profiling.

6. Data Protection by Design and Default

- **Data Minimisation**: Implement measures to ensure only necessary data is processed.
- **Pseudonymisation**: Use pseudonymisation techniques to protect personal data.
- **Encryption**: Encrypt personal data to protect it from unauthorised access.
- **Access Controls**: Implement strict access controls to limit who can access personal data.

7. Data Protection Impact Assessments (DPIAs)

- Conduct DPIAs for processing activities that are likely to result in a high risk to the rights and freedoms of data subjects.
- Document the assessment process and outcomes.

8. Data Breach Management

- **Reporting**: Report data breaches to the relevant supervisory authority within 72 hours.
- **Notification**: Notify affected data subjects without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
- **Response Plan**: Implement a data breach response plan to manage and mitigate the effects of data breaches.

9. Third-Party Management

- Ensure third-party service providers comply with GDPR requirements.
- Include data protection clauses in contracts with third parties.

10. Training and Awareness

- Provide regular GDPR training to employees.
- Raise awareness about data protection responsibilities and best practices.

07876761713
info@alphait.uk
www.alphait.uk
60 Sandringham Street,
HU3 6EB

11. Monitoring and Review

- Regularly review and update the GDPR compliance policy.
- Conduct audits to ensure ongoing compliance with GDPR.