DATA PROTECTION AND DATA SECURITY PROCEDURE

1. PURPOSE

This procedure is designed to ensure the confidentiality, integrity, and availability of data processed by our organization, prevent data breaches, and ensure compliance with legal requirements regarding personal data protection.

2. SCOPE

This procedure applies to all data processed within our organization, including employees, business partners, suppliers, and third-party service providers.

3. DEFİNİTİONS

Personal Data: Any information relating to an identified or identifiable natural person.

Sensitive Personal Data: Information such as race, health, religion, and biometric data that require special protection.

Data Controller: The entity that determines the purposes and means of data processing.

Data Processor: A third party that processes data on behalf of the Data Controller.

Data Subject: The natural person whose personal data is being processed.

4. RESPONSİBİLİTİES

Data Protection Officer: Manages and oversees data security processes.

IT Department: Implements technical security measures.

All Employees: Are responsible for maintaining data confidentiality.

5. DATA SECURİTY MEASURES

5.1. Technical Measures

Access Controls: Authorization policies must be implemented to prevent unauthorized access.

Encryption: Sensitive data should be protected through strong encryption algorithms during transmission and storage.

Firewalls and Antivirus Software: Up-to-date security solutions must be used to protect against cyber threats.

Backups: Data should be regularly backed up and stored securely.

Monitoring and Logging: System logs should be monitored to detect unauthorized access or data breaches.

5.2. Administrative and Organizational Measures

Employee Training: Employees should receive regular training on data security.

Confidentiality Policies: Employees and business partners must sign confidentiality agreements.

Risk Assessment: Data security risks should be regularly evaluated.

Data Processing Inventory: All processed data, their purposes, and retention periods should be documented.

6. ACTİONS İN CASE OF A DATA BREACH

1. Detection of the Breach: Systems should be continuously monitored to identify potential breaches.

2. Breach Notification: If a data breach is detected, it must be reported to the relevant authorities and affected individuals within 72 hours.

3. Mitigation of Damage: Affected systems should be quickly isolated, and damage should be minimized.

4. Post-Breach Analysis: The root causes of the breach should be investigated, and necessary measures should be taken to prevent recurrence.

7. Data Retention and Disposal Policy

Retention Periods: Data should only be retained for the necessary duration and securely deleted once the retention period expires.

Disposal Methods: Digital data should be securely erased using specialized software.

Physical documents should be destroyed using secure shredding machines.

8. AUDİTS AND UPDATES

This procedure should be reviewed and updated at least once a year.

Internal and external audits should be conducted to ensure compliance with data security policies.

9. LEGAL COMPLİANCE

This procedure has been prepared in accordance with GDPR (General Data Protection Regulation) and KVKK (Personal Data Protection Law), as well as other applicable local and international regulations.