

1. Introduction

Line Security Services Ltd is committed to protecting personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy outlines the measures we take to safeguard the personal data of our employees, customers, and other stakeholders.

2. Scope

This policy applies to all personal data processed by Line Security Services Ltd, including data belonging to employees, customers, contractors, and partners. It also applies to all employees, contractors, and third parties who process data on behalf of the company.

3. Key Definitions

- **Personal Data:** Any information relating to an identified or identifiable individual.
- **Data Subject:** The individual whose personal data is being processed.
- **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.
- **Processing:** Any operation performed on personal data, including collection, storage, modification, and destruction.

4. Data Protection Principles

Line Security Services Ltd adheres to the following principles in line with the UK GDPR:

- **Lawfulness, Fairness, and Transparency:** Data must be processed lawfully, fairly, and transparently.
- **Purpose Limitation:** Data is collected for specified, explicit, and legitimate purposes.
- **Data Minimisation:** Only the necessary data for the intended purposes is collected.
- **Accuracy:** Personal data must be kept accurate and up-to-date.
- **Storage Limitation:** Data should be kept no longer than necessary.
- **Integrity and Confidentiality:** Personal data must be processed securely to prevent unauthorised access or loss.
- **Accountability:** The company is responsible for ensuring compliance with these principles and can demonstrate this.

5. Lawful Basis for Processing

Personal data must be processed on a lawful basis, including:

- **Consent:** The data subject has given clear consent to process their data.
- **Contract:** Processing is necessary for a contract with the data subject.
- **Legal Obligation:** Processing is necessary to comply with the law.
- **Legitimate Interests:** Processing is necessary for the legitimate interests of Line Security Services Ltd or a third party, provided these interests are not overridden by the data subject's rights.

6. Rights of Data Subjects

Under UK GDPR, data subjects have the following rights:

- **Right to be Informed:** Transparency about how their data is being used.
- **Right of Access:** The right to request access to their personal data.
- **Right to Rectification:** The right to correct inaccurate or incomplete data.
- **Right to Erasure:** The right to request deletion of their data (the "right to be forgotten").
- **Right to Restrict Processing:** The right to request the restriction of data processing.
- **Right to Data Portability:** The right to transfer their data to another service provider.
- **Right to Object:** The right to object to data processing based on legitimate interests.
- **Rights related to Automated Decision-Making:** The right to not be subject to decisions based solely on automated processing.

7. Data Collection and Use

- **Types of Data Collected:** [Detail the personal data categories, e.g., names, email addresses, phone numbers, financial information].
- **Purpose of Collection:** delivering services,

- **Consent:** Explicit consent will be obtained where necessary for data processing.

8. Data Retention

Personal data will only be retained for as long as necessary for the purposes for which it was collected, or as required by law. Regular reviews will be conducted to ensure that data is either securely deleted or anonymized when no longer required.

9. Data Security

Line Security Services Ltd implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks associated with processing personal data. These measures include:

- **Encryption:** Sensitive data is encrypted in transit and at rest.
- **Access Control:** Personal data is accessible only to authorized personnel.
- **Regular Security Audits:** Security measures are tested and updated regularly.

10. Data Breach Notification

In the event of a personal data breach, Line Security Services Ltd will:

- Report the breach to the Information Commissioner's Office (ICO) within 72 hours if it poses a risk to individuals' rights and freedoms.
- Notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

11. Third-Party Data Sharing

Line Security Services Ltd may share personal data with third parties, such as service providers or partners, only if they have data protection agreements in place to ensure compliance with UK GDPR. Data transfers to countries outside the UK will only occur if adequate safeguards are in place, such as Standard Contractual Clauses (SCCs) or other mechanisms approved by the ICO.

12. Data Protection Officer (DPO)

The Managing Director is responsible for overseeing compliance with this policy. The DPO is responsible for:

- Monitoring compliance with data protection laws.
- Advising on data protection impact assessments (DPIAs).
- Acting as a contact point for the ICO and data subjects.

13. Data Subject Access Requests (DSARs)

Data subjects can submit access requests to view their personal data. Line Security Services Ltd will respond within one month, providing the requested data in a structured, commonly used, and machine-readable format.

14. Employee Responsibilities

All employees are responsible for ensuring that they follow this policy and any associated procedures to protect personal data. They must complete regular training on data protection and report any potential breaches immediately.

15. Review and

This policy will be reviewed annually or in response to changes in legislation, regulations, or operational changes within Line Security Services Ltd.

16. Compliance and Enforcement

Non-compliance with this policy may result in disciplinary action and, in certain cases, legal consequences



Hafiz Rehman
Managing Director
27/10/2024