

MPS Group - GDPR Policy

1. Introduction

MPS Group is committed to ensuring the protection of personal data in accordance with the General Data Protection Regulation (GDPR) and other applicable data protection laws. This policy outlines our commitment to the lawful, fair, and transparent processing of personal data and our responsibilities under the GDPR.

2. Scope

This policy applies to all personal data processed by MPS Group, whether collected from customers, employees, suppliers, or other individuals.

3. Principles of Data Protection

Lawfulness, Fairness, and Transparency: We will process personal data lawfully, fairly, and transparently, and will only collect data for specified, explicit, and legitimate purposes.

Purpose Limitation: Personal data will only be collected for specified, explicit, and legitimate purposes and will not be further processed in a manner that is incompatible with those purposes.

Data Minimisation: We will ensure that personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Accuracy: We will take reasonable steps to ensure that personal data is accurate and kept up to date.

Storage Limitation: Personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

Integrity and Confidentiality: We will process personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

4. Data Subjects' Rights

We will respect the rights of data subjects as outlined in the GDPR, including the right to access, rectification, erasure, restriction of processing, data portability, and the right to object to processing.

5. Lawful Basis for Processing

We will ensure that personal data is processed lawfully, fairly, and transparently, and that we have a lawful basis for processing data in accordance with the GDPR.

6. Data Security

We will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

7. Data Breach Management

We will have procedures in place to detect, report, and investigate personal data breaches in accordance with the requirements of the GDPR.

8. Data Protection Impact Assessments (DPIAs)

We will conduct DPIAs where necessary to assess and mitigate the risks associated with processing personal data, particularly where processing is likely to result in a high risk to the rights and freedoms of data subjects.

9. Data Protection Officer (DPO)

We will appoint a Data Protection Officer (DPO) responsible for overseeing compliance with the GDPR and other data protection laws and regulations.

10. Training and Awareness

We will provide training and awareness-raising activities for employees involved in the processing of personal data to ensure they understand their obligations under the GDPR.

11. Third-Party Data Processors

We will only engage third-party data processors who provide sufficient guarantees to implement appropriate technical and organisational measures to ensure the protection of personal data.

12. Review and Monitoring

This policy will be regularly reviewed and updated as necessary to ensure ongoing compliance with the GDPR and other applicable data protection laws and regulations.

Signed:

Mike Short : MPS Group Director..

04.01.2024