

GDPR Data Protection Policy

Introduction

We hold personal data about our Employees, Clients, Suppliers and Service Providers (Data Subjects) for a variety of business purposes. This Policy sets out how we seek to protect personal data and ensure that Employees understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this Policy requires employees to ensure that the Data Protection Officer (DPO) (Bradley Smith) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

Responsibilities of the Office Manager:

- Addressing Data Protection queries from Clients, Sub-Contractors or Employees
- Coordinating with the DPO to ensure all marketing initiatives adhere to Data Protection laws and the company's Data Protection Policy
- Keeping the board updated about Data Protection responsibilities, risks and issues
- Reviewing all Data Protection procedures and Policies on a regular basis
- Answering questions on Data Protection from Employees and other stakeholders
- Responding to individuals such as Clients and Employees who wish to know which data is being held on them by M&T Midlands Ltd.

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

The Privacy Statement

- Sets out the purposes for which we hold personal data on Clients
- Highlights that our work may require us to give information to third parties such as business professionals
- Provides that Clients have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data, we will require the Data Subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work).

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Office Manager so that they can update your records.

Data security

We must keep personal data secure against loss or misuse.

Storing data securely

In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.

Printed data should be shredded when it is no longer needed

Data stored on a computer should be protected by strong passwords that are changed regularly.

We encourage all Employees to use a password manager to create and store their passwords. Data stored on CDs or memory sticks must be locked away securely when they are not being used

The DPO must approve any cloud used to store data

Servers containing personal data must be kept in a secure location, away from general office space

Data should be regularly backed up in line with the company's backup procedures

Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Training

All M&T Midlands staff will receive training on this Policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our Policy and procedure.

Training is provided through a Toolbox Talk on a regular basis. It will cover:

- The law relating to Data Protection
- Our Data Protection and related Policies and Procedures.

- Completion of training is compulsory.
- Conditions for processing
- We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All Employees who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to Data Subjects in the form of a Privacy Statement REM 116.
- Justification for personal data
- We will process personal data in compliance with all six Data Protection principles.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject but must also be by the permission of the individual.
Right to be forgotten

A Data Subject may request that any information held on them is deleted or removed.
Monitoring

Everyone must observe this Policy. The DPO has overall responsibility for this Policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this Policy very seriously. Failure to comply puts both you and the organisation at risk. The importance of this Policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this Policy, do not hesitate to contact Head Office

