Mapeley

1 Introduction

1.1 Mapeley is committed to protecting the privacy and personal information of all our clients, employees, contractors, and suppliers by striving to ensure we handle personal data fairly, lawfully, sensitively and with justification.

1.2 Personal data is any recorded information held by us from which a living individual can be identified. It will include a variety of information including names, addresses, date of birth, NI number, telephone numbers, photographs of people and other personal details. It will include any expression of opinion about a living individual or any indication of our intentions about that individual. Identification can be directly from the information alone or indirectly from any other information in Mapeley's possession or likely to come into our possession.

1.3 We aim to comply with The Data Protection Act 2018 ("the Act") and The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) (the "Regulations").

1.4 Mapeley Estates Limited is the service company for the Mapeley group of companies, excluding the Salisbury group. It manages the group's data. In this policy statement the terms Mapeley, we and us refer to the Mapeley group or the relevant Mapeley entity in its capacity as data controller or data processor.

2 Purposes of the Processing

2.1 Mapeley processes personal data to enable us to perform our contracts with clients and contractors, maintain our own accounts and records and support and manage our people.

3 How We Collect Personal Data

3.1 Mapeley handles a range of personal data relating to clients, tenants, visitors, suppliers, contractors and employees. Our collection and processing of personal data is subject to a variety of legal requirements. We process and retain personal data for purposes which include:

- 3.1.1 Recruitment, screening, vetting and identity checks
- 3.1.2 Contracts of employment and payroll purposes, including tax and National Insurance
- 3.1.3 Equal opportunities monitoring
- 3.1.4 Commercial contracts and compliance
- 3.1.5 Medical and health records
- 3.1.6 External supplier and customer relationships
- 3.1.7 Disciplinary and grievance procedures
- 3.1.8 Training/development records and performance information
- 3.1.9 Management purposes
- 3.1.10 IT Services and management, computer records and emails

4 How We Process Personal Data

4.1 Mapeley is responsible for compliance with its obligations under the Act and the Regulations by ensuring that personal data is:

4.1.1 Processed lawfully, fairly and in a transparent manner

4.1.2 Collected for specified, explicit and legitimate purposes

4.1.3 Adequate, relevant and limited to what is necessary

4.1.4 Accurate and kept up to date

4.1.5 Retained only as long as necessary

4.1.6 Processed in an appropriate manner to maintain security

5 Legal Basis for Processing Personal Data

5.1 Mapeley will only process data in compliance with one of the following conditions:

5.1.1 Consent of the data subject – must be freely given, specific, informed and unambiguous by clear explicit means.

5.1.2 Processing essential to the performance of a contract or steps required to enter into a contract.

5.1.3 Compliance with a legal obligation.

5.1.4 When necessary to protect the vital interests of a data subject.

5.1.5 When necessary in the public interest or in the exercise of authority vested in the data controller.

5.1.6 Legitimate interests pursued by the data controller.

6 Record of Processing

6.1 Mapeley will process personal data for the following purposes:

6.1.1 Property and Asset Management

6.1.2 Complying with contracts with client, contractors, landlords, tenants and suppliers

6.1.3 Marketing and promoting our business

6.1.4 Managing accounts

6.1.5 Maintaining personnel records

6.1.6 Managing our people

6.1.7 Complying with the law

6.1.8 Processing personal data as a contractual requirement for the purposes of security screening and vetting of staff, and contractors in relation to:

6.1.9 Baseline Personnel Security Standard

6.1.10 Counter Terrorism Check

6.1.11 Security Clearance

7 Sharing of Personal Data

7.1 Mapeley will only share personal data with GDPR compliant organisations. Information is shared on a need to know basis and only the necessary information is shared. Typical examples where we are required to share personal data are:

7.1.1 HM Revenue and Customs.

7.1.2 HM Government Screening and Vetting Unit.

7.1.3 Payroll bureau and benefits systems, including expenses system.

7.1.4 Clients and customers who restrict access to their premises for security reasons.

7.1.5 Training providers and accrediting bodies.

7.1.6 Marketing (including websites).

7.1.7 Travel and accommodation bookings.

7.1.8 Anti-money laundering checks.

7.1.9 Technology providers who host our business data.

7.2 We also process and share personal data from the following sources as a direct consequence of our business:

7.2.1 Service partners, suppliers of services and contractors.

7.2.2 Consultants.

7.2.3 Clients and customers.

7.3 Legal Requirements

7.3.1 We may be required to share personal data in pursuance of sub-section 5.1. - legal basis, for processing personal data above – 'compliance with a legal obligation' or 'when necessary in the public interest'. An example would be release of personal data when required by law, such as during the course of legal proceedings or to law enforcement agencies in the course of a criminal investigation, matters of public health and substantial public interest.

8 Retention of Personal Data

8.1 We keep personal data for no longer than reasonably necessary.

9 Security of Personal Data

9.1 Mapeley takes the security of its personal data very seriously and takes many measures to safeguard against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data.

10 Transfer of Data Abroad

10.1 Mapeley do not ordinarily transfer personal data outside of the European Community. On occasions personal data may be transferred to the USA under the protection of USA Privacy Shield agreement.

11 Further Processing

11.1 If Mapeley wishes to process personal data for a new purpose, not covered by this policy, then we shall provide you with a new notice explaining this new issue prior to commencing the processing and setting out the relevant purpose and processing conditions. Whenever necessary we will seek your prior consent to the new processing.

12 Right to be Informed

12.1 If the personal data is not obtained directly from the data subject, the Human Resources Department will provide the data subject with the following additional items of information within one month of having received their personal data:

12.1.1 The categories of personal data we are processing

12.1.2 The source from where the personal data originates and whether it came from publicly accessible sources

13 Data Subjects' Rights

13.1 The right to request a copy of the personal data which Mapeley holds about you

13.2 The right to request that Mapeley corrects any personal data that is found to be inaccurate or out of date

13.3 The right to request your personal data is erased where it is no longer necessary to retain such data

13.4 The right to withdraw consent to processing at any time – if consent is relied upon as a processing condition

13.5 The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing

13.6 The right to object to the processing of personal data – where processing is based on legitimate interests or performance of a task in the public interest/exercise of official authority, and direct marketing

13.7 The right to lodge a complaint with The Information Commissioners Office (ICO)

14 Subject Access Requests

14.1 The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) details rights of

access to data subjects to their personal data held by Mapeley. A Subject Access Request is a written request for personal information held about a data subject who generally has the right to see what personal data we hold about them. All requests for information must be directed to The Head of Human Resources without delay and will be dealt with in accordance with 'Subject Access Request Policy'.

15 Obligation of Mapeley Employees and Contractors

15.1 All employees and contractors working for Mapeley must be aware of the importance of handling personal data while working on Mapeley business and ensure:

15.1.1 They understand their responsibilities when handling or managing personal data;

15.1.2 That the only individuals authorised to access personal data are those who need it for their work

15.1.3 All personal data is kept secure by using strong passwords which should be kept confidential

15.1.4 Personal data is not disclosed to unauthorised people, either within Mapeley or externally

15.1.5 Personal data is reviewed and updated if found to be out of date and if no longer required, should be deleted or safely disposed of.

16 Mapeley's Commitment to Data Protection

16.1 We aim to ensure that:

16.1.1 Everyone managing and handling personal data understands that they are responsible for following good GDPR practice.

16.1.2 Methods of managing or handling personal data are regularly reviewed and evaluated.

16.1.3 Any disclosure of personal data will comply with approved procedures.

16.1.4 We take all necessary steps to ensure that personal data is always kept secure against unauthorised or unlawful loss or disclosure.

16.1.5 This policy will be reviewed regularly to ensure it remains fit for purpose.

Key Contact

To exercise all relevant rights, or in case of queries or complaints please contact:
enquiries@mapeley.com