M GROUP

Employee Privacy Notice Handbook

DP@mgroupservices.com

Contents

Data Protection

This Employee Privacy Notice ("Notice") describes the manner by which the M Group Services group of companies ("M Group", "we" or "us") collects, uses, and otherwise processes certain individually identifiable information ("Employee Data") about the persons who work for (or who have worked for) us, whether employees or not, whether on a part-time, temporary or full-time basis, and including current and former employees, contingent workers, contractors, interns, trainees and others working at or attached to us in connection with individuals' employment relationship with M Group Services Limited and its associated companies.

In the course of our business we will process Employee Data (which may be held on paper, electronically, or otherwise) about our staff. M Group businesses respect the privacy rights of individuals, understand the importance of the protection of your Employee Data and are committed to using good practices in how we handle your Employee Data. Our processes are designed to ensure that we collect, process, use and transfer that data in accordance with applicable law. If you are in any doubt regarding the applicable standards, or have any comments or questions about this Notice, please contact us at DP@mgroupservices.com.

1. Categories of Employee Data

In the course of your employment, we will process personal data about you and your dependents, beneficiaries and other individuals whose personal data has been provided to us.

1.1. Sources of personal data

We collect this personal data from the following different sources:

- Information that you provide directly - When your working relationship starts with us, the initial information about you that we process is likely to come from you directly: for example, contact details, CV, bank details and information on your immigration status and whether you can lawfully work. We may also require references and information to carry out background checks. In the course of your employment or engagement, you may be required to provide us with information for other purposes such as sick pay and family rights (e.g. maternity and paternity leave and pay). If you do not provide information that you are required by statute or contract to give us, you may lose benefits or we may decide not to employ / engage you or to end your contract. If you have concerns about this in a particular context, you should speak to People Services.

- Information from third parties - In the course of your employment with us, we may receive personal data relating to you from others, including from recruitment agencies, academic institutions, referees, background checking agencies and other third parties during your recruitment.

- Information that we collect indirectly - We collect your personal data indirectly, including through our Company's IT systems and other devices as described in the "IT Data" section below.

- Information that we collect from publicly available sources - We may collect information about you from news sources and/or social media platforms, for example in connection with any investigation or formal procedure concerning the same (for instance, for the investigation of an allegation that a staff member has breached our rules on social media use or conduct generally).

1.2. Categories of personal data

The table below describes the categories of personal data we collect from and about you and your dependents, beneficiaries and other individuals as well as the source of that information.

Data Categories	Personal Data Description	Source
Identity Data	Name or alias, gender, passport number, driver's license number, social security number or other government-issued identification number, tax registration number and other details in and copies of identity documents.	• Directly from you
Contact Data	Home and business address, personal and work telephone number, personal and work email addresses, emergency contact details (including emergency contact person and their telephone number).	• Directly from you
Employment Data	Job title/position, staff reference number, photograph, office location, employment contract, employment start and leaving date, working times and days and records relating to performance, disciplinary processes, training history, grievance procedures, accidents, sickness/holiday, leave (including parental and adoption leave), family rights and working days and hours.	• Directly from you • Third parties
Background Data	Age, date of birth, marital status, gender, pronouns, academic/professional qualifications, education, CV/résumé, criminal records data and security clearance status.	• Directly from you • Third parties

Family Data	Including information relating to your next-of-kin, spouse, partner, dependents and other family members (in particular, their names and dates of birth and details of entitlements under relevant benefit schemes).	• Directly from you
Payroll Data	Banking details, tax information (such as tax registration number), withholdings, salary, benefits, expenses, loans, company allowances, stock and equity grants.	• Directly from you • Third parties
Audio/Visual Data	Photographs and other audio-visual information used for workplace initiatives and promotional materials.	• Directly from you • Third parties
Geolocation Data	Information received from company vehicles, mobile devices and laptops which reveals the location of company assets.	• Indirectly from you
Special Category Data	Information that reveals your racial or ethnic origin, religious, political or philosophical beliefs, genetic data, biometric data for the purposes of unique identification, trade union membership, information about your health (including mental health and vaccination status), disability, sexual orientation or sex life.	• Directly from you • Third parties (from medical professionals)
Communication Data	Contact details and content of communications when you communicate with us, for example, to inquire about employee benefits.	• Directly from you • Indirectly from you
IT Data	Information required to provide access to company IT systems and networks (and information collected by / through those systems) such as IP addresses, log files and login information. IT Data may also include inferred location based on your IP address or activities, device identifiers associated with your computer or device, mobile carrier and related information, activity logs, and other information about activities you engage in on M Group's property, equipment, accounts, systems and networks. M group may monitor and review your uses of M Group equipment, accounts, information technology systems and networks, including its phone networks, computer networks, including those used to access the Internet, videoconferencing systems and other company-provided electronic communications tools. M Group may access and review electronic files, messages, and emails sent or stored on its information technology systems, including accounts, computers and devices provided to you.	• Indirectly from you

Security and Access Data	Closed-circuit television (CCTV) footage in public or common areas in our premises and near our premises (such as in car parking areas and in which case footage may include vehicle licence plates). It may also include other information obtained through electronic means such as security records (e.g. swipe card records, building entry / exit data) and if you are visiting a premises, physical or electronic guest book information containing name, vehicle licence plate and person(s) you are visiting).	• Indirectly from you • Third parties (where used for CCTV, security and access systems)
Ethics Reporting Data	In addition to certain Identity Data and Contact Data such as name, telephone number and email, which office you work from and also employee reference number (unless you report anonymously), IP address and inferred location based on your IP address, device identifiers associated with your computer or device and activity logs. If you use our telephone reporting hotline, we collect voice recordings. Information reported to us, which may include personal data about other individuals such as those that have engaged in alleged misconduct (including criminal activity). Information collected in connection with an investigation, such as description of the alleged misconduct, witness statements and evidence gathered to ascertain the facts and circumstances. Conclusions of the investigation.	• Indirectly from you • Directly from you • Third parties
Survey Data	Answers to survey questions, date and time survey completed and IP address. Although this data will usually be aggregated, technically (even though we do not intend to look at this data), you may be identifiable from your IP address when completing a survey.	• Indirectly from you • Directly from you

2. How we use your personal data (our purposes) and our lawful basis for processing it.

2.1. Purposes and lawful basis for processing personal data

The following table provides more details on our purposes for processing your personal data and the related legal bases. The legal basis under which your personal data is processed will depend on the data concerned and the specific context in which we use it.

Purpose/ Activity	Type of personal data	Lawful basis
Administering your contract including entering it, performing it and changing it	**Identity Data** **Contact Data** **Employment Data** **Communications Data** Including information on your terms of employment or engagement, your pay and benefits, your participation in pension arrangements, life and medical insurance and any bonus or share scheme.	• Performance of a contract with you • Legal obligation • Legitimate interests
Contacting you or others on your behalf	**Identity Data** **Contact** **Data** **Communications Data** **Spouse and Dependent data**	• Performance of a contract with you • Legitimate interests
Payroll administration	**Identity Data** **Contact** **Data Payroll** **Data** Including your bank account details, salary, pension contributions and details of other benefits, and information on tax and social security / national insurance, information on attendance, holiday and other leave and sickness absence.	• Performance of a contract with you • Legal obligation • Legitimate interests
Supporting and managing your work and performance and any health concerns	**Employment Data** **Special Category Data (specifically health data) IT Data** Including information connected with your work, anything you do at work and your performance including records of documents and emails created by or relating to you and information on your use of our systems including computers, laptops or other devices. Management information regarding you including notes of meetings and appraisal / performance records. Information relating to your compliance with our policies. Information concerning disciplinary allegations, investigations and processes and relating to grievances in which you are or may be directly or indirectly involved. To the extent required or permitted by local law, information concerning your health, including self-certification forms, medical and occupational health reports.	• Performance of a contract with you • Legal obligation • Legitimate interests In relation to Special Category Data: • Employment obligations, Occupational health and working capacity, Public health or in limited cases, Consent.
Changing or ending your working arrangements	**Identity Data** **Contact Data** **Employment Data** Including information connected with anything that may affect your continuing employment or the terms on which you work including any proposal to promote you, to change your pay or benefits, to change your working arrangements or to end your employment.	• Performance of a contract with you • Legitimate interests • Legitimate interests • Legal obligations • Consent
Physical and system security	**Security and Access** **Data IT Data** **Location Data** Including CCTV images and records of use of swipe and similar entry cards / systems. To the extent required or permitted by local law, records of your use of our systems including computers, phones and other devices and passwords. In some premises we may use fingerprint or retina scanning for access. This biometric data is Special Category Data.	• Legitimate interests • Legal obligations • Consent

Providing references in connection with you finding new employment	**Employment Data** Specifically, information on your working for us and on your performance.	• Legitimate interests
Providing information to third parties in connection with transactions that we contemplate or carry out	**Employment data** Including information on your contract and other employment data that may be required by a party to a transaction such as a prospective purchaser, seller or provider of outsourced services.	• Legitimate interests • Consent
Monitoring of diversity and equal opportunities	**Background Data** **Special Category Data** Specifically, to the extent required or permitted by local law, information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, philosophical beliefs, disability, age and other diversity markers	• Consent • Legitimate interests • Legal obligations • Public interest In relation to Special Category Data: • Employment obligations, Consent, or substantial public interest.

Monitoring and investigating compliance with law, regulations policies, codes of practice and rules both generally and specifically	**Contact Data** **Employment Data** **Background Data** Ethics Reporting Data IT Data Security and Access Data Payroll Data Communications Data Special Category Data Location Data We expect our staff to comply with our policies and rules and monitor our systems to check compliance. If we have specific concerns about compliance, we may check systems and other data to look into those concerns (e.g. log in records, records of usage and emails and documents, CCTV images). We may from time to time conduct investigations if we receive any report of non-compliance with the law and regulations or with our codes of practice, policies and rules.	• Legitimate interests • Legal obligation In relation to Special Category Data: • Employment obligations, • Legal Claims, or in limited cases substantial public interest
Disputes and legal proceedings	**Contact Data** **Employment Data** **Payroll Data** **IT Data** **Communications** **Data** **Special Category Data** **Location Data** Any other information relevant or potentially relevant to a dispute or legal proceeding affecting us.	• Legitimate interests • Legal obligation In relation to Special Category Data: • Legal Claims
Day to day business operations including marketing and customer/ client relations	**Contact Data** **Employment Data** **Audio/Visual Data** Specifically information used on global or local internal or external directories to identify what you do and how you can be contacted (to enable collaboration with colleagues and others). Any other Information relating to the work you do for us, your role and contact details including relations with current or potential customers or clients. This may include a picture of you for internal or external use.	• Legitimate interests

Carrying out staff surveys	**Survey Data** We will typically aggregate survey responses and do not require details of specific persons responding. However, if you are completing a survey electronically even if no direct identifying information is provided, you technically might be identifiable from your IP address. We are only interested in looking at the aggregated information and not any information linking individuals to survey responses.	• Legitimate interests
Maintaining appropriate business records during and after your employment or engagement	**Employment Data** Other information relating to your work, anything you do at work and your performance relevant to such records.	• Contract • Legal obligation • Legitimate interests
Emergency medical treatment	**Family Data** **Health Data** Any other information required to notify your close contact(s) of any incident at or in connection with work and to allow responsible people to administer emergency medical treatment.	• Vital interests
Acquisitions, divestitures and integrations; restructuring and relocation	**Contact Data** **Employment Data** **Background Data** **Ethics Reporting Data** **IT Data** **Security and Access** **Data Payroll Data** **Communications Data** **Special Category Data** Information will be processed and potentially shared with a third party (such as a purchaser of the business) relating to your role - as relevant to the particular context.	• Legitimate interests In relation to Special Category Data: • Employment obligations, or in limited cases Consent

2.2. Lawful basis for processing descriptions

Depending on our purpose for collecting your information, we rely on one of the lawful bases described in the table below (i.e. legally permitted reasons under GDPR/UK GDPR).

Lawful basis	Description
Contract	We require certain personal data to carry out our contractual duties and exercise our contractual rights as an employer.
Consent	In certain circumstances, we may ask for your consent (separately from any contract between us) before we collect, use, or disclose your personal data, in which case you can voluntarily choose to give or deny your consent without any negative consequences to you. In general, processing of your data in connection with employment will not be conditional on your consent. But there may be occasions where we do specific things such as seeking to monitor inclusion and diversity or providing a one-off voluntary benefit and rely on your consent to our doing so.
Legitimate interests	We may collect, use or disclose your personal data for the legitimate interests of either M Group or a third party, but only when we are confident that your privacy rights will remain appropriately protected. If we rely on our (or a third party's) legitimate interests, these interests will normally be to: operate, manage, administer our respective businesses effectively and properly. Where we require your data to pursue our legitimate interests or the legitimate interests of a third party, it will be in a way which is reasonable for you to expect as part of the running of our organization and which does not materially affect your rights and freedoms.
Legal obligation	There may be instances where we must process and retain your personal data to comply with laws or to fulfil certain legal obligations. For example, providing a safe place of work and avoiding unlawful discrimination.

Public interest	There may be instances where processing your data is necessary to perform a specific task in the public interest or for a substantial public interest which could include, for example, prevention and detection of unlawful acts such as fraud or other crime or assisting third parties prevent or detect unlawful acts or dishonesty, or for diversity and inclusiveness monitoring purposes.
Vital interests	Although unlikely, it may be necessary to process your data (including Special Category Data such as health data) to protect someone's life. In general, we will not process your data on this ground but there may be rare occasions when we need to do so, for example, if we need to process personal data to save your life and administer emergency medical treatment.
Legal claims	To establish, make or defend legal claims.
Public health	To protect against serious cross-border threats to health.

3. Who we share your personal data with

We share your personal data with the following categories of recipients:

- our group companies in order to administer human resources, staff member compensation and benefits at an international level on our People Services platform, as well as for other legitimate business purposes such as IT services/security, tax and accounting, and general business management;
- third party service providers and partners on a "need to know basis" and in accordance with applicable data privacy law. We may disclose your data if it is necessary for our legitimate interests as an organization or the interests of a third party (but we will not do this if these interests are over-ridden by your interests and rights in particular to privacy). We may also disclose your personal data if you consent, where we are legally required to disclose and in connection with criminal or regulatory investigations.

specific examples of such third parties and the circumstances in which your personal data may be disclosed to them include the following:

- any competent law enforcement body, regulatory, government agency, court or other third party (such as our professional advisers) where we believe disclosure is necessary (i) as a matter of applicable law or regulation (e.g. to provide certain salary information to tax authorities), (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person;
- a buyer (and its agents and advisers) in connection with any actual or proposed purchase, merger or acquisition of any part of our business as permitted by law and/or contract, provided that we inform the buyer it must use your personal data only for the purposes disclosed in this Notice;
- any other person with your consent to the disclosure (obtained separately from any contract between us);
- our key service providers (e.g. providers of our employee benefit plan, payroll and travel).

4. Data security and data integrity

We will ensure that appropriate measures are taken against unlawful or unauthorized processing of Employee Data, and against the loss of, or damage to, misuse, unauthorized access, disclosure, alteration or destruction of Employee Data. We have in place technical and organizational measures to maintain the confidentiality, integrity and availability of the Employee Data.

Your personal data will be stored in different locations including in your personnel file, in the relevant company's People Services systems and in other IT systems (including our email system and IT data server files). However, it is only stored within our network. The periods for which your data is held after the end of employment are set out in the Data Retention Procedure, MGS-PRO-DP-002.

5. International data transfers

Where your personal data is transferred to a third party, it may be processed in countries other than the country in which you are resident. These countries may have data protection laws that are different to the laws of your country (and, in some cases, may not be as protective).

Where we transfer your personal data to countries and territories outside of the European Economic Area and the UK, which have been formally recognized as providing an adequate level of protection for personal data, we rely on the relevant "adequacy decisions" from the European Commission and "adequacy regulations" (data bridges) from the Secretary of State in the UK.

Where the transfer is not subject to an adequacy decision or regulations, we have taken appropriate safeguards to ensure that your personal data will remain protected in accordance with this Privacy Notice and applicable laws. The safeguards we use to transfer personal data are the European Commission's Standard Contractual Clauses as issued on 4 June 2021 under Article 46(2), including the UK Addendum or the UK International Data Transfer Agreement permitted under Article 46(2) of the UK GDPR for the transfer of data originating in the UK.

6. Your data protection rights

Individuals located in the UK and EEA have the following data protection rights. To exercise any of them see specific instructions below or contact us using the contact details provided under the “How to contact us” heading below.

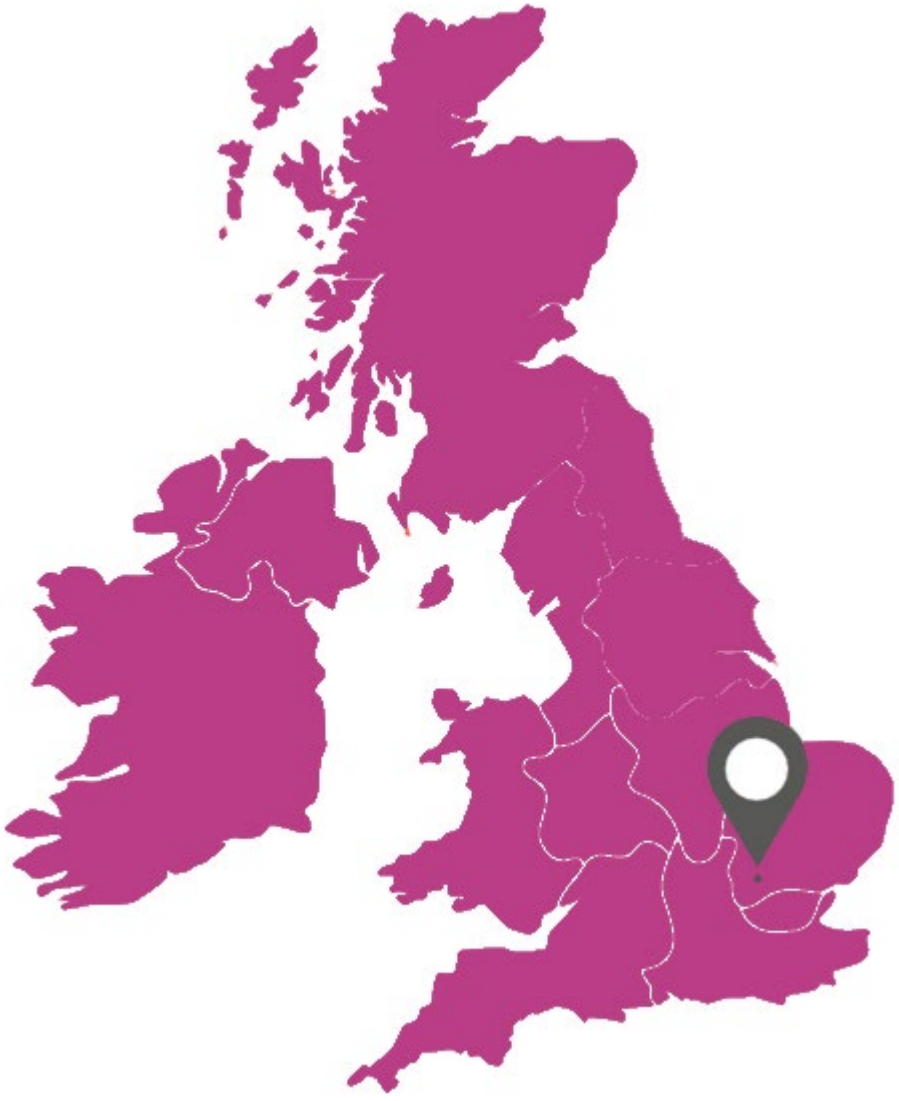
- You may access, correct, update or request deletion of your personal data.
- You can object to processing of your personal data, ask us to restrict processing of your personal data or request portability of your personal data, (i.e. your data to be transferred in a readable and standardized format).
- If we have collected and processed your personal data with your consent, then you can withdraw your consent at any time by using the contact details provided under the “How to contact us” heading below. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal data conducted in reliance on lawful processing grounds other than consent.
- You have the right to complain to a supervisory authority about our collection and use of your personal data. For more information, please contact your local supervisory authority. Contact details for supervisory authorities in Europe are available here and for the UK here. Certain supervisory authorities may require that you exhaust our own internal complaints process before looking into your complaint.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

7. How to contact us

We trust you are clear about how we manage your data but if you are unhappy with how we’ve handled your information or you would like to exercise your rights, please contact our Data Protection Officer using this email address: **DP@mgroupservices.com**.

M GROUP



Head office

Abel Smith House | Gunnels Wood Road
Stevenage | Hertfordshire SG1 2ST
TEL: 01438 743 744
www.mgroupservices.com