Home House
10 Church Street Old Isleworth London TW7 6DA

T: +44 (0) 20 8232 7000
M-is.com

Employment Data Protection Policy (GDPR Compatible)

Introduction

This Policy sets out the obligations of M-Integrated Solutions PLC (M), a company registered in England under number 6311065, whose registered office is at Home House 10 Church Street Old Isleworth London TW7 6DA. M regards data protection and the rights of its employees (in this context, "employee data subjects") in respect of their personal data under Data Protection Law (all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, EU Regulation 2016/679 General Data Protection Regulation (GDPR), the Data Protection Act 2018, and any successor legislation or other directly applicable EU regulation relating to data protection and privacy for as long as, and to the extent that, EU law has legal effect in the UK).

This Policy sets out our obligations regarding the collection, processing, transfer, storage, and disposal of personal data relating to employee data subjects. The procedures and principles set out herein must be followed at all times by M, its employees, independent professional contributors, contractors, and other parties working on behalf of M.

Definitions

consent means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

data controller means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data.

data processor means a natural or legal person or organisation which processes personal data on behalf of a data controller.

data subject means a living, identified, or identifiable natural person about whom M holds personal data (in this context, employee data subjects).

EEA means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway.

personal data means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject. personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

processing means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

special category personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

Scope

M is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it works.

M's Data Protection Officer is Rathan Dubey, telephone: +44 208 232 7051, email: rathan.dubey@m-is.com

The Data Protection Officer is responsible, working together with the HR and Organisational Development team for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

All Line Managers are responsible for ensuring that all employees, independent professional contributors, contractors, or other parties working on behalf of M comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

- if there is any uncertainty relating to the lawful basis on which employee personal data is to be collected, held, and/or processed
- if consent is being relied upon in order to collect, hold, and process employee personal data
- if there is any uncertainty relating to the retention period for any particular type(s) of employee personal data
- if any new or amended privacy notices or similar privacy-related documentation are required
- if any assistance is required in dealing with the exercise of an employee data subject's rights (including, but not limited to, the handling of subject access requests)
- if a personal data breach (suspected or actual) has occurred
- if there is any uncertainty relating to security measures (whether technical or organisational) required to protect employee personal data
- if employee personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors)

- if employee personal data is to be transferred outside of the EEA and there are questions relating to the legal basis on which to do so
- when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment
- when employee personal data is to be used for purposes different to those for which it was originally collected
- if any automated processing, including profiling or automated decision-making, is to be carried out
- if any assistance is required in complying with the law applicable to direct marketing

The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The GDPR sets out the following principles with which anyone handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

- processed lawfully, fairly, and in a transparent manner in relation to the data subject
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures

The Rights of Data Subjects

The GDPR sets out the following key rights applicable to data subjects:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure (also known as the ‘right to be forgotten’)
- the right to restrict processing
- the right to data portability
- the right to object
- rights with respect to automated decision-making and profiling

Transparent Data Processing

Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the GDPR states that processing of personal data shall be lawful only if at least one of the following applies:

- the data subject has given consent to the processing of their personal data for one or more specific purposes
- the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract
- the processing is necessary for compliance with a legal obligation to which the data controller is subject
- the processing is necessary to protect the vital interests of the data subject or of another natural person
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller
- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

If the personal data in question is special category personal data (also known as sensitive personal data), at least one of the following conditions must be met in addition to one of the conditions set out above:

- the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so)
- the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject)
- the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects
- the processing relates to personal data which is manifestly made public by the data subject
- the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity
- the processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject

- the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR
- the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy)
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing any personal data, the following shall apply:

- consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent
- where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters
- data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly
- if personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject
- where special category personal data is processed, M shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent
- in all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that M can demonstrate its compliance with consent requirements

Specified, Explicit, and Legitimate Purposes

M collects and processes the employee personal data set out in this Policy. This includes personal data collected directly from employee data subjects and personal data obtained from third parties.

M only collects, processes, and holds employee personal data for the specific purposes or for other purposes expressly permitted by Data Protection Law.

Employee data subjects shall be kept informed at all times of the purpose or purposes for which M uses their personal data.

Relevant and Limited Data Processing

M will only collect and process employee personal data for and to the extent necessary for the specific purpose or purposes of which employee data subjects have been informed (or will be informed).

Employees, independent professional contributors, contractors, or other parties working on behalf of M may collect employee personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

Employees, independent professional contributors, contractors, or other parties working on behalf of M may process employee personal data only when the performance of their job duties requires it. Employee personal data held by M cannot be processed for any unrelated reasons.

Accuracy and updating of Data

M shall ensure that all employee personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of an employee data subject.

The accuracy of employee personal data shall be checked when it is collected and at regular intervals thereafter. If any employee personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

It is the responsibility of individual employee data subjects to ensure that the personal data they have provided to M is kept up-to-date. If any such personal data changes, employees should ensure that the relevant member of staff and/or department is informed as soon as is reasonably possible. M relies on the cooperation of its employees to help meet its obligations under Data Protection Law.

Data Retention

M shall not keep employee personal data for any longer than is necessary in light of the purpose or purposes for which it was originally collected, held, and processed.

When employee personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it securely and without delay.

For full details of M's approach to data retention, including retention periods for specific personal data types held by M, please refer to our Data Retention Policy.

Secure Processing

M shall ensure that all employee personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

All technical and organisational measures taken to protect employee personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of employee personal data.

Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all employee personal data as follows:

- only those with a genuine need to access and use employee personal data and who are authorised to do so may access and use it
- employee personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed
- authorised users must always be able to access employee personal data as required for the authorised purpose or purposes

Accountability and Record-Keeping

The Data Protection Officer shall be responsible, working together with the HR and Organisational Development team for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

M shall follow a 'privacy by design' approach at all times when collecting, holding, and processing employee personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of employee data subjects.

All employees, independent professional contributors, contractors, or other parties working on behalf of M shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

M's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

M shall keep written internal records of all employee personal data collection, holding, and processing, which shall incorporate the following information:

- the name and details of M, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared)
- the purposes for which M collects, holds, and processes employee personal data
- M's legal basis or bases (including, where applicable, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing em ployee personal data
- details of the categories of employee personal data collected, held, and processed by M, and the categories of employee data subject to which that personal data relates
- details of any transfers of employee personal data to non-EEA countries including all mechanisms and security safeguards
- details of how long employee personal data will be retained by M (please refer to M's Data Retention Policy)
- details of employee personal data storage, including location(s)
- detailed descriptions of all technical and organisational measures taken by M to ensure the security of employee personal data

Data Protection Impact Assessments and Privacy by Design

In accordance with the 'privacy by design' principles, M shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of employee personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of employee data subjects.

The principles of 'privacy by design' should be followed at all times when collecting, holding, and processing employee personal data. The following factors should be taken into consideration:

- the nature, scope, context, and purpose or purposes of the collection, holding, and processing
- the state of the art of all relevant technical and organisational measures to be taken
- the cost of implementing such measures
- the risks posed to employee data subjects and to M, including their likelihood and severity

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- the type(s) of employee personal data that will be collected, held, and processed
- the purpose(s) for which employee personal data is to be used
- M's objectives
- how employee personal data is to be used
- the parties (internal and/or external) who are to be consulted
- the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed
- risks posed to employee data subjects
- risks posed both within and to M
- proposed measures to minimise and handle identified risks

Keeping Data Subjects Informed

M shall provide the information to every data employee data subject:

- where employee personal data is collected directly from employee data subjects, those employee data subjects will be informed of its purpose at the time of collection; and
- where employee personal data is obtained from a third party, the relevant employee data subjects will be informed of its purpose:
  - if the personal data is used to communicate with the employee data subject, when the first communication is made
  - if the personal data is to be transferred to another party, before that transfer is made
  - as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided in the form of a privacy notice:

- details of M including, but not limited to, all relevant contact details, and the names and contact details of any applicable representatives and its Data Protection Officer
- the purpose(s) for which the employee personal data is being collected and will be processed and the lawful basis justifying that collection and processing
- where applicable, the legitimate interests upon which M is justifying its collection and processing of the employee personal data
- where the employee personal data is not obtained directly from the employee data subject, the categories of personal data collected and processed
- where the employee personal data is to be transferred to one or more third parties, details of those parties
- where the employee personal data is to be transferred to a third party that is located outside of the EEA, details of that transfer, including but not limited to the safeguards in place
- details of applicable data retention periods
- details of the employee data subject's rights under the GDPR
- details of the employee data subject's right to withdraw their consent to M's processing of their personal data at any time (where applicable)
- details of the employee data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the GDPR)
- where the employee personal data is not obtained directly from the employee data subject, details about the source of that personal data

- where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the employee personal data and details of any consequences of failing to provide it
- details of any automated decision-making or profiling that will take place using the employee personal data, including information on how decisions will be made, the significance of those decisions, and any consequences

Data Subject Access

Employee data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which M holds about them, what it is doing with that personal data, and why.

Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to our Data Protection Officer.

Responses to SARs must normally be made within one month of receipt; however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

M does not charge a fee for the handling of normal SARs. M reserves the right to charge reasonable fees for additional copies of information that has already been supplied to an employee data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

Employee data subjects have the right to require M to rectify any of their personal data that is inaccurate or incomplete.

M shall rectify the employee personal data in question, and inform the employee data subject of that rectification, within one month of the employee data subject informing M of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the employee data subject shall be informed.

In the event that any affected employee personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Employee data subjects have the right to request that M erases the personal data it holds about them in the following circumstances:

- it is no longer necessary for M to hold that employee personal data with respect to the purpose(s) for which it was originally collected or processed
- the employee data subject wishes to withdraw their consent (where applicable) to M holding and processing their personal data
- the employee data subject objects to M holding and processing their personal data (and there is no overriding legitimate interest to allow M to continue doing so)
- the employee personal data has been processed unlawfully;
- the employee personal data needs to be erased in order for M to comply with a particular legal obligation

Unless M has reasonable grounds to refuse to erase employee personal data, all requests for erasure shall be complied with, and the employee data subject informed of the erasure, within one month of receipt of the employee data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the employee data subject shall be informed.

In the event that any employee personal data that is to be erased in response to an employee data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing

Employee data subjects may, in certain limited circumstances, request that M ceases processing the personal data it holds about them. If an employee data subject makes a valid request, M shall retain only the amount of employee personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected employee personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Data Portability

M processes personal data relating to employees using automated means.

Where employee data subjects have given their consent to M to processing their personal data in such a manner, or the processing is otherwise required for the performance of a contract between M and the employee data subject, employee data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

Where technically feasible, if requested by an employee data subject, personal data shall be sent directly to the required data controller.

All requests for copies of employee personal data shall be complied with within one month of the employee data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the employee data subject shall be informed.

Objections to Personal Data Processing

Employee data subjects have the right to object to M processing their personal data based on legitimate interests, for direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where an employee data subject objects to M processing their personal data based on its legitimate interests, M shall cease such processing immediately, unless it can be demonstrated that M's legitimate grounds for such processing override the employee data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where an employee data subject objects to M processing their personal data for direct marketing purposes, M shall cease such processing promptly.

Where an employee data subject objects to M processing their personal data for scientific and/or historical research and statistics purposes, the employee data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". M is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

Automated Processing, Automated Decision-Making, and Profiling

The activities described below are generally prohibited under Data Protection Law where the resulting decisions have a legal or similarly significant effect on data subjects unless one of the following applies:

- the data subject has given their explicit consent
- the processing is authorised by law
- the processing is necessary for the entry into, or performance of, a contract between M and the data subject

If special category personal data is to be processed in this manner, such processing can only be carried out if one of the following applies:

- the data subject has given their explicit consent
- the processing is necessary for reasons of substantial public interest

Where decisions are to be based solely on automated processing (including profiling), employee data subjects have the right to object, to challenge such decisions, request human intervention, to express their own point of view, and to obtain an explanation of the decision from M. Employee data subjects must be explicitly informed of this right at the first point of contact.

In addition to the above, clear information must be provided to employee data subjects explaining the logic involved in the decision-making or profiling, and the significance and envisaged consequences of the decision or decisions.

When employee personal data is used for any form of automated processing, automated decision-making, or profiling, the following shall apply:

- appropriate mathematical or statistical procedures shall be used
- technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected
- all personal data to be processed in this manner shall be secured in order to prevent discriminatory effects arising

Personal Data

M holds a range of personal data about its employees. Employee personal data shall be collected, held, and processed in accordance with employee data subjects' rights and M's obligations under the GDPR and with this Policy. M may collect, hold, and process the employee personal data detailed:

- identification information relating to employees:
  - name
  - contact details
- equal opportunities monitoring information:
  - age
  - gender
  - ethnicity
  - nationality
  - religion
- health records:
  - details of sick leave
  - medical conditions
  - disabilities
  - prescribed medication

• employment records:

- interview notes
- CVs, application forms, covering letters, and similar documents
- assessments, performance reviews, and similar documents
- details of remuneration including salaries, pay increases, bonuses, commission, overtime, benefits, and expenses
- details of trade union membership (where applicable)
- employee monitoring information, below, for further information)
- records of disciplinary matters including reports and warnings, both formal and informal
- details of grievances including documentary evidence, notes from interviews, procedures followed, and outcomes

Equal Opportunities Monitoring Information

M collects, holds, and processes certain information for the purposes of monitoring equal opportunities. Some of the personal data collected for this purpose, such as details of ethnic origin and religious beliefs, falls within the GDPR's definition of special category data. Where possible, such data will be anonymised. Where special category personal data remains, it will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data.

Non-anonymised equal opportunities monitoring information shall be accessible and used only by the HR and Organisational Development team and shall not be revealed to other employees, independent professional contributors, contractors, or other parties working on behalf of M without the express consent of the employee data subject(s) to whom such data relates, except in exceptional circumstances where it is necessary to protect the vital interests of the employee data subject(s) concerned.

Equal opportunities monitoring information will only be collected, held, and processed to the extent required to prevent, reduce, and stop unlawful discrimination in line with the Equality Act 2010, and to ensure that recruitment, promotion, training, development, assessment, benefits, pay, terms and conditions of employment, redundancy, and dismissals are determined on the basis of capability, qualifications, experience, skills, and productivity.

Employee data subjects have the right to request that M does not keep equal opportunities monitoring information about them.

Health Records

M holds health records on employee data subjects which are used to assess the health, wellbeing, and welfare of employees and to highlight any issues which may require further investigation. In particular, M places a high priority on maintaining health and safety in the workplace, on promoting equal opportunities, and on preventing discrimination on the grounds of disability or other medical conditions. In most cases, health data on employees falls within the GDPR's definition of special category data. Any and all data relating to employee data subjects' health, therefore, will be collected, held, and processed strictly in accordance with the conditions for processing special category personal data.

Health records shall be accessible and used only by the Head of Finance and the HR and Organisational Development team, and shall not be revealed to other employees, independent professional contributors, contractors, or other parties working on behalf of M (without the express consent of the employee data subject(s) to whom such data

relates), except in exceptional circumstances where it is necessary to protect the vital interests of the employee data subject(s) concerned, and such circumstances satisfy one or more of the conditions set out in of this Policy.

Health records will only be collected, held, and processed to the extent required to ensure that employees are able to perform their work correctly, legally, safely, and without unlawful or unfair impediments or discrimination.

Employee data subjects have the right to request that M does not keep health records about them.

Benefits

In cases where employee data subjects are enrolled in benefit schemes which are provided by M, it may be necessary from time to time for third party organisations to collect personal data from relevant employee data subjects.

Prior to the collection of such data, employee data subjects will be fully informed of the personal data that is to be collected, the reasons for its collection, and the way(s) in which it will be processed.

M shall not use any such personal data except insofar as is necessary in the administration of the relevant benefits schemes.

Employee Monitoring

M may from time to time monitor the activities of employee data subjects. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. In the event that monitoring of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a matter of equal severity, justify covert monitoring), employee data subjects will be informed of the exact nature of the monitoring in advance.

Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's normal duties.

Monitoring will only take place if M considers that it is necessary to achieve the benefit it is intended to achieve. Personal data collected during any such monitoring will only be collected, held, and processed for reasons directly related to (and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects' rights and M's obligations under the GDPR.

M shall ensure that there is no unnecessary intrusion upon employee data subjects' personal communications or activities, and under no circumstances will monitoring take place outside of an employee data subject's normal place of work or work hours, unless the employee data subject in question is using M equipment or other facilities including, but not limited to, M email, M intranet, or a virtual private network ("VPN") service provided by M for employee use.

Data Security - Transferring Personal Data and Communications

M shall ensure that the following measures are taken with respect to all communications and other transfers involving employee personal data:

- all emails containing employee personal data must be encrypted
- all emails containing employee personal data must be marked confidential
- employee personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances
- employee personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- employee personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted

- where employee personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data
- where employee personal data is to be transferred in hardcopy form it should be passed directly to the recipient
- all employee personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked confidential

Data Security - Storage

M shall ensure that the following measures are taken with respect to the storage of employee personal data:

- all electronic copies of employee personal data should be stored securely using passwords and data encryption
- all hardcopies of employee personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar
- all employee personal data stored electronically should be backed up
- no employee personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to M or otherwise
- no employee personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of M and employee personal data may only be transferred to devices belonging to independent professional contributors, contractors, or other parties working on behalf of M where the party in question has agreed to comply fully with the letter and spirit of this Policy and of Data Protection Law, including but not limited to the GDPR, (which may include demonstrating to M that all suitable technical and organisational measures been taken)

Data Security - Disposal

When any employee personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to M's Data Retention Policy.

Data Security - Use of Personal Data

M shall ensure that the following measures are taken with respect to the use of employee personal data:

- no employee personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of M requires access to any employee personal data that they do not already have access to, such access should be formally requested from the HR and Organisational Development team
- no employee personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of M or not, without the authorisation of the HR and Organisational Development team
- employee personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, independent professional contributors, contractors, or other parties at any time
- if employee personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it

Data Security - IT Security

M shall ensure that the following measures are taken with respect to IT and information security:

- all passwords used to protect employee personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.
- under no circumstances should any passwords be written down or shared between any employees, independent professional contributors, contractors, or other parties working on behalf of M, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords
- all software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Our IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible
- no software may be installed on any Company-owned computer or device without the prior approval of the Group Head of IT

Organisational Measures

M shall ensure that the following measures are taken with respect to the collection, holding, and processing of employee personal data:

- all employees, independent professional contributors, contractors, or other parties working on behalf of M shall be made fully aware of both their individual responsibilities and our responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy
- only employees, independent professional contributors, contractors, or other parties working on behalf of M that need access to, and use of, employee personal data in order to carry out their assigned duties correctly shall have access to employee personal data held by M
- all sharing of employee personal data shall comply with the information provided to the relevant employee data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data
- all employees, independent professional contributors, contractors, or other parties working on behalf of M handling employee personal data will be appropriately trained to do so
- all employees, independent professional contributors, contractors, or other parties working on behalf of M handling employee personal data will be appropriately supervised
- all employees, independent professional contributors, contractors, or other parties working on behalf of M handling employee personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to employee personal data, whether in the workplace or otherwise
- methods of collecting, holding, and processing employee personal data shall be regularly evaluated and reviewed
- all employee personal data held by M shall be reviewed periodically, as set out in M's Data Retention Policy
- the performance of those employees, independent professional contributors, contractors, or other parties working on behalf of M handling employee personal data shall be regularly evaluated and reviewed
- all employees, independent professional contributors, contractors, or other parties working on behalf of M handling employee personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract

- all independent professional contributors, contractors, or other parties working on behalf of M handling employee personal data must ensure that any and all of their employees who are involved in the processing of employee personal data are held to the same conditions as those relevant employees of M arising out of this Policy and Data Protection Law
- where any agent, contractor or other party working on behalf of M handling employee personal data fails in their obligations under this Policy, that party shall indemnify and hold harmless M against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure

Sharing Personal Data

M may only share employee personal data with third parties if specific safeguards are in place.

Employee personal data may only be shared with other employees, independent professional contributors, contractors, or other parties working on behalf of M if the recipient has a legitimate, job-related need-to-know. If any employee personal data is to be shared with a third party located outside of the European Economic Area, the provisions below, shall also apply.

Where a third-party data processor is used, that processor shall process personal data on behalf of M (as data controller) only on the written instruction of M.

Employee personal data may only be shared with third parties in the following circumstances:

- the third party has a legitimate need to know the information for the purpose of providing services to M under a contract
- the sharing of the employee personal data concerned complies with the privacy notice provided to the affected employee data subjects and, if required, the employees concerned have consented to the sharing of their personal data
- the third-party recipient has agreed to comply with all applicable data security standards, policies, and procedures, and has put in place adequate security measures to protect the employee personal data
- (where applicable) the transfer complies with any cross-border transfer restrictions
- a fully executed written agreement containing GDPR-approved third party clauses has been entered into with the third-party recipient

Transferring Personal Data to a Country Outside the EEA

M may from time to time transfer ('transfer' includes making available remotely) employee personal data to countries outside of the EEA.

The transfer of employee personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data
- the transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority

- the transfer is made with the informed and explicit consent of the relevant employee data subject(s)
- the transfer is necessary for the performance of a contract between the employee data subject and M (or for pre-contractual steps taken at the request of the employee data subject)
- the transfer is necessary for important public interest reasons
- the transfer is necessary for the conduct of legal claims
- the transfer is necessary to protect the vital interests of the employee data subject or other individuals where the employee data subject is physically or legally unable to give their consent
- the transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

All personal data breaches concerning employee personal data must be reported immediately to M's Data Protection Officer.

If an employee, agent, contractor, or other party working on behalf of M becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of employee data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of employee data subjects, the Data Protection Officer must ensure that all affected employee data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- the categories and approximate number of data subjects concerned
- the categories and approximate number of personal data records concerned
- the name and contact details of M's data protection officer (or other contact point where more information can be obtained)
- the likely consequences of the breach
- details of the measures taken, or proposed to be taken, by M to address the breach including, where appropriate, measures to mitigate its possible adverse effects

Implementation of Policy

This Policy shall be deemed effective as of the date below. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Data Protection Officer

Rathan Dubey, Head of Information Technology

D: +44 208 232 7051

E: rathan.dubey@m-is.com

Last Reviewed on: 12 November 2019

Jim Curley
Managing Director