GENERAL DATA PROTECTION REGULATION PRIVACY POLICY

October 2023

1. Introduction

This Privacy Standard sets out how MGTS manage the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Privacy Standard applies to all Company Personnel. You must read, understand, and comply with this Privacy Standard when Processing Personal Data on our behalf and as may be required from time to time, attend training on its requirements. This Privacy Standard sets out what we expect from you for the Company to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Privacy Standard may result in disciplinary action.

This Privacy Standard (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO/DPM.

2. Interpretation

Definitions:

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members, and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Manager (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, the term Data Protection Manager (**DPM**) is used as a person who acts as a point of engagement with Data Protection issues.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein, and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy or notice) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data, for example any IT Security policy.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

3. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The Board and individual business area managers are responsible for seeking to ensure all Company Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

There is a nominated individual with specific responsibility for Data Protection. MGTS Data Protection is the collective responsibility of the management team. The Business Systems and Contracts Manager takes the lead on Data. Protection.

Please contact the DPO with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see paragraph 5.1 below);

(b) if you need to draft Privacy Notices or Fair Processing Notices (see paragraph 5.3 below);

(c) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 9 below);

(d) if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 10.1 below);

(e) if there has been a Personal Data Breach (paragraph 10.2 below);

(f) if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 12);

(g) whenever you are engaging in a significant new, or change in, Processing activity or plan to use Personal Data for purposes others than what it was collected for;

(h) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 13.6 below); or

(i) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 13.7 below).

4. Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Lawfulness, fairness, transparency

5.1 Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing. The restrictions ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent.

(b) the Processing is necessary for the performance of a contract with the Data Subject.

(c) to meet our legal compliance obligations.

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

The Company must identify and document the legal ground being relied on for each Processing activity, for existing Processing activities the Company have already undertaken an exercise to establish the legal ground for Processing.

5.2 Consent

A Data Controller must only process Personal Data based on one or more of the lawful grounds set out in the GDPR, which include Consent.

The Company has identified that as at the date of this Privacy Standard that only a very limited aspect of marketing activity might require Consent, systems have been established to address this effectively, this will be kept under review.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Where Consent is the appropriate approach, you will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

The Company have identified the activities which require Consent needs to be gained and have automated that procedure in most cases. You simply need to follow the guidance provided to You.

5.3 Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand it.

Where we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we shall provide the Data Subject with information required by the GDPR, which will usually including how and why we will use, Process, disclose, protect, and retain that Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR promptly after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

N.B. Purchasing lists of contacts for sales and marketing purposes requires particular care. Privacy and Electronic Communication Regulations 2003 (as amended) as well as GDPR have an impact on what such data can be used for and how. Such lists should only be acquired and utilised in accordance with direction from the Sales Director and in accordance with the Company's then current Sales and Marketing Guidance.

6. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different, or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have provided Consent where necessary, if you consider this might arise, please speak to the Data Protection Manager.

7. Data minimisation

Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing the duties of your employment requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines. If you are in doubt as to the approach you should take, please speak to the DPM before erasing Personal Data.

8. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without undue delay when inaccurate.

You will try and ensure that the Personal Data used and held by the Company is accurate, complete, kept up to date and relevant to the purpose for which it is collected. The accuracy of Personal Data should be checked at the point of collection and at reasonably regular intervals as appropriate, inaccurate, or out-of-date Personal Data, should be archived and/or destroyed.

9. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is reasonably necessary for the purposes for which the data is processed.

The Company will maintain retention policies and procedures for Personal Data deletion after a reasonable time for the purposes for which it was being held, unless legally required to be kept for a minimum time.

10. Security integrity and confidentiality

10.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage.

We have and will continue to develop, implement, and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity, and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and/or are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users can access the Personal Data when they need it for authorised purposes.

You must comply with any information security policy we provide.

10.2 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulatory and, in certain instances, the Data Subject.

We have put in place procedures to deal with this process.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches. You should preserve all evidence relating to the potential Personal Data Breach.

11. Transfer limitation

The Company have no plans to allow transfer of Personal Data outside of the UK or EEA, if you consider any activity may involve such a transfer, please notify the DPM, you may not proceed with the transfer until you are informed in writing by the DPM or a Director of the Company.

The GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

Although we do not expect to transfer Personal Data outside of the EEA, the following is useful to understand. The Company may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms.

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

You must comply with the Company's guidelines on cross border data transfers.

12. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time (this does not mean they can require the Company to stop Processing where the Condition for Processing is not Consent based);

(b) receive certain information about the Data Controller's Processing activities.

(c) request access to their Personal Data that we hold.

(d) prevent our use of their Personal Data for direct marketing purposes.

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.

(f) restrict Processing in specific circumstances.

(g) challenge Processing which has been justified based on our legitimate interests or in the public interest.

(h) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else.

(i) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms.

(j) make a complaint to the supervisory authority; and

(k) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format, we do not expect this to apply to the business of the Company.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to your supervisor and the DPM, do not attempt to respond to a request for information or action in relation to Data Subject rights.

13. Accountability

13.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company has taken steps to ensure that it will have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy.

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects, this is unlikely in relation to most of the activities the Company are involved with, however if you are involved in any new activity which may involve a concern in this respect, please liaise with the DPM before commencing the activity.

(c) integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices;

(d) regularly training Company Personnel on the GDPR, this Privacy Standard, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

13.2 Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities.

The Company must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Company's record keeping guidelines. In most cases, Consent recording is automatic if you use the correct supplied technology.

13.3 Training and audit

The Company will ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We also intend to regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

13.4 Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

We have assessed what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by considering the following:

(a) the state of the art.

(b) the cost of implementation.

(c) the nature, scope, context, and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high-risk Processing.

Further guidance will be provided by the DPM, If your role involves implementing major system or business change programs involving the Processing of Personal Data including:

(e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(f) Automated Processing including profiling and ADM.

(g) large scale Processing of Sensitive Data; and

(h) large scale, systematic monitoring of a publicly accessible area.

If a DPIA is required the DPM will assist and guide you through the process, it is not complex, it does however require:

(i) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate.

(j) an assessment of the necessity and proportionality of the Processing in relation to its purpose.

(k) an assessment of the risk to individuals; and

(l) the risk mitigation measures in place and demonstration of compliance.

13.5 Direct marketing

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text, or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details during a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

13.6 Sharing Personal Data

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. Key commercial arrangements have been identified and appropriate documentation has been provided to them.

You may only share the Personal Data we hold with another employee, agent, or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services.

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained.

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and

(d) the arrangement is documented correctly.

14. Changes to this Privacy Standard

We reserve the right to change this Privacy Standard at any time so please check back regularly to obtain the latest copy of this Privacy Standard. We last revised this Privacy Standard on 12 May 2018.

This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where the Company operates.

David Bridgens
Chief Executive

Reviewed: October 2023	**Next Review:** October 2024