

## Purpose and Scope

Mitie Group plc and its subsidiaries (together "Mitie") is committed to complying with its legal obligations under the UK GDPR, the Data Protection Act 2018 and, the General Data Protection Regulation 2016 ("GDPR") relating to the protection of the rights and freedoms of individuals whose personal data Mitie obtains or generates as part of its business operations.

This Data Privacy Policy sets out how Mitie handles the personal data of our employees, customers, suppliers, contractors, and other third-party data subjects. It applies to all personal data we process regardless of the media on which it is stored or the source from which it is obtained.

Please contact [privacy@mitie.com](mailto:privacy@mitie.com) with any questions about the operation of this Data Privacy Policy or Data Privacy legislation. Or, if you have any concerns, this Data Privacy Policy has not been or is not being followed.

## Application

This Privacy Policy applies to all Mitie personnel who must read it carefully and comply with it when processing personal data on Mitie's behalf.

No third party should access (or attempt to access) personal data held by Mitie without first agreeing to be bound by (i) appropriate confidentiality obligations no less onerous than that Mitie is committed to, and (ii) contractual terms which gives Mitie the right to audit compliance with Data Protection legislation. Suppliers, contractors, and any other third parties working with Mitie, who have or may have access to personal data, will also be expected to read and understand this Data Privacy Policy and comply with their obligations under all applicable Data Protection regulations.

Any breach of Data Protection legislation, this Data Privacy Policy or related policies and procedures may result in disciplinary action and be considered a criminal offence. In which case, we will report this matter to the relevant authorities.

## Definitions

**'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an 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 natural person.

**'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether 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.

**'Restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future.

**'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

**‘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 are not attributed to an identified or identifiable natural person.

**‘Filing system’** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

**‘controller’** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; (but see section 6 of the 2018 Act);

**‘processor’** means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

**‘recipient’** means a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with domestic law shall not be regarded as recipients; the processing of those data by those public authorities shall follow the applicable data protection rules according to the purposes of the processing.

**‘Third party’** means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

- a) ‘Public authority’ and ‘public body’ are to be interpreted in accordance with section 7 of the 2018 Act and provision made under that section.

**‘consent’** of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**‘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.

**‘Genetic data’** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result from an analysis of a biological sample from the natural person in question.

**‘Biometric data’** means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.

**‘data concerning health’** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

**‘representative’** means a natural or legal person established in the United Kingdom who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor regarding their respective obligations under this Regulation.

'Third country' means a country or territory outside the United Kingdom.

## Data Protection Officer

Mitie's Data Protection Officer ("DPO") is responsible for overseeing this Privacy Policy and for developing related policies and procedures. That post is held by Katherine Woods, Deputy General Counsel ([katherine.woods@mitie.com](mailto:katherine.woods@mitie.com)).

The DPO is accountable to the Board of Directors Mitie for managing personal data within Mitie and ensuring that compliance with data protection legislation and good practice can be demonstrated. The DPO is also responsible for, amongst other things, procedures such as the Subject Access Request Procedure and regularly reviewing Mitie's register of processing in the light of any changes to Mitie's activities and any additional requirements identified through data protection impact assessments.

## Data Protection Principle

Mitie recognises that maintaining the confidentiality, integrity, and availability of personal data is a critical responsibility. It has designed its policies and procedures to comply with the data protection principles defined by Chapter 2, Article 5 of UK GDPR when processing personal information details of which are below:

### (a) lawfulness, fairness, transparency

**Lawfulness** – A lawful basis must always be identified before processing personal data. These are often referred to as the "conditions for processing", for example, consent or legitimate interest.

**Fairness** – For processing to be fair, the data controller must make certain information available to the data subjects. This applies whether the personal data was obtained directly from the data subjects or other sources.

**Transparency** – UK GDPR includes rules on providing privacy-related information to data subjects in Articles 12, 13 and 14. These are detailed and specific, emphasising making privacy notices understandable and accessible. The information must be communicated to the data subject in an intelligible form using clear and plain language. The specific information provided to the data subject must, as a minimum, include:

- The Controller's identity and contact details and, if any, of the Controller's representative.
- The contact details of the Data Protection Officer.
- The purpose of processing the personal data as well as the legal basis for the processing.
- The period for which the personal data will be processed, including storage.
- The existence of the rights to request access, rectification, erasure, or to object to the processing, and the conditions (or lack of conditions) to exercising these rights, such as whether the lawfulness of previous processing will be affected.
- The categories of personal data concerned.
- Where applicable, the recipients or categories of recipients of the personal data.
- Where applicable, that the Controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data; and
- any further information necessary to guarantee fair processing.

(b) Personal data can only be collected for specific, explicit, and legitimate purposes

Data obtained for specified purposes, where Mitie is the Data Controller, must not be used for a purpose that differs from those notified to the ICO as part of Mitie's ICO registrations or those purposes notified to the individual data subject concerned.

(c) Personal data must be adequate, relevant, and limited to what is necessary for processing

Mitie must not collect information that is not strictly necessary for the purpose for which it is obtained. All media through which data is collected (whether electronic or paper-based) must include a fair processing statement or link to <https://www.mitie.com/footer-links/privacy/>.

The DPO will ensure that all data collection methods are regularly reviewed to ensure that collected data continues to be adequate, relevant, and not excessive.

(d) Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

All staff engaged in processing personal data for or on behalf of Mitie must be trained in the importance of collecting accurate data and maintaining it. Data that is stored by Mitie must be reviewed and updated as necessary, and no data should be kept unless it is reasonable to assume that it is accurate.

It is also the data subject's responsibility to ensure that the data held by Mitie is accurate and up to date. Registration or application forms completed by a data subject should therefore include a statement that the data contained in the form is correct at the submission date. In addition, Mitie personnel, clients, suppliers and other relevant third parties are required to notify Mitie of any relevant changes in circumstance to enable personal records to be updated accordingly.

The DPO is responsible for assessing the appropriateness of organisation-wide measures. In doing so, the DPO The DPO is responsible for ensuring that appropriate group-wide procedures and policies are in place to keep personal data accurate and up to date, considering the volume of data collected, the speed with which it might change and any other relevant factors.

Mitie must respond to requests for rectification from data subjects within one month, and this can be extended to a further two months for complex requests. If Mitie decides not to comply with the request, Mitie must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

Where third-party organisations may have been passed inaccurate or out-of-date personal data, they must be informed that the information is incorrect or outdated and is not to be used to inform decisions about the individuals concerned. Any correction to the personal data must be passed to the third party.

(e) Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

Where personal data is retained beyond the processing date, it will be appropriately minimised and protected (through methods such as encryption, anonymisation and pseudonymisation).

Personal data will be retained in line with documented records retention schedules. Once its retention date is passed, it must be securely destroyed as set out in Mitie's Information Security Management System. The DPO must specifically approve any data retention that exceeds the retention periods defined in the documented records retention schedule. The justification must be in line with the requirements of the data protection legislation. All approvals and related justifications must be maintained as an evidentiary record.

**(f) Personal data must be processed in a manner that ensures the appropriate security**

Risk assessments must be undertaken relating to all operations where Mitie controls or processes personal data. A risk assessment must include consideration of the extent of possible damage or loss that might be caused to individuals (e.g., staff or customers) if a security breach occurs, the effect of any security breach on Mitie itself, and any likely reputational damage, including the possible loss of customer trust.

When assessing appropriate technical measures for individual processing activities, the following should be considered:

- Password protection.
- Automatic locking of idle terminals.
- Removal of access rights for USB and other memory media.
- Virus checking software and firewalls.
- Role-based access rights, including those assigned to temporary staff.
- Encryption of devices that leave Mitie's premises, such as laptops.
- Security of local and wide area networks.
- Privacy-enhancing techniques such as pseudonymisation and anonymisation; and
- Identifying and applying appropriate international security standards relevant to Mitie.

Further information can be found in the Mitie Acceptable Usage Policy on the protection and use of data.

The DPO is responsible for assessing the appropriateness of organisation-wide measures. In doing so, the DPO will consider the following:

- The appropriate training levels throughout Mitie.
- Measures that consider the reliability of employees (such as references, etc.).
- The inclusion of data protection provisions in employment contracts.
- Identification of disciplinary action measures for data breaches.
- Monitoring of staff for compliance with relevant security standards.
- Physical access controls to electronic and paper-based records.
- Adoption of a clear desk policy.
- Storing of paper-based data in lockable fire-proof cabinets.
- Restricting the use of portable electronic devices outside of the workplace.
- Limiting the use of employees' personal devices being used in the workplace.
- Adopting clear rules about passwords.
- Making regular backups of personal data and storing the media off-site; and
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the United Kingdom.

These controls have been selected based on identified risks to personal data and the potential for damage or distress to individuals whose data is processed.

The Controller must be able to demonstrate compliance with UK GDPR's other principles (accountability).

UK GDPR includes provisions that promote accountability and governance, complementing UK GDPR's transparency requirements. The accountability principle in Article 5(2) requires Mitie to demonstrate compliance with the principles. Mitie will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, and adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

Further information regarding Mitie's UK GDPR compliance programme can be requested from [privacy@mitie.com](mailto:privacy@mitie.com).

## Data Subject Rights

Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-making process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by the automated process.
- To sue for compensation if they suffer damage by any contravention of the UK GDPR.
- To take action to rectify and erase, including the right to be forgotten or destroy inaccurate data.
- To request the supervisory authority to assess whether any provision of the UK GDPR has been contravened.
- To have personal data provided to them in a structured, commonly used, and machine-readable format; and
- To have personal data transmitted to another controller.

## Data Subject Access Requests

Data subjects may exercise these rights under UK GDPR by making data processing requests commonly referred to as a Subject Access Request ("SAR"). These can be made verbally, in writing, or conveyed over email or other electronic methods. Any member of staff can receive a request to provide personal information. If a request for personal information is received, you must inform [privacy@mitie.com](mailto:privacy@mitie.com) without delay. The Mitie Data Privacy Team will assess and address all subject access requests it receives following its SAR Procedure, as these are designed to ensure that its response to the request is in line with UK GDPR guidelines.

Data subjects may also submit complaints to Mitie and the relevant Supervisory Authority (the Information Commissioners Office ("ICO") in the UK) concerning the processing of their personal data, handling a request from a data subject, and appeals from a data subject regarding how complaints have been handled. Further information regarding the submission of complaints is set out in Mitie's Privacy Notice at <https://www.mitie.com/footer-links/privacy/>.

## Consent

Mitie may rely on a data subject's consent as the valid basis for processing personal data in certain circumstances. Mitie understands 'consent' to mean that:

- It has been explicitly and freely given, and a specific, informed, and unambiguous indication of the data subject's wishes that, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to them; and
- The data subject has been fully informed of the intended processing and has signified their agreement while in a fit state of mind to do so and without pressure being exerted upon them.

Consent obtained under duress or based on misleading information will not be a valid basis for processing. A data subject can withdraw their consent at any time.

There must be some active communication between the parties to demonstrate active consent, and consent cannot be inferred from non-response to a communication. Mitie must be able to demonstrate that consent was obtained for the processing operation.

In most instances, consent to process personal and sensitive data is obtained routinely by Mitie using standard consent documents. For example, when a new client signs a contract or during induction for participants on programmes. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative lawful basis for processing exists.

## Security Data

All Mitie personnel are responsible for ensuring that any personal data that Mitie holds and for which they are responsible is kept securely and is not, under any conditions, disclosed to any third party unless that third party has been specifically authorised by Mitie to receive that information and has entered appropriate obligations of confidentiality.

All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security and must be kept in a controlled manner, for example:

- in a lockable room with controlled access.
- in a locked drawer or filing cabinet.
- if computerised, password protected; and/or
- stored on (removable) computer media which are appropriately encrypted.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Mitie personnel. All Mitie personnel must comply with Mitie's Information Security Acceptable Usage Procedure when accessing organisational information of any sort.

Paper-based records must not be left where unauthorised personnel can access them and may not be removed from business premises without explicit authorisation.

Personal data may only be deleted or disposed of in line with the Retention of Records Schedule. Paper-based records that have reached their retention date must be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be securely erased in line with the Information Security Management System requirements.

Processing personal data 'off-site' presents a potentially greater risk of loss, theft, or damage to personal data. All Mitie personnel must be specifically authorised to be processed off-site.

## Sharing and Disclosure of Personal Data

Mitie must ensure that personal data is not disclosed to unauthorised third parties, including family members, friends, government bodies, and in certain circumstances, the Police. All Mitie personnel should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether the disclosure of the information is relevant to and necessary for the conduct of Mitie's business.

The provision of data to a third party must be supported by appropriate paperwork. All disclosures outside those set out in Mitie's privacy notices must be authorised explicitly by the DPO.

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 and the transfer complies with any applicable cross-border transfer restrictions.

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 to provide 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.
- d) The transfer complies with any applicable cross-border transfer restrictions; and
- e) A fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

## Retention and Disposal of Personal Data

Mitie must not keep personal data in a form that permits the identification of data subjects for a longer period than is necessary relating to the purpose(s) for which the data was originally collected. Mitie may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Retention of Records Schedule and the criteria used to determine this period, including any statutory obligations to which Mitie is subject.

Personal data must be disposed of securely following the sixth principle of the UK GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

## Data Transfers

Data Transfers from the United Kingdom to EU and EEA countries.

The United Kingdom is recognised as an 'adequate' country, allowing for the continual flow of data transfers to and from EU and EEA countries; this is kept under review by the UK Government.

### Data Transfers to countries outside of the EU and EEA

The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations. These restrictions apply to all transfers, no matter the transfer size or how often you carry them out.

You may only transfer Personal Data outside the UK if one of the following conditions applies:

- The UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms.
- Appropriate safeguards are in place, such as binding corporate rules (BCR), standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO.
- The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- The transfer is necessary for one of the other reasons set out in the UK GDPR, including the performance of a contract between the Data Subject and us, 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.

## Record Keeping

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

We keep and maintain accurate corporate records reflecting our Processing, including records of Data Subjects Consents and procedures for obtaining Consents [following the Company's record-keeping guidelines].

These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. Data maps are created and include the detail set out above together with appropriate data flows.

## Privacy by Design and Data Protection Impact Assessments (DPIA)

We must implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) effectively to ensure compliance with data privacy principles.

We must assess what Privacy by Design measures can be implemented on all programmes, systems, or processes that Process Personal Data by considering the following:

- State of the art and the cost of implementation.
- The nature, scope, context, and purposes of Processing; and
- The risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

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

A DPIA is conducted when implementing major system or business change programs involving the Processing of Personal Data, including:

- The use of new technologies (programs, systems, or processes) or changing technologies (programs, systems, or processes).
- Automated Processing, including profiling and ADM.
- Large-scale processing of Special Categories of Personal Data or Criminal Convictions Data; and
- Large-scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- A description of the Processing, its purposes and the Controller's legitimate interests if appropriate.
- An assessment of the necessity and proportionality of the Processing relating to its purpose.
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

## Automated Processing (including profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similarly significant effect on an individual unless:

- a) a Data Subject has Explicitly Consented.
- b) the Processing is authorised by law; or
- c) the Processing is necessary for the performance of or entering a contract.

If certain types of Special Categories of Personal Data or Criminal Convictions Data are processed, then (b) or (c) will not be allowed. However, the Special Categories of Personal Data and Criminal Convictions Data can be Processed where necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision. A DPIA must be carried out before any Automated Processing (including profiling), or ADM activities are undertaken.

## 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 or are marketing similar products or services. They must be given 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 intelligibly to distinguish it 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.

## Information asset register/data inventory

Mitie has established a data inventory and data mapping process as part of its approach to identify and address risks and opportunities throughout its UK GDPR compliance project. Mitie's data inventory and data mapping:

- determines business processes that use personal data.
- identifies sources of personal data.
- identifies the volume of data subjects.
- describes relevant categories of personal data.
- describes processing activity.
- acts as an inventory of data categories of personal data processed.
- documents the purpose(s) for which each category of personal data is used.
- identifies recipients, and potential recipients, of the personal data.
- details key systems and repositories, data transfers and retention and disposal requirements.

## Additional provisions applicable to Mitie's subcontractors and suppliers

Mitie expects all subcontractors and suppliers to comply with their obligations under the UK GDPR and follow appropriate policies and procedures when processing personal data under or in connection with any services provided for or on behalf of Mitie.

All subcontractors and suppliers must, when processing personal data under or in connection with any services provided for or on behalf of Mitie:

- Process that personal data only on the documented instructions of Mitie unless required by applicable laws to otherwise process that personal data. A supplier or contractor relies on laws of a member of the European Union or European Union law as the basis for processing that personal data. It must notify Mitie of this before performing the processing unless those applicable laws prohibit such notification.
- Ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, appropriate to the harm that might result from

the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it).



- Ensure that all of its employees, consultants, contractors, agents, and representatives who have access to or process personal data are obliged to keep the personal data confidential.
- Ensure operational risks regarding data protection are reviewed at regular periodic intervals under a formal process.
- Notify Mitie (without delay) of any security breach affecting personal data processed on behalf of Mitie.

## Changes to this Data Privacy Policy

Mitie reserves the right to change this Data Privacy Policy at any time. To obtain the latest copy of this Privacy Policy, please contact [privacy@mitie.com](mailto:privacy@mitie.com).

We keep this Data Privacy Policy under regular review. This version was last updated on 21 January 2025.

## Approvals

Name	Signature	Issue Date
Chris Gould		05/04/2025
John Cruise		05/04/2025



Phil Bentley  
Chief Executive Officer  
Mitie Group plc

21<sup>st</sup> January 2025