



FARADAY GROUP DATA PROTECTION POLICY

We protect your property and your data!

1. Introduction

- a. The EU General Data Protection Regulation (GDPR) becomes effective 25 May 2018. This legislation strengthens the rights that UK individuals have over their data, and creates a uniform data protection law across the European Union. These provisions supplement the requirements of the Data Protection Act (The Act).
- b. Faraday manages the communal and amenity areas for a wide range of properties including blocks of flats, housing estates and mixed-use developments. Faraday has developed Data Protection policies and procedures to ensure that we and our clients comply with our Data Protection obligations.

2. Faraday's Services and Approach

- a. Faraday acts as an agent and advisor to its client. Although primary legal responsibility for the management of the property and the control of records is with our client, part of Faraday's service is to ensure our clients' compliance with the law, their leases, and codes of practice. The client is however, responsible for setting policy and monitoring the work of their agent.
- b. In order to perform the daily duties of running a property on behalf of the client, Faraday's service is to ensure our clients compliance with the law, their leases, and codes of practice. Data collected is also used to promote and advertise its services; maintain its own accounts and records; and support and manage its employees and contractors. In specific circumstances, Faraday gathers data for marketing its services but client and tenant information is not used for this purpose.
- c. This personal information is collected and dealt with appropriately whether it is collected on paper, stored in a computer database or recorded on other material. Faraday has put in place

safeguards to ensure this information is protected under the Data Protection Act 1998 and General Data Protection Regulation (GDPR).

- d. Our data protection policy outlines what Faraday does with the data that is collected, who it will be shared with and how it will be stored using the agency based relationship between Faraday and its clients

3. Faraday's Commitment

- a. Faraday complies with the GDPR regulations as a 'Data Processor' and where applicable as a 'Controller'. We will assist our clients wherever possible to meet their GDPR obligations.
- b. This policy sets out Faraday's approach to the protection of data for all leaseholders, tenants, clients and other service users with whom we interact including our employees. Faraday wishes to stress the high level of importance that it places upon complying with the requirements of GDPR.

4. Data Controller and Data Processor

- a. Faraday can be both a Data Processor and a Data Controller under the regulations. Faraday is a Data Processor when data is being processed on behalf of our instructing clients. This data includes anything to do with the management of our clients' buildings. We are the Data Controller under the Act when we create or collect personal data other than on behalf of our clients. This could be for example when Faraday is using the data for the purposes of its own communications. Interpretation of this difference could be difficult and in the event of any doubt Faraday's Data Controller should be contacted to provide clarification.
- b. Faraday is also responsible for notifying the Information Commissioners Office (ICO) of the data it holds or is likely to hold, and the general purposes that this data will be used for.
- c. The Faraday Data Protection Officer (DPO), is responsible for ensuring that we comply with all provisions within this policy and the Act.

5. Data Protection Principles

- a. Faraday regards the lawful and correct treatment of personal information as critical to maintaining the confidence of those with whom we deal.
- b. To this end, Faraday will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998. Specifically, the Principles require that personal information:
 - i. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
 - ii. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with those purposes,
 - iii. Shall be adequate, relevant and not excessive in relation to those purposes,
 - iv. Shall be accurate and, where necessary, kept up to date,
 - v. Shall not be kept for longer than is necessary,
 - vi. Shall be processed in accordance with the rights of data subjects under the Act,
 - vii. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information
 - viii. Shall not be transferred to a country or territory outside the European Economic Area.

6. Disclosure

- a. Faraday may share data, that it could reasonably be expected to with other agencies such as local authorities or the police.
- b. The leaseholders, clients, and other service users will be made aware how and with whom their data will be shared via Faraday documentation which may include this policy, management agreements, works orders, resident's handbooks and welcome letters. There are circumstances where the law requires Faraday to disclose data (including sensitive data) without the data subject's consent. These are:
 - i. Carrying out a legal duty or as authorised by the Secretary of State
 - ii. Protecting vital interests of an Individual/Service User or other person
 - iii. The Individual/Service User has already made the information public
 - iv. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
 - v. Monitoring for equal opportunities purposes – i.e. race, disability or religion
- c. Thirdly, Faraday may need to disclose data without the data subject's consent in order to allow Faraday to carry out our duties as a Data Processor and a property manager to clients. Examples of this include:
 - i. Providing Individual/Service User's personal information in an emergency, such as contact details to a tradesman who needs to carry out urgent repairs on behalf of a client
 - ii. Disclosing information to a debt collection company when a leaseholder is in service charge arrears
 - iii. Data can be shared with clients' (the landlord or a client company director) where necessary in order for them to monitor our work and maintain the Data Processing obligation of the client and agent relationship. The relationship is based on the premise that documents which relate to the affairs of a client, resident management company or Right to Manage company are not the property of the managing agent and should always be handed over to Faraday on request. Examples where data may be shared with a client are set out below:
 - iv. Legal proceedings brought against a client,
 - v. Leaseholder not paying service charges,
 - vi. Complaints from leaseholders regarding service levels,
 - vii. Concerns raised by a tenant, lessee or freeholder in respect of matters relating to the management of a building.
- d. Leaseholder account information is not divulged to other leaseholders, tenants or third parties. Members of a Residents Association or Committee are not considered Directors for this purpose therefore personal leaseholder information cannot be disclosed to them.
- e. There are circumstance where clients have a legal obligation to disclose data. This includes their obligations under S22 of the Landlord and Tenant Act 1985. (Receipts and invoices supporting service charge accounts).
- f. Neither Faraday nor our clients should disclose any information that could not reasonably be expected to be disclosed in the normal course of duties.

7. Data Collection

- a. Faraday will ensure that data is collected within the terms set out in this policy. This applies to data that is collected in person, or in the written word from the completion of a form.

- b. When collecting data, Faraday will ensure that the leaseholder, tenant, client and other service user clearly understands what the data will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing.
- c. Faraday collects the type of information set out below to carry out our property management services as well as maintain our own records. These records include addresses, financial and bank details for the following groups:
 - i. Clients
 - ii. Tenants
 - iii. Leaseholders
 - iv. Professional advisers and consultants
 - v. Complainants, enquirers
 - vi. Suppliers/contractors
 - vii. Landlords
- d. Faraday collects the following type of information to support and manage our employees and contractors.
 - i. Personal details
 - ii. Family details
 - iii. Lifestyle and social circumstances
 - iv. Employment and education details
 - v. Goods and services
 - vi. Financial details
 - vii. All information contained in references
 - viii. Faraday also processes sensitive classes of information that may include:
 - ix. Racial or ethnic origin
 - x. Religious or other beliefs
 - xi. Trade union membership
 - xii. Physical or mental health details

8. Faraday Staff Roles and Responsibilities

Ensuring compliance with our statutory duties under GDPR is everyone's responsibility. To provide the leadership and overarching policy direction Faraday will appoint:

Data Protection Officer (DPO) is responsible to the CEO for:

- i. Ensuring staff and authorised users are aware of this policy;
- ii. Monitoring compliance;
- iii. Conducting regular review of all policies, having regard to any changes in contractual obligations, organisational changes, and legislation;
- iv. Ensuring there is clear direction and visible management support for security initiatives.
- v. Chair bi-annual meetings with 'information owners' to review compliance and the Faraday Information Security risk register.

Information Owners

Faraday has designated information owners who are responsible for Data Protection compliance within their area.

Information Owners are responsible to the DPO for:

- i. Completing a Privacy Impact Assessment (PIA) on systems/data when required. A PIA shall be performed for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limit. Information owners must be satisfied that the controls will reduce any residual risk to an acceptable level.
- ii. Mitigate identified risks by ensuring information security is an integral part of information management, whether the information is held in electronic or hard-copy form. Faraday is committed to protecting the security of its information and information systems in order to ensure that:
 - a. The integrity of information is maintained, so that it is accurate, up to date and 'fit for purpose';
 - b. Information is always available to those who need it and there is no disruption to the Faraday business and operational activities;
 - c. Confidentiality is not breached, so that information is accessed only by those authorised to do so'
 - d. Faraday meets its legal and contractual requirements, including those applicable to personal data under GDPR;
 - e. The reputation of Faraday is safeguarded.
- iii. Faraday shall establish and maintain appropriate contacts with other organisations, regulatory bodies, and network/telecommunications operators in respect of its information security policy. Breaches of information security must be recorded and reported to the DPO, who will act and inform the relevant authorities.
- iv. Ensure 3rd Parties that are used to support Faraday in conducting its functions are compliant with GDPR regulations.

Contractor Accreditation Team

- i. Ensure that all suppliers on Faraday's Contractor Approved list will comply with Faraday's Data Protection Policy.

Faraday Managers are responsible for:

- i. Ensuring that data protection requirements are observed;
- ii. Providing clear messages to their staff regarding appropriate processing of the personal data that they handle;
- iii. Identifying and addressing training needs within the team and informing the DPO if the available training will not address their needs;
- iv. Consulting the DPO before processing personal data for a new purpose;
- v. Informing the DPO of any data subject requests or complaints;
- vii. Ensure staff are trained in Data Protection/Information security and have regular update training.

All employees are responsible for:

- i. Complying with the data protection principles, as supported by the Policy, guidance on the application of the Policy and associated policies and guidance;
- ii. Contacting their manager or the DPO for guidance if they are in any doubt about how they should deal with certain personal data;
- ii. Only processing personal data in the manner that is authorised for the purpose of carrying out their responsibilities or with management authorisation.

9. Data Storage

- a. Faraday is accountable to maintain control of confidentiality of its and its clients' records. Faraday must therefore take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. Faraday undertake as and when necessary Privacy Impact Assessments to access the risk to individual's rights when using new or enhanced systems. The following measures are taken:
 - i. Using lockable cupboards (restricted access to keys)
 - ii. Archived data is kept off site with a secure third-party storage company
 - iii. Password protection on personal information files
 - iv. Setting up computer systems to allow restricted access to certain areas
 - v. Copies of programs or data must not be taken or removed from Faraday's premises without the express permission of a line manager. However, when data is taken off site on laptops and mobiles, Faraday aims to protect the data on these medias by instructing staff to log-on to the network using their own account and keeping their passwords confidential.
 - vi. Back up of data on computers kept on separate hard drives on a secure server on site
 - vii. A clear desk and screen culture
- b. Information will be stored for only as long as it is needed as laid out in Faraday's Data Retention Policy, or as required by statute and will be disposed of appropriately.
- c. It is Faraday's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed to a third party.

10. Data Access and Accuracy

- a. Service users whose personal information are processed by Faraday have the right to know:
 - i. What information we hold and process on them
 - ii. How to gain access to this information
 - iii. How to keep it up to date
 - iv. What controls we have in place to ensure we comply with the Act.
- b. Service users also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information determined to be wrongfully collected.
- c. Service users have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to the Data Protection Officer (set out in (i) below).
- d. The following information will be required before access is granted:
 - i. Full name and contact details of the person making the request
 - ii. Their relationship with Faraday
 - iii. Any other relevant information - e.g. timescales involved
 - iv. Reference number held on record by Faraday - e.g. 'T' reference or company reference
 - i. photographic identification - e.g. Passport, drivers licence.
- e. Faraday may also require proof of identity before access is granted.
- f. Queries about handling personal information will be dealt with swiftly and politely.
- g. Faraday will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request.

- h. This policy was last updated in March 2018 and will be reviewed regularly and updated as necessary to reflect any additional regulatory requirements as well as best practice in data management, security and control.
- i. In case of any queries or questions in relation to this policy please contact Faraday's Data Protection Officer:

11. Compliance

Faraday takes data protection compliance very seriously; any breach of data protection legislation, local data protection procedures and/or the provisions of the Data Protection Policy may render staff liable to internal disciplinary proceedings. Staff should be aware that it is a criminal offence to breach certain provisions of the Act and GDPR regulations. Knowingly or recklessly obtaining or disclosing personal data may leave an individual employee liable to prosecution.

12. Policy Subdivision

This policy is the overarching foundation where all other subdivisions of Faraday information security policy shall conform to. While most policies are department specific, the small subset below will be applicable to all Faraday staff:

- Clear Desk and Screen Policy
- Document Retention Policy
- Privacy Policy

Glossary of Terms

The Act

- a. Data Protection Act. The UK legislation that provides a framework for responsible behaviour by those using personal information.
- b. Agent – Individual/company instructed to act on behalf of the client when it comes to day to day management of their development. In relation to this policy the agent is Faraday.
- c. Client – This term refers to any one of the following property owners or landlords; freeholder, resident management company (RMS), right to management company (RTM) or developer which instructs Faraday.
- d. Data Controller – The person who (either alone or with others) decides what personal information Faraday will hold and how it will be held or used.
- e. Data Protection Officer – The person responsible for ensuring that Faraday follows its data protection policy and complies with the Data Protection Act 1998.
- f. Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.
- g. GDPR. General Data Protection Regulations.
- h. Faraday is the agent working on behalf of the client
- i. Individual/Service User – The person whose personal information is being held or processed by Faraday for example: a client, an employee, a leaseholder, a tenant, a contractor, and a supplier etc.
- j. Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Act 1998.
- k. Notification – Notifying the Information Commissioner about the data processing activities of Faraday.

- l. Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees of Faraday.
- m. Processing – means collecting, amending, handling or storing personal information.
- n. Sensitive data – refers to data about:
 - i. Racial or ethnic origin
 - ii. Political affiliations
 - iii. Religion or similar beliefs
 - iv. Trade union membership
 - v. Physical or mental health

COMPANY DETAILS:

FARADAY PROPERTY MANAGEMENT LIMITED
Data Protection No: Z9628495