Quadrant

PROPERTY MANAGEMENT LTD

115 Hammersmith Road
London W14 0QH

Telephone 020-7386 8800
Facsimile 020-7386 0440
e-mail:
managers@quadman.co.uk
website:
www.quadrantpm.co.uk

Data Protection Policy

General Data Protection Regulations

Context and overview

Key details

- Policy prepared by: Quadrant Property Management Ltd
- Approved by board on: 21st May 2018
- Policy became operational on: 25th May 2018
- Next review date: May 2021

Introduction

Quadrant Property Management Ltd (The Company) needs to gather and use certain information about individuals.

These can include clients, lessees, tenants, employees, contractors and other people the Company has a relationship with or may need to contact.

This policy describes how this personal data is collected, handled and stored to meet the Company's data protection standards - and to comply with the law.

Why this policy exists

This data protection policy ensures the Company:

- Complies with data protection law and follows good practice
- Protects the rights of staff, clients, lessees, tenants and others
- Is open about how its stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Regulations describe how organisations - including Quadrant Property Management Ltd - must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The regulations are underpinned by the following principles. These say that personal data must:

1. Be processed fairly, lawfully and in a transparent manner.
2. Be obtained only for specific, lawful purposes and not be further processed in a manner that is incompatible with those purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Processed in a manner that ensures appropriate security of the personal data.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, risks and responsibilities
Policy Scope

This policy applies to:

- The office of the Company
- All staff and volunteers of the Company
- All contractors, suppliers and other people working on behalf of the Company

It applies to all personal data that the company holds relating to identifiable individuals, as set out on the Privacy Notices. This will include:

- Names of Individuals
- Postal addresses
- Email addresses
- Telephone numbers
- And any other information as set out on the Privacy Notices

Data protection risks

This policy helps to protect the Company from data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.

- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for the Company has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy, data protection principles and accountability requirements.

- The **board of directors** is ultimately responsible for ensuring that the Company meets its legal obligations.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**.
- **The Company will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the Company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from one of the Directors if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to one of the Directors.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them** (e.g. a printer).
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically,** it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services.**

- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to the Company unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.

- Personal data **should not be shared informally**.

- Sensitive data must be **suitably protected before being transferred electronically**.

- Personal data should **never be transferred outside of the European Economic Area**.

- Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data accuracy

The law requires the Company to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort the Company should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.

- Staff should **take every opportunity to ensure data is updated**.

- The Company will make it **easy for data subjects to update the information** it holds about them. For instance, via the service charge demands.

- Data should be **updated as inaccuracies are discovered**.

Rights for the data subject

The Regulations provide the data subject with the following rights:

- The right to be informed.
- The right of access (subject access request - see below).
- The right to rectification.

- The right to erasure.

- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

Subject access requests

All individuals who are the subject of personal data held by the Company are entitled to:

- Ask **what information** the company holds about them and why.

- Ask **how to gain access** to it.

- Be informed **how to keep it up to date**.

- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the Company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made in writing, addressed to Jeremy Neville (jeremy.neville@quadman.co.uk) who will arrange to provide the relevant data within 28 days.

The data controller will always verify the identity of anyone making a subject access request as set out in the privacy notices before handing over any information.

Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulations allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Company will disclose data. However, we will ensure the request is legitimate, seeking assistance as necessary.

Providing information

The Company aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used

- How to exercise their rights

To these ends, the Company has a privacy statement, setting out how data relating to individuals is used by the Company, a copy of which is on the website www.quadrantpm.co.uk.