

WHAT IS GDPR ?

GDPR stands for General Data Protection Regulation, which comes into force on 25 May 2018 and replaces the Data Protection Act.

It is a legal framework of guidelines that regulates the collection, storing and processing of personal information of individuals within the European Union (EU).

Everyone in Seths is a Data Controller; a person who determines the purpose for which, and the manner in which, any personal data has been or is to be processed.

A Data Processor refers to any person (other than someone in Seths) who processes the data on behalf of the data controller; e.g. Jupix, Contractors, Fix Flo, Tenant Shop, etc.

Lawful Basis for Processing Data

As a data controller, you must have a lawful basis for processing data. Lawful basis includes:

Consent - Personal data may be processed on the basis that the data subject has consented to such processing.

Contractual necessity - Personal data may be processed on the basis that such processing is necessary in order to enter into or perform a contract with the data subject. For example, supplying data to contractors or to EPC assessors.

Compliance with legal obligations - Personal data may be processed on the basis that the controller has a legal obligation to perform such processing. For example, anti money laundering regulations.

Vital interests - Personal data may be processed on the basis that it is necessary to protect the "vital interests" of the data subject. This essentially applies in "life-or-death" scenarios, for example if there is a fire or flood and you have to supply information to the Emergency Services.

Public interest - Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest. This point does not really apply to Estate Agency Work.

Legitimate interests - Personal data may be processed on the basis that the controller has a legitimate interest in processing those data, provided that such legitimate interest is not overridden by the rights or freedoms of the affected data subjects. This basis will be the most used one for Estate Agency work; e.g. canvassing.

Rights for Consumers

The GDPR includes the following rights for individuals:

- the right to be informed; an individual has the right to be provided with information on how their data is processed
- the right of access; an individual has the right to request deletion of their data
- the right to rectification; an individual has right to rectify or change if data is inaccurate or incomplete
- the right to be forgotten; an individual has the right to request deletion of their data
- the right to restrict processing; an individual can limit use of data
- the right to data portability; an individual has right to obtain and reuse their personal data

- the right to object; an individual has right to object to data being processed for marketing, profiling or either public interest or legitimate interest of the controller – if justified, the data controller must cease

Subject Access Requests

If we hold data on anyone, under GDPR, they will have the right to see all the data that we hold on them:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month

MAARK Estates GDPR POLICY

Consent

Prior to GDPR coming into force, all applicants were automatically put onto the mailing list for matching properties and almost all clients, new and old, were automatically signed up for newsletters, etc.

As per the new GDPR rules, we now have to ask for consent, both for matching properties and for adding them to our newsletter and general mailing list.

In Jupix, there are two sections when registering applicants that must be filled in when registering applicants:

When an applicant / vendor / landlord comes into the office or is on the phone, these questions must be asked. Start practicing and get used to the following script:

Property Match Details: “Would you like to be amongst the first to know when matching properties come onto the market ?”

Marketing Information: “Would you like to be added onto our mailing list and receive market updates and information about off market properties ?”

Please note that consent must be given; you can no longer automatically qualify them, and then they have an option to opt out.

Going forward these boxes must not be left as unknown.

Canvassing

Canvassing plays an important part of Estate Agency work, especially in sales.

Writing canvassing comes under the legitimate interest basis mentioned above. When you write letter addressed to “The Legal Owner” then GDPR rules do not apply as you are not using any personal data.

When conducting a land registry search, then you must put in the letter that their details have been obtained from the Land Registry Database.

When emailing / writing to vendors or landlords, we have already been out and met, then this will be covered by legitimate interest. However, they have the right to opt out of any further contact / marketing, and their request must be complied with.

Storing Information

It is crucial that all information is kept confidentially and out of sight. All computers, phones and tablets with customer data on it must be protected by a password.

Whilst serving customers at your desk, all other files on your desk must be kept closed and papers with sensitive information must be kept out of sight.

Also ensure that there are no notes attached to your computer screen / notebooks, with passwords for software, etc. Keep passwords in a safe place that cannot be easily lost.

Bank Details

Landlords usually supply bank details through the terms of business and emails. Terms of business must be filed away. When they send sensitive details in emails, print this out, file it, and delete the original email.

It would be far easier for someone to hack into our computer systems and get this information, rather than having to break into the office and go through each individual file. Information stored on third party software such as Jupix, Rentman, etc will be covered by their own GDPR policy.

Privacy Policy

By law every company that conducts business within the EU has to have a Privacy Policy which is easily accessible to anybody who wishes to see it.

The Privacy Policy is a legal document that explains how you handle customer client and employee information gathered in your operation.

For ease of access.

Customer's Right To Access Information

Information access is most often used by individuals who want to see a copy of the information an organisation holds about them.

However, access goes further than this and an individual is entitled to be:

- Told whether any personal data is being processed.
- Provided with a description of the personal data, the reason, for processing, and whether it will be given to any other organisations or people.
- Given a copy of the personal data.
- Given details of the source of the data (if applicable).

Right to be Forgotten

Every individual has the right to have their data deleted from your database at any time, providing that they are not currently benefiting from any services or you are contractually obligated to store their data (i.e. keep files for 6 years). This applies when:

- The personal data is no longer needed for the purpose that it was collected.
- The individual withdraws consent.
- The individual objects to the processing in cases where there is no overriding legitimate reason for continuing.
- The personal data was processed unlawfully.
- The personal data has to be erased to comply with a legal obligation.

Third Party Suppliers

As a Data Controller, Seths need to have written confirmation from all third part suppliers, e.g. Jupix, Tenant Shop, contractors, etc that they are GDPR Compliant. The best way to do this is have commercial contract with them, especially contractors where they can confirm not only that they are GDPR compliant, but have the necessary insurance, etc. GDPR also states that all third part suppliers are to be documented in the Privacy Policy.

Breaches

The Information Commissioners Office's definition of a personal data breach is:

"A breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."

The Information Commissioner's Office (ICO) must be informed of all data breaches in which there is a high risk to the individual's rights and freedoms.

If there is a data breach, even as simple as sending an email containing sensitive information to the wrong person, you must inform your manager immediately, who will then take the decision of whether it needs reporting further.