

Introduction

The General Data Protection Regulation (GDPR) represents a significant modernisation of data protection law, taking into account new developments in technology and the needs of the time of the Data Protection Act 1998.

Landlords are "data controllers" of personal data about prospective tenant/resident. The GDPR imposes new obligations on data controllers, including a requirement to register with the Information Commissioner (ICO) and new requirements relating to "data protection impact assessments" (DPIAs), storing, altering, sharing data with someone else and destroying data.

The GDPR brings with it a number of changes to data protection law including:

- Enhanced documentation and record keeping requirements;
- Enhanced privacy notice (data protection notices) requirements;
- Stricter rules on consent to processing;
- A new mandatory requirement to notify the ICO of a data breach;
- Enhanced rights for data subjects;
- New obligations for data processors;
- New rules requiring the appointment of a Data Protection Officer; and
- New, tougher penalties for non-compliance with the law.

In addition to these headline changes, the GDPR also changes the subject matter of all data protection law. The definition of "personal data" means: "any information relating to an identified or identifiable natural person ('data subject')". An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The core principles of the GDPR are set out in Article 5. Personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are accurate and, where necessary, kept up to date;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

not only simply as the GDPR, represents a significant modernisation of data protection law that takes into account significant new developments in technology and the needs of the time of the Data Protection Act 1998.

Landlords are "data controllers" of personal data about a tenant/resident or prospective tenant/resident. The GDPR imposes new obligations on data controllers, including a requirement to register with the Information Commissioner (ICO) and new requirements relating to "data protection impact assessments" (DPIAs), storing, altering, sharing data with someone else and destroying data.

The GDPR brings with it a number of changes to data protection law including:

- Enhanced documentation and record keeping requirements;
- Enhanced privacy notice (data protection notices) requirements;
- Stricter rules on consent to processing;
- A new mandatory requirement to notify the ICO of a data breach;
- Enhanced rights for data subjects in certain cases)

the appointment of Data Protection Officers; and new, tougher penalties for non-compliance with the law.

The GDPR also changes the definition of "personal data" – the key subject matter of all data protection law. The definition of "personal data" means: "any information relating to an identified or identifiable natural person ('data subject')". An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The core principles of the GDPR are set out in Article 5. Personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are accurate and, where necessary, kept up to date;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

or statistical purposes subject to appropriate technical and organisational measures required to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Under Article 5(2) of the GDPR, the controller must be able to demonstrate, compliance with the principle of accountability.

Data Protection Audit

An essential starting point in compliance, is a Data Audit. This involves identifying what data is held and on what lawful basis. It also records what data is shared with third parties. A completed Data Audit can be used to demonstrate compliance (see below).

Lawful Basis for Processing

In order for the collection and processing of personal data by a landlord must have a lawful basis under the GDPR. Four of these are relevant to landlords:

- You have the consent of the data subject for one or more specific purposes;
- The processing is necessary for the performance of a contract or to take steps to enter into a contract;
- The processing is necessary for compliance with a legal obligation; and
- The processing is necessary for the purposes of the legitimate interests of the data controller (the landlord) or of a third party, provided that the interests or fundamental rights and freedoms of the data subject do not override those of the data controller, particularly where the data subject is a child.

Different conditions apply if the data is sensitive personal data or, "special categories of personal data". The following conditions may be relevant to landlords:

- You have the explicit consent of the data subject, unless reliance on such consent is prohibited by law;
- The processing is necessary for reasons of substantial public interest, on the basis of legal obligations under employment law, social security or social protection law, or collective agreements;
- The processing is necessary for reasons of substantial public interest, in the interests of the data subject or another person where the data subject is unable, physically or legally, of giving consent;
- The processing concerns manifestly made public by the data subject; and
- The processing is necessary for the establishment, exercise, or defence of legal claims, or where the courts have jurisdiction.

of the appropriate technical and organisational measures required to safeguard the rights and freedoms of individuals;

the security of the personal data, against unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

responsible for, and be able to demonstrate, compliance with the principle of accountability.

and being able to demonstrate that compliance. This involves identifying what data is held, why it is held and on what lawful basis. The audit should also record what data is shared with third parties. A completed Data Audit can be used to demonstrate compliance (see below).

to be lawful under the GDPR, the controller must have a lawful basis under the GDPR. Four of these are relevant to landlords:

respect to one or more specific purposes; The processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract; The processing is necessary for compliance with a legal obligation; and The processing is necessary for the purposes of the legitimate interests pursued by the data controller (the landlord) or of a third party, provided that the interests or fundamental rights and freedoms of the data subject do not override those of the data controller, particularly where the data subject is a child.

on is sensitive personal data or, "special categories of personal data". The following conditions may be relevant to landlords:

unless reliance on such consent is prohibited by law; The processing is necessary for reasons of substantial public interest, on the basis of legal obligations under employment law, social security or social protection law, or collective agreements; The processing is necessary for reasons of substantial public interest, in the interests of the data subject or another person where the data subject is unable, physically or legally, of giving consent; The processing concerns manifestly made public by the data subject; and The processing is necessary for the establishment, exercise, or defence of legal claims, or where the courts have jurisdiction.

The standards of consent under the GDPR are even more so where the data concerned is sensitive personal data. The GDPR is to give data subjects more control over what happens to their data.

Under the GDPR, in order to be valid, consent must be:

- Be freely given;
- Specifically state the controller's name and the purposes for which the landlord requires the personal data;
- Be requested prominently, in a clear and understandable manner, in user-friendly, easy-to-understand language;
- Be obvious, requiring a positive action. Opt-out boxes should be avoided;
- Be expressly confirmed in writing.

Consent under the GDPR must be a clear affirmative action on the part of the data subject. The following mechanisms should comply with the following:

- Consent should be separate from any other terms and conditions. It should also generally not be a precondition to signing a contract.
- If you use opt-in boxes to obtain consent, these should not be pre-checked.
- The GDPR requires "granular" consent, meaning that separate consent for different purposes should be obtained.
- Clear records must be kept of consent.

It is also important to note that data subjects are free to withdraw that consent at any time. Landlords should provide easy means to exercise it. More importantly, the time limit for consent. How long it lasts will depend on the context in which it is given.

Having obtained consent, ensure you keep a record of it, including the identity of the data subject, what information they were provided with, and the date of consent (for example, your privacy notice).

It is also important to remember that consent is not the only criterion that can be satisfied. For example, a certain amount of consent may be necessary for the management of the tenancy between a landlord and a tenant.

Privacy Notice

Landlords must provide certain information to data subjects. This information will often be provided in your Privacy Notice. The information provided will vary depending upon whether you have obtained the data directly from the subject or obtained it from a third party:

Information	Obtained Directly	Obtained from Third Party
Identity and contact details of the data controller's Data Protection Officer	Yes	Yes

Purpose of collection and process for it.	Yes	Yes
(Where applicable) the legitimate i	Yes	Yes
The categories of personal data.	No	Yes
Details of any third party recipients	Yes	Yes
Details of any “third country” (non-safeguards in place.	Yes	Yes
How long the data will be retained determine how long).	Yes	Yes
The existence of data subjects’ rig	Yes	Yes
The data subject’s right to withdraw applicable).	Yes	Yes
The data subject’s right to complain authority (e.g. the ICO).	Yes	Yes
The source of the personal data, a publicly accessible sources.	No	Yes
Whether the provision of the perso or contractual requirement or oblig consequences of not supplying it.	Yes	No
The existence of any automated d profiling) with details of how the de significance, and the consequence	Yes	Yes

This information should be provided if the data is obtained directly from the data subject. If the data is obtained from a third party, the information must be provided to the data subject within one month (not more than one month); or, if the data is to be disclosed to a third party, before that disclosure takes place.

The Right of Access

Data subjects have the right to access their personal data held by you along with supplementary information. In response to a Subject Access Request (“SAR”) you must provide confirmation of the personal data you hold on the data subject, the same information you would provide in a privacy statement).

Under the Data Protection Act, it is usually £10 - however the GDPR request is “manifestly unfounded” and charged. Further copies of the same information are free of charge.

You should respond to SARs no later than one month. In the case of complex requests, this can be extended to three months.

The Right to Rectification

Personal data should be accurate and up to date. If a data subject requests the rectification of

personal data is obtained if it is being obtained from a third party, the information must be provided to the data subject within one month (not more than one month); or, if the data is to be disclosed to a third party, before that disclosure takes place.

Personal data held by you along with supplementary information. In response to a Subject Access Request (“SAR”) you must provide confirmation of the personal data you hold on the data subject, the same information you would provide in a privacy statement).

Under the Data Protection Act, it is usually £10 - however the GDPR request is “manifestly unfounded” and charged. Further copies of the same information are free of charge.

You should respond to SARs no later than one month. In the case of complex requests, this can be extended to three months.

Personal data should be accurate and up to date. If a data subject requests the rectification of

any personal data you hold about them. If the request is complex, this can take up to one month.

If the personal data in question has been shared with any third parties, the data subject should be informed of this.

The Right to Erasure

This is also known as the “right to be forgotten”. In broad terms, data subjects have the right to request the deletion or destruction of personal data unless there is a sound reason for retaining it.

The most obvious way of exercising this right is by asking you to stop your use of their personal data where there is no legitimate interest that justifies continuing to do so.

- When it is no longer necessary for the processing for which it was originally collected;
- The personal data has been collected unlawfully;
- The personal data has to be erased in order to comply with a legal obligation;

There are some circumstances where you are not required to erase personal data. The following are the most common circumstances that might be relevant:

- When exercising the right of freedom of expression and information;
- In order to comply with a legal obligation or the exercise of official authority;
- For the exercise or defence of legal claims;

If any personal data affected by a request has been disclosed to a third party, that third party must also be informed (unless it is disproportionate effort to do so).

The Right to Restrict Processing

If a data subject asserts this right, you must stop processing their personal data, but must not process it. In practice, this may require retaining the data about the data subject so as to ensure that the restriction is respected in the future.

The right to restrict processing applies in the following circumstances:

- If a data subject has informed you that the personal data you hold about them is inaccurate, processing of that data should be restricted until its accuracy is verified;
- If a data subject objects to you processing their personal data and you are considering whether your business’s legitimate interests override the data subject’s interests (this applies where you are processing that data for the performance of a public interest task or for the exercise of official authority);
- Where the processing is unlawful, the data subject requests restriction; or
- Where you no longer require the personal data for the purposes for which you established, exercise, or defend your legitimate interests.

If any personal data affected by a request has been disclosed to a third party, that third party must also be informed (unless it is disproportionate effort to do so).

within one month of their request. If the request is complex, this can take up to one month.

If the personal data in question has been shared with any third parties, the data subject should be informed of this.

This is also known as the “right to be forgotten”. In broad terms, data subjects have the right to request the deletion or destruction of personal data unless there is a sound reason for retaining it.

The most obvious way of exercising this right is by asking the data subject to withdraw their consent to your use of their personal data where there is no overriding legitimate interest that justifies continuing to do so.

- When it is no longer necessary for the processing for which it was originally collected;
- The personal data has been collected unlawfully;
- The personal data has to be erased in order to comply with a legal obligation;

There are some circumstances where you are not required to erase personal data. The following are the most common circumstances that might be relevant:

- When exercising the right of freedom of expression and information;
- In order to comply with a legal obligation or the exercise of official authority;
- For the exercise or defence of legal claims;

If any personal data affected by a request has been disclosed to a third party, that third party must also be informed (unless it is impossible or would require disproportionate effort to do so).

If a data subject asserts this right, you must stop processing their personal data, but must not process it. In practice, this may require retaining the data about the data subject so as to ensure that the restriction is respected in the future.

The right to restrict processing applies in the following circumstances:

- If a data subject has informed you that the personal data you hold about them is inaccurate, processing of that data should be restricted until its accuracy is verified;
- If a data subject objects to you processing their personal data and you are considering whether your business’s legitimate interests override the data subject’s interests (this applies where you are processing that data for the performance of a public interest task or for the exercise of official authority);
- Where the processing is unlawful, the data subject requests restriction; or
- Where you no longer require the personal data for the purposes for which you established, exercise, or defend your legitimate interests.

If any personal data affected by a request has been disclosed to a third party, that third party must also be informed (unless it is impossible or would require disproportionate effort to do so).

If any personal data affected by a request has been disclosed to a third party, that third party must also be informed (unless it is impossible or would require disproportionate effort to do so).

disproportionate effort to do so).

The Right to Data Portability

Data subjects, under the GDPR, have the right to obtain from a data controller in a commonly-used format a copy of their personal data and to have it transferred to a different data controller. This enables data subjects to move their personal data across different services. As with many other rights, the right to data portability applies only:

- To personal data provided by the data subject;
- Where the personal data is processed by automated means for the performance of a contract or for the purposes of the controller's legitimate interests;
- Where the processing of the data is based on the data subject's consent or on a contract.

Landlords must respond to requests for a copy of their personal data within one month. This can be extended by up to two months where the request is complex or if you receive a number of requests.

The Right to Object

Under the GDPR, data subjects have the right to object to the processing of their personal data and must be informed of the right to object. The right to object applies where the data processing is based on the controller's legitimate interests unless you can demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or where the processing is necessary for the exercise of legal claims.

Sharing of Personal Data

Landlords may need to share personal data with utility companies and contractors who will be data processors.

Landlords, as data controllers, should have a processing agreement with any third party data processors. However, if the data will themselves be data controllers, a processing agreement is required (e.g. if the landlord is a self-employed tradesperson) it need not be in writing.

- The subject matter and the purposes of the processing;
- The nature of the processing;
- The type of personal data to be processed;
- The rights and obligations of the data subject;

As a guide, contracts between controllers and processors should contain the following requirements:

- The processor acts only on the instructions of the controller (unless required by law to act without);
- The processor ensures that the data is processed securely;
- The processor takes suitable measures to protect the data;

copy of their personal data from a data controller and to have it transferred to a different data controller. This enables data subjects to move their personal data across different services. As with many other rights, the right to data portability applies only:

- To personal data provided by the data subject;
- Where the personal data is processed by automated means for the performance of a contract or for the purposes of the controller's legitimate interests;
- Where the processing of the data is based on the data subject's consent or on a contract.

Landlords must respond to requests for a copy of their personal data within one month. This can be extended by up to two months where the request is complex or if you receive a number of requests.

Under the GDPR, data subjects have the right to object to the processing of their personal data and must be informed of the right to object. The right to object applies where the data processing is based on the controller's legitimate interests unless you can demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or where the processing is necessary for the exercise of legal claims.

Landlords may need to share personal data with utility companies and contractors who will be data processors.

Landlords, as data controllers, should have a processing agreement with any third party data processors. However, if the data will themselves be data controllers, a processing agreement is required (e.g. if the landlord is a self-employed tradesperson) it need not be in writing.

- The subject matter and the purposes of the processing;
- The nature of the processing;
- The type of personal data to be processed;
- The rights and obligations of the data subject;

As a guide, contracts between controllers and processors should contain the following requirements:

- The processor acts only on the instructions of the controller (unless required by law to act without);
- The processor ensures that the data is processed securely;
- The processor takes suitable measures to protect the data;

- The processor may not ... consent, and then not witho
- The processor must assis otherwise allowing data su
- The processor must assist with respect to security, PL
- At the end of the contract, personal data; and
- The processor must comp carry out, provide the cont both parties are meeting th immediately if the process data protection laws (wheth

Data Retention and Delet

Personal data must be kept in a f longer than is necessary for the processed.

Data relating to a prospective te retained for one year. Information end of the tenancy (i.e. the six year be notified).

S A M P L E

or without the controller's written place with the sub-contractor; necessary, in handling SARs and DPR rights;

g its obligations under the GDPR of data breaches;

te and/or return (as requested) all

inspections that the controller may information required to ensure that e GDPR, and inform the controller g that infringes the GDPR or other

entification of data subjects for no e personal data is collected and

come an actual tenant should be d retained for seven years from the n extra year to allow for a claim to