General Data Protection Regulation Guidance Notes for Landlords

Introduction

The General Data Protection Regulation, commonly known simply as the GDPR, represents a significant modernisation of data protection law and one that takes into account significant new developments in technology and new uses of personal data that simply did not exist at the time of the Data Protection Act 1998.

Landlords are "data controllers" of any information they hold about a tenant/resident or prospective tenant/resident. The GDPR places various obligations on data controllers, including a requirement to register with the Information Commissioner (ICO) and requirements relating to “data processing” (collecting, using, storing, altering, sharing data with someone else and destroying/deleting data).

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

- Enhanced documentation and record-keeping requirements;
- Enhanced privacy notice (or “fair processing notice”) requirements;
- Stricter rules on consent to data processing;
- A new mandatory requirement to notify the ICO (and data subjects in certain cases) of a data breach;
- Enhanced rights for data subjects;
- New obligations for data processors;
- New rules requiring the appointment of Data Protection Officers; and
- New, tougher penalties for failure to comply with the law.

In addition to these headline changes, the all-important definition of “personal data” – the key subject matter of all data protection law – has expanded considerably. Under the GDPR, 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, in particular 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.

The core principles of the GDPR set out the central responsibilities for organisations. 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 to be 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 that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

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 insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order 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 unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Under Article 5(2) of the GDPR "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Data Protection Audit

An essential starting point in complying with the GDPR, and being able to demonstrate that compliance, is a Data Audit. This will help the landlord to identify what data is held, why it is held and on what lawful basis. "Lawful basis" is explained below. The audit should also record what data is shared with third parties and the reason for the data sharing. The completed Data Audit can be used to form the basis of a landlord's Privacy Notice (see below).

Lawful Basis for Processing

In order for the collection and processing of personal data to be lawful under the GDPR, the landlord must have a lawful basis for doing so. The GDPR specifies six conditions under which personal data processing will be deemed lawful. Four of these are relevant to landlords:

- You have the consent of the data subject with 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) unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, particularly where the data subject is a child.

Different conditions apply if the personal data in question is sensitive personal data or, "special categories of personal data" as it is known in the GDPR. 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 carrying out obligations under employment law, social security or social protection law, or under a collective agreement;
- The processing is necessary to protect the vital interests of the data subject or another person where the data subject is incapable, physically or legally, of giving consent;
- The processing concerns sensitive personal data 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 are acting in their judicial capacity.

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

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

- Be freely given;
- Specifically state the controller's name (i.e. the landlord), the purposes for which the landlord requires the personal data, and the type(s) of processing undertaken;
- Be requested prominently, separately from other terms and conditions, in a way that is user-friendly, easy-to-understand, and concise;
- Be obvious, requiring a positive action to opt-in (meaning that pre-checked boxes and opt-out boxes should be avoided); and
- Be expressly confirmed in words.

Consent under the GDPR must be unambiguous and involve some kind of clear affirmative action on the part of the data subject, moreover, consent mechanisms should comply with the following:

- Consent should be separate from the tenancy agreement. It should also generally not be a precondition to signing up for a service;
- If you use opt-in boxes to obtain consent, note that the GDPR expressly prohibits these from being pre-checked;
- The GDPR requires "granular consent" for distinct data processing operations (i.e. separate consent for different purposes); and
- Clear records must be kept in order to demonstrate consent.

It is also important to note that even once you have consent, data subjects are free to withdraw that consent at any time. You must inform data subjects of this right and provide easy means to exercise it. Moreover, there is no specific time limit for consent. How long it lasts will depend on the context in which it is provided.

Having obtained consent, ensure that you have in place a suitable system for recording that consent, including the identity of the data subject, how they consented, when, to what, and what information they were provided prior to giving that consent (for example, your privacy notice).

It is also important to remember the other bases for lawful processing as described above. If another criterion can be satisfied, it will not always be necessary to obtain consent. For example, a certain amount of personal data processing will be necessary for the management of the tenancy between a landlord and tenant.

Privacy Notice

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

Information	Obtained Directly	Obtained from Third Party

Identity and contact details of the data controller and the data controller's Data Protection Officer (if any).	Yes	Yes
Purpose of collection and processing and the lawful basis for it.	Yes	Yes
(Where applicable) the legitimate interests relied upon.	Yes	Yes
The categories of personal data.	No	Yes
Details of any third party recipients of the personal data.	Yes	Yes
Details of any "third country" (non-EU or EEA) transfers and safeguards in place.	Yes	Yes
How long the data will be retained (or the criteria to determine how long).	Yes	Yes
The existence of data subjects' rights under the GDPR.	Yes	Yes
The data subject's right to withdraw consent (where applicable).	Yes	Yes
The data subject's right to complain to a supervisory authority (e.g. the ICO).	Yes	Yes
The source of the personal data, and whether it came from publicly accessible sources.	No	Yes
Whether the provision of the personal data is part of a legal or contractual requirement or obligation and the potential consequences of not supplying it.	Yes	No
The existence of any automated decision-making (including profiling) with details of how the decisions are made, their significance, and the consequences.	Yes	Yes

This information should be provided at the time the personal data is obtained if it is being obtained directly from the data subject. If it is obtained from a third party, the information must be provided to the data subject within a reasonable time (not more than one month); when communicating with the data subject (if the data is being used to communicate with them); or, if the data is to be disclosed by you to another 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 what is known as a Subject Access Request ("SAR") you must provide confirmation that personal data is being processed; access to the personal data you hold on the data subject; and other supplementary information (in broad terms, the same information you would be expected to provide in a privacy statement).

Under the Data Protection Act, it was permissible to charge a fee for complying with SARs - usually £10 - however the GDPR requires SAR responses to be free of charge unless the request is "manifestly unfounded or excessive" in which case a "reasonable fee" can be charged. Further copies of the same information can also be charged for.

You should respond to SARs no later than one month after receipt. In the case of complex and numerous requests, this can be extended by up to two months.

The Right to Rectification

Personal data should be accurate and complete. If a data subject requests the rectification of any personal data you hold about them, this must be done within one month of their request. If the request is complex, this can be extended by up to two months.

If the personal data in question has been disclosed to 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". It is not an unqualified right, but in broad terms, data subjects have the right to request the deletion or destruction of personal data unless there is a sound reason for its continued processing.

The most obvious way of exercising this right is for a data subject to withdraw their consent to your use of their personal data or object to you using it (and there is no overriding legitimate interest that justifies continuing). Other circumstances are:

- When it is no longer necessary to hold the personal data with respect to the purpose for which it was originally collected and processed;
- The personal data has been unlawfully processed; and
- The personal data has to be erased to comply with a legal obligation;

There are some circumstances in which you may refuse to erase personal data. The circumstances that might be relevant to landlords are:

- When exercising the human right to freedom of expression and information;
- In order to comply with a legal obligation for the performance of a public interest task or the exercise of official authority; and
- For the exercise or defence of legal claims.

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

The Right to Restrict Processing

If a data subject asserts this right, you may hold their personal data, but must not process it. In practice, this may require retaining sufficient information about the data subject so as to ensure that the restriction is respected, but no more.

The right to restrict processing applies in the following circumstances:

- If a data subject has informed you that 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 your processing of personal data and you are considering whether your business's legitimate grounds for processing that data override the data subject's interests (this applies only where the processing is necessary for the performance of a public interest task or based on legitimate interests);
- Where the processing is unlawful but rather than erasure, the data subject requests restriction; or
- Where you no longer require the personal data, but the data subject requires it to establish, exercise, or defend a legal claim.

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

The Right to Data Portability

Data subjects, under the GDPR, have the right to obtain a copy of their personal data from a data controller in a commonly-used format and to have it transferred to a different data controller. This enables data subjects to easily re-use their personal data across different services. As with many other rights, however, this one is not unqualified. The right to data portability applies only:

- To personal data provided directly by the data subject;
- Where the personal data is being processed either with the data subject's consent or for the performance of a contract; and
- Where the processing of the personal data is carried out by automated means.

Landlords must respond to requests for data portability 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 certain uses of their personal data and must be informed of the right clearly, explicitly, and separately from other information. If the data processing is based on the landlord's legitimate interests data processing must stop unless you can demonstrate compelling legitimate grounds to continue which override the interests, rights, and freedoms of the data subject. Alternatively you may continue if the processing is necessary for the establishment, exercise, or defence of legal claims.

Sharing of Personal Data

Landlords may need to share personal data with a range of third parties, such as solicitors, utility companies and contractors who provide services to a property. These third parties will be data processors.

Landlords, as data controllers, should have a written data processing agreement with any third party data processors. However, many of the third parties with whom landlords share data will themselves be data controllers, so an agreement may not be appropriate. If a data processing agreement is required (it may, e.g. be required where the data processor is a self-employed tradesperson) it needs to cover the following:

- The subject matter and the duration of the processing;
- The nature of the processing and its purpose;
- The type of personal data to be processed and the categories of data subject; and
- The rights and obligations of the data controller.

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

- The processor acts only on the written instructions of the controller (unless required by law to act without);
- The processor ensures that people processing the personal data are subject to duties

of confidentiality;

- The processor takes suitable measures to ensure that the data is processed securely;
- The processor may not engage a sub-contractor without the controller's written consent, and then not without a written contract in place with the sub-contractor;
- The processor must assist the controller, where necessary, in handling SARs and otherwise allowing data subjects to exercise their GDPR rights;
- The processor must assist the controller in meeting its obligations under the GDPR with respect to security, PIAs, and the notification of data breaches;
- At the end of the contract, the processor must delete and/or return (as requested) all personal data; and
- The processor must comply with all audits and inspections that the controller may carry out, provide the controller with any and all information required to ensure that both parties are meeting their obligations under the GDPR, and inform the controller immediately if the processor is asked to do anything that infringes the GDPR or other data protection laws (whether EU or national).

Data Retention and Deletion

Personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is collected and processed.

Data relating to a prospective tenant who does not become an actual tenant should be retained for one year. Information relation to tenants should retained for seven years from the end of the tenancy (i.e. the six year limitation period plus an extra year to allow for a claim to be notified).