Transparency and Trust: A guide to data protection and privacy for landlords and tenants

Jane Burns
Anthony Collins solicitors

Marianne Hood OBE
HouseMark associate

January 2017
We are living in a new digital age and it is continually evolving. In the last decade or so we have witnessed dramatic technological development. Individuals can now access the personal data of others and can share their own personal information in a way which would have been unimaginable until relatively recently.

These advances in technology have also allowed both public and privately owned organisations to collect and share citizens’ personal data on an unprecedented scale, both for their own legitimate business purposes and also to make our daily lives run more smoothly.

In the social housing sector, many organisations are seeking to realise the value of the data they hold, particularly that relating to their customers, and are therefore investing more in analysing it.

Many see the benefit of collecting more customer data to improve the services they currently offer and plan future provision. Housing organisations also need to use customer data to manage risks around welfare reform and respond to government obligations in terms of immigration checks.

Going forward, the availability of ‘near real time’ data from mobile workers’ tablets and the ‘Internet of Things’ devices such as sensor-based monitoring of gas or fire safety or property condition, opens up new opportunities for data analysis.

However, the use of individuals’ personal data carries with it great responsibility to ensure such use is carried out in a manner which protects their privacy rights. Housing providers need to be very clear about their obligations under the UK’s Data Protection Act 1998.

In addition, the new General Data Protection Regulation, which will come into force throughout the EU in May 2018, will significantly raise the bar in terms of the standards to which the organisations in the EU countries will be subject when sharing individuals’ personal data. Notwithstanding the EU referendum result, if the UK wishes to continue to do business in Europe, it is likely that privacy standards will need to be at least commensurate with those in the EU countries. Housing organisations, should therefore ensure that, as a minimum, their processing of personal data is at least in line with current UK Law.

This guide sets out current regulatory requirements in respect of the use of personal data gathered from tenants and other customers and discusses ethical as well as legal considerations.

Whilst organisations in other sectors are increasingly focussed on the issue of data privacy, not least due to the commercial advantage to be gained by establishing greater customer trust than competitors, housing providers are not in same competitive position.
The issue of ethics is equally important to our sector. In practice, housing organisations that adopt an ethical approach of being transparent, open, and honest, and who seek customer consent for the use of personal data where it is required, are unlikely to fail many (although not all) of the requirements of the Data Protection Act.

The issue therefore is not simply one of compliance but is about having a clear strategy for the use of tenant personal data and executing and communicating it effectively. Failure to meet the requirements of the Data Protection Act can lead to heavy fines from the Information Commissioner’s Office (ICO), loss of business reputation and trust. Failure to tackle Data Protection in an ethical manner could lead to a complete loss of customer trust and reduced willingness to provide personal data to the landlord.

This guide, jointly published by HouseMark (sector data experts and thought leaders) and Anthony Collins solicitors (leading experts on data issues) and sponsored by Amicus Horizon (a major housing association that prides itself on its use of customer data and its commitment to data protection), seeks to explain the legal and ethical issues for housing organisations and their customers.

It is also published to assist tenants to understand how sharing their personal data can enable their landlord to help them and, conversely, know their legal rights of redress should their landlord fail to meet its legal obligations. By upholding key data protection principles and safeguards, social landlords can realise the benefits of access to customer data whilst protecting and promoting the interests of their tenants.

We have sought to make the guide as practical and up-to-date as possible. We hope you find it useful.

**Arturo Dell,**
Director of Product Development, HouseMark

**Helen Tucker,**
Partner, Anthony Collins

**Jane Porter,**
Executive Director of Operations, Amicus Horizon

**Definitions**

**Big Data:** "high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making" (Definition from the Information Commissioner’s Office).

**Data Protection Act 1988 (DPA):** the Data Protection Act (DPA) gives individuals the right to know what information is held about them, and provides a framework to ensure that personal information is handled in a way which protects their privacy.

**Data controller:** an individual or an organisation who decides the manner and purpose of how personal data is processed.

**Data processor:** an individual or an organisation who processes personal data on behalf of, and under instructions from, the data controller.

**Data Sharing:** this term covers a wide range of situations in which personal data may be transferred from one organisation to another

**Data subject:** the living individual whose personal data is processed by either the data controller or data processor or both. In the case of social landlords, possible data subjects will include:

- tenants
- relatives of tenants
- the landlord’s own staff
- individuals employed by suppliers or third parties who provide outsourced services e.g. payroll or secure waste disposal, for example
- consultants
- individuals who fall in to the above category but who have 'moved on' (e.g. ex-tenants or staff) who are still living but whose personal data is still held by the landlord

The above will all possess the rights available to data subjects under the DPA such as the right to obtain a copy of their own personal data held by the landlord.

**EEA:** the European Economic Area and includes all of the territories of the European Union (EU) plus Norway, Liechtenstein and Iceland.

**Personal Data:** this is information about a living individual who can be identified from that information or from this information and other information which the data controller already possesses. It can include expressions of opinion about a data subject.

**Privacy Notice:** this should contain the ‘Fair Processing’ information required to be given to data subjects i.e.

- the identity of the data controller
- the purpose of purposes for which the data are intended to be processed
- any other information that is necessary to enable the processing to be fair to the data subject. This could include the identity of anyone else with whom the data subject’s information is likely to be shared and how long the personal data will be held.
Definitions

Processing: anything that can be done to personal data, although the most well-known processing operations are: retain/store, disclose (share), edit and delete/erase/destroy.

The Information Commissioner’s Office (ICO): the independent body responsible for regulating the DPA. Its remit is to promote good practice, provide information to individuals and organisations and to take enforcement action where there has been a breach of the DPA.

Sensitive Personal Data: this is personal data relating to:

- racial or ethnic origin
- political opinions
- religious belief or similar
- trade union membership
- physical/mental health or condition
- sexual life
- commission or allegation of an offence
- proceedings for any offence, disposal of proceedings or sentence

In this guide, references to one gender are given for illustrative purposes only and are meant to refer to both genders equally.

Acknowledgements

The authors would like to acknowledge Ross Fraser (formerly CEO of HouseMark), Jonathan Cox, Helen Tucker, Gemma Bell, Will Allen and Danielle Chetwynd for their help and support whilst writing this Guide.

This guide was edited by Ross Fraser.

Contents

1. INTRODUCTION 8
   1.1 About this Guide 8
   1.2 Data protection and privacy: law and regulations 11

2. LANDLORD OBLIGATIONS UNDER THE DATA PROTECTION ACT 1998 13
   2.1 Data controller or processor: the legal distinction 14
   2.2 The landlord’s duties as data controller 17
   2.3 Responsibilities of the data controller relating to the data processor 18
   2.4 Requirement to be fair and transparent 19
   2.5 Processing personal data: landlord requirements 21
   2.6 Checklist: questions for landlords 26

3. TENANTS’ RIGHTS UNDER THE DATA PROTECTION ACT 1998 27
   3.1 The basis of tenants’ legal rights 27
   3.2 Specific rights for tenants under the DPA 27
   3.3 The right to say ‘no’ and to say ‘stop’ 31
   3.4 The right to complain 31
   3.5 Putting rights into practice 32
   3.6 Checklist: questions for tenants 33

4. DATA SHARING 34
   4.1 Data sharing with third parties: landlord obligations 34
   4.2 Data sharing with contractors: examples 36
   4.3 Requests for disclosure by third parties 39
   4.4 Mandatory legal disclosures 40

5. THE DATA PROTECTION ACT 1988: ENFORCEMENT ACTION 47
   5.1 Reporting a breach of the DPA to the ICO 47
   5.2 Enforcement by the ICO 48
   5.3 Checklist: Avoiding intervention by the ICO 49

6. GETTING IT RIGHT: DATA PROTECTION AND PRIVACY 50
   6.1 Transparency and the business case for ethical behaviour 50
   6.2 Involving tenants 51
   6.3 Accountability and tenant consent 52
   6.4 Transparency and fairness 53
   6.5 Privacy by Design 54
   6.6 Privacy Impact Assessments (PIAs) 55
   6.7 Using anonymised data 56
   6.8 Landlord Checklist: getting it right 63

7. DATA SECURITY 64
   7.1 Key security issues for social landlords 66
   7.2 Staff training 67
   7.3 Appointment of Data Processors 68
   7.4 Cloud processing and international transfers of personal data 69
   7.5 Checklist: security 69

APPENDIX 70
Data which landlords can legitimately request from tenants 70
1.1 ABOUT THIS GUIDE

Development of new computing and data processing technology has led to an increase in the volume of data being collected by organisations. We are now living in the era of **Big Data**. The Information Commissioner’s Office (ICO) has defined this as “high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making”.

Put more simply, big data is about being able to get hold of, and process, enormous amounts of very varied data very quickly. New tools for analysing data are becoming available as financial pressures on social landlords and their tenants make it even more important to have better understanding of customer needs and personal circumstances.

Much more can now be learnt and understood about people than was previously possible, but it also means there is much greater potential for abuse.

The significant increase in the collection and sharing of personal data brings risks to individuals of the disclosure of personal details to which they have not agreed, of which they may be unaware, and where such disclosure might cause concern and distress.

There is a strong case for tenants to agree to the proper use of their personal data held by their landlord – but one that the landlord needs to make in a transparent manner.

The challenge for social housing landlords is that this is a complex area of legislation and regulation. Failure to comply carries severe legal and financial penalties – and significant business risks. However, the legal and regulatory framework also brings opportunities for tenant empowerment through providing rights to information, rights to ‘say no’, and rights to redress.

Opportunities are available for landlords and tenants to work in partnership to put in place a strategy to ensure effective compliance and to avoid these penalties and business risks.

By processing tenants’ data, landlords may be able to offer their tenants:

- **Support in paying rent**
  - Access to bank accounts and credit
  - Access to benefits information

- **Access to cheaper services and utilities**
  - Cheaper power
  - Eligibility for grants, adaptations

- **Better living environment**
  - Tackling tenancy fraud, crime and illegal subletting on estates
  - Safer homes
  - Social networking

By being open, honest, and transparent and working in collaboration with their tenants and other customers, social landlords can embed an approach to data protection and privacy that will not only enable them to meet statutory and regulatory requirements but also to gain tenant support in using their data to improve services and business efficiency.

This guide summarises the legal requirements relating to Data Privacy and Data Protection with information about tenants’ rights, landlords’ responsibilities, and the importance of compliance. It also provides suggestions, examples and checklists as ‘tools’ to help both landlords and tenants.

The target audience for this guide is:

- **Social Landlords**
- **Tenants Groups**
- **Active Tenants** who act as representatives on panels, forums or any other body set up to enable tenants and their landlord to work together.
The aims of this guide are to:

• provide a resource for landlords and active tenants
• explain in simple terms the law and guidance on data protection and data privacy
• help landlords achieve legal and regulatory compliance
• examine the ethical issues surrounding data privacy
• empower tenants by providing clear information about their rights in relation to protection of their privacy, including rights to information and rights to redress

This is a joint publication with Anthony Collins Solicitors LLP, a leading law firm which specialises in providing advice to housing associations, charities and public sector organisations. It is not a definitive legal guide to Data Privacy and the Data Protection Act 1998 but instead provides a summary of the key requirements as the law stands at September 2016. It contains signposts to where further information can be found and provides recommendations where appropriate.

However, the Data Protection Act and, in particular, its interaction with overlapping and Housing sector specific legislation, is a complex one and landlords should seek legal advice where further clarification is required.

Landlords should be aware that on 25th May 2018 a new General Data Protection Regulation (GDPR) will come into force throughout all of the countries of the European Union (EU). Although the result of the UK Referendum means that the UK will now be leaving the EU, the future of the UK data protection regime is far from clear.

If, as is very likely, the UK has not left the EU by the above date, the GDPR will come into force in the UK.

However, the outgoing UK Minister for Data Protection, has recently stated that "One problem is that we do not know how closely the UK will be involved with the EU system in future. On one hand if the UK remains within the single market EU rules on data might continue to apply fully in the UK. On other scenarios we will need to replace all EU rules with national ones. Currently it seems unlikely we will know the answer to these questions before the withdrawal negotiations get under way."

1. Baroness Lucy Neville-Rolfe speaking at the 2016 annual Privacy Laws and Business Data Protection Conference in Cambridge. On 15th July 2016 The Rt Hon Matt Hancock MP was appointed as the new Minister of State for Digital and Culture, which includes responsibility for Data Protection.

2. Statement issued by former Information Commissioner, Christopher Graham at the ICO’s annual report launch on 28 June 2016.

3. ICO’s dedicated data protection reform website can be found at: for-organisations/data-protection-reform/

4. The terms, "established", "in the context of", and "equipment" have been interpreted very widely in case law and this means, in practice, that non-UK based organisations can be caught within the UK’s DPA. There have been a number of cases in which this has produced somewhat surprising and controversial results.

1.2: DATA PROTECTION AND PRIVACY: LAW AND REGULATIONS

The Data Protection Act 1998 (DPA)

The DPA came into force throughout the UK in 2000. Whilst this is UK legislation its legal application reaches much further and can apply to data controllers established outside of the UK but who process ‘in the context of a UK establishment’ or who use equipment in the UK for processing personal data.

Under the DPA the personal data of a living individual can only be used by an organisation for precisely specified objectives and in accordance with the rights of the individual to whom the information relates.

This means organisations should:

• keep personal information private, securely stored and deleted when no longer needed in relation to the purpose(s) for which it was collected
• be transparent and fair to the individuals whose personal information is held
• collect only the information necessary for a particular purpose
• make sure that only those who need the information and are legally entitled to do so, have access to it
Data Privacy

In the UK, the law does not recognise any general civil wrong known as ‘invasion of privacy’ and there is no specific legislation in the UK which provides an individual with an all-encompassing right to privacy.

However, it is not true to say that no law of privacy exists. Whilst there may be no single source of privacy law upon which an individual may rely, the law has for a long time protected different forms of privacy*, such as that afforded to information provided in confidence and/or which an individual regards as private.

Moreover, with the introduction of the Human Rights Act 1998 (HRA) and The Data Protection Act 1998, case law has developed to the point where there are three possible grounds for taking proceedings through the civil courts where an individual’s personal, private or confidential information has been mishandled:

1. Breach of the Common Law Duty of Confidence
2. Misuse of Private Information

Where the information relates to a living individual as defined in the Data Protection Act 1998, unlawful use of that individual’s personal information would represent a breach of the Data Protection Act 1998. This carries with it the potential for individuals or corporate entities to be prosecuted in the criminal courts in certain circumstances.

DATA CONTROLLER: this is an individual or an organisation who decides the manner and purpose of how personal data is processed.

DATA PROCESSOR: this is an individual or an organisation that processes personal data on behalf of, and under instructions from, the data controller.

There are three key concepts which it is helpful to understand before exploring the legal details of landlord obligations in this chapter, and tenants’ rights in Chapter 3:

• the information which is regulated under the DPA relates to personal data (of a living individual)
• data protection obligations primarily fall upon the data controller (the person or organisation who decides the manner and purpose of how personal data is processed)
• in most cases a landlord will act as a data controller when collecting and using tenants’ personal data. However, in some cases, a landlord may also act as a data processor, or it may share personal data with an external contractor which may be acting as a data processor for the landlord.

There are very important implications for the landlord in terms of compliance and legal liability, dependent upon whether it acts as a data controller or data processor and in relation to any data processors it appoints to act on its behalf. This is explored later in this chapter.

The starting point is that wherever personal data is processed, the Data Protection Act 1998 will apply.

DATA PROCESSING

The term ‘processing’ is defined very widely and covers anything that could be done with personal data. This includes, but is not limited to:

• collecting
• editing
• retaining/storing
• disclosing (or sharing)
• deleting/erasing/destroying
• viewing (e.g. looking at someone’s personal data, which could include their image, on screen or on paper)
• archiving
• listening to (audio recording of a living person speaking)

5. Including the law relating to trespass, defamation and libel.

6. Although under the new GDPR, liability is imposed on data processors in certain circumstances, for the first time.
2.1 DATA CONTROLLER OR PROCESSOR: THE LEGAL DISTINCTION

The ICO has also said that a data controller will decide:

• to collect the personal data in the first place and the legal basis for doing so
• which items of personal data to collect, i.e. the content of the data
• the purpose or purposes for which the personal data are to be used
• which individuals to collect data about
• whether to disclose the data, and if so, to whom
• whether subject access and other individuals’ rights apply i.e. the application of exemptions, and
• how long to retain the data or whether to make non-routine amendments to the data

Whereas a data processor may decide:

• what IT systems or other methods to use to collect personal data
• how to store the personal data
• the detail of the security surrounding the personal data
• the means used to transfer the personal data from one organisation to another
• the means used to retrieve personal data about certain individuals
• the method for ensuring a retention schedule is adhered to, and
• the means used to delete or dispose of the data

Whether or not a service provider is likely to be acting as a data processor for a landlord in any particular situation will be a question of fact and will depend upon the level of control exercised over key decisions by the service provider when processing the landlord’s personal data.

This is not always easy to determine. The ICO has therefore produced a useful guidance document on this point; ‘Data controllers and data processors: what the difference is and what the governance implications are’ (2014) which can be found on its website.

Processing personal data

‘Personal Data’ has a specific legal definition under the Data Protection Act. In general terms, it means information about a living individual in either:

• electronic format
  e.g. email, computer/ portable hard drive file, CCTV, text, fax, digital camera, mobile telephone or landline voicemail message; or
• an organised paper filing system
  e.g. a filing cabinet containing files organised in alphabetical order, so that it would be fairly easy to locate information relating to a specific individual

PERSONAL DATA

Personal data includes information that is about someone or relates to someone - known under the DPA as a data subject.

For example, an organisation may hold the name of an individual on its computer system, together with their address, date of birth, next of kin, disabilities and details of support services provided. Each of these items of information will be the personal data of the individual to whom it relates. It also includes the opinions of an individual or opinions of them by others.

See Appendix for examples of the kinds of personal data which a landlord may hold on a tenant.

Tenants often provide their landlords with quite extensive personal information, much of which may also be sensitive in some form or another. Information might be financially sensitive because, for example, it comprises tenants’ bank statements or information relating to finances for the purposes of the calculation of benefit payments. It might be personally sensitive relating to health or disabilities, which the landlord may have collected in order to ensure the tenant is provided with the most suitable accommodation in relation to his or her needs.
Sensitive Personal Data, as defined by the DPA, need to be treated even more carefully because the consequences for the individual in terms of damage or distress caused, if such information is lost or disclosed in error, can be much more serious.

The tenant will have provided this information to the landlord in the expectation that the landlord will retain it securely and disclose it only to those who really need to be aware of the data. It would be reasonable for the tenant to expect that this information will not be disclosed to anyone without his or her consent unless it falls within the purposes for which the landlord needs to maintain the conditions of the tenancy agreement or some other legal ground for the sharing. To make a disclosure outside of these terms would not only be a breach of the DPA but would represent a breach of trust and confidence and would open up the landlord to the possibility of an action through the civil courts by the tenant for breach of the DPA, breach of the common law duty of confidentiality or misuse of private information.

2.2: THE LANDLORD’S DUTIES AS DATA CONTROLLER

When processing the personal data relating to its own tenants, contractors, and staff, for its own legitimate business purposes, a landlord will be acting as a data controller and obliged to comply with the provisions of the DPA.

As a data controller, the DPA provides landlords with a statutory duty to:

(i) register with the UK regulator (the Information Commissioner’s Office or ICO called ‘notification’) to inform the ICO of their processing and pay the requisite fee. It is important to keep this notification up to date and advise the ICO of any changes as failure to do so is a criminal offence.

(ii) comply with the eight data protection principles

The Eight Data Protection Principles
Personal data must be:

1. Processed fairly and lawfully and with a legal ground for the processing
2. Processed for specified purposes only
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Not kept longer than is necessary
6. Processed in line with data subjects’ rights
7. Kept securely
8. Not be transferred to other countries outside the EEA without an adequate level of protection for the rights of data subjects

© HouseMark and Anthony Collins 2016-17

Transparency and Trust: A guide for landlords and tenants to data protection and privacy
2.3 RESPONSIBILITIES OF THE DATA CONTROLLER RELATING TO THE DATA PROCESSOR

Data controllers are required to comply with the DPA but there is no legal requirement for data processors to be DPA compliant in relation to any processing which they undertake for a data controller.13 The act of becoming a data processor brings the data processor ‘within the fold’ of the data controller’s organisation and the data controller will be liable for all breaches of its data processor when that data processor is processing the data controller’s personal data.

Under Principle 7 of the DPA, a data controller must have a contract in writing with the data processor. This data processor could be an organisation or an individual. Thus, wherever a landlord asks a third party to carry out a service on its behalf, the landlord will need to consider the capacity in which that service provider will process any of the landlord’s personal data. If the expectation is that the service provider will act on the landlord’s instructions, when processing the landlord’s personal data, it will be important to ensure that there is a written contract in place with that third party and to ensure that the data processor can produce a sufficient ‘guarantee’ as to the adequacy of the security arrangements which they will have in place when processing the landlord’s personal data. Security is a key consideration when appointing a data processor. This is explained further in Chapter 7.

During the ‘life cycle’ of personal data, from collection until it is finally removed from the landlord’s computer system, many different processing operations will be performed on it. The landlord will need to ensure that it has a legal ground under the DPA for each separate processing operation – though in practice a particular legal ground will often cover many different processing operations in one go and this is subject to the proviso that the tenant has been notified in advance of these processing operations.

2.4 REQUIREMENT TO BE FAIR AND TRANSPARENT

‘Fairness’ is a crucial element of Principle 1. This requires the landlord to be transparent to tenants about the nature of the processing of their personal data (see page 20).

This information must be provided to the tenant at the point at which the tenant’s personal data is collected or at the point at which the landlord wishes to use tenants’ personal data for a new purpose e.g. for research or to provide a new service to tenants.

The information is often provided by data controllers to their data subjects in the form of a written notice or statement. The manner in which this information is conveyed to the individual will, in practice, best be provided in a similar manner to that in which the information is collected. Thus, in the case of CCTV recording, this may be in the form of a prominent written notice in the vicinity of the camera.14

i) The Privacy Notice

This written notice, has, rather confusingly, come to be known by several names, all of which (usually) are referring to the same thing. They are:

• Fair Processing Notice (FPN) or Statement
• Privacy Notice or Statement
• Data Protection Notice or Statement

PRIVACY STATEMENT or PRIVACY NOTICE

Throughout this Guide, we use the term, ‘privacy statement’ to refer to the inclusion of the fair processing information within a document. A tenancy application form is an example of where a ‘privacy statement’ may be included as part of the document.

Where fair processing information is provided in a separate document, which may be given to the tenant prior to, or simultaneously with, the tenancy application, or at a later stage in relation to intended new processing, we will use the term, ‘privacy notice.’

---

13. Data processor organisations are, however, required to comply with the DPA with regard to any processing they carry out for their own purposes as data controller in their own right e.g. in respect of their own staff and customer personal data.

14. Sometimes one hears recorded messages e.g. at the railway station, in order to advise travellers that their images are being captured on CCTV for security purposes. This is an example of an aural privacy notice.
Involving tenants

A landlord should have a clear, understandable privacy notice in place. It would be good practice if, before producing it, the landlord has involved tenants’ representatives in the development and wording of the notice to make sure it is clear and unambiguous.

All tenants’ representatives should read their landlord’s privacy notice and put it to the test, challenging the landlord if the notice isn’t clear, fair and comprehensive.

2.5 PROCESSING PERSONAL DATA:

LANDLORD REQUIREMENTS

Principle 1 requires the landlord to ensure that it has legal grounds (such as consent) under the DPA to process any personal data it holds.

It is a statutory requirement for a landlord to have a legal ground (or condition) for processing tenants’ personal data\(^1\). A number of grounds are set out in the Data Protection Act\(^1\) which provide a lawful basis for landlords to process tenants’ personal data.

The DPA does not prescribe the format in which the fair processing information\(^1\) is to be provided.

However, landlords will not just collect personal data of staff and tenants. They will also hold contact details for other individuals with whom they have a commercial relationship e.g. names of staff of their suppliers or contractors. The same DPA rules apply to the processing of all of this personal data.

Landlords should be aware that wherever they collect new personal data from a tenant or where they wish to re-use a tenant’s personal data for a different purpose, then provided that there are the appropriate legal grounds to do so (e.g. such as consent) this can be done – as long as the fair processing information is provided at that point, for example, in the form of a privacy notice or statement.

\(^{11}\) The Privacy Notice and tenant consent

The provision of a privacy notice to a tenant informs the tenant about how their personal data will be used. It is not, of itself, evidence that the tenant has actually consented to this processing. However, in some circumstances, where the landlord needs to obtain the tenant’s consent for the processing of his or her personal data, it may be most efficient to use the Privacy Notice itself to enable the tenant to say whether or not they do consent to whatever is described in the Notice, for example, by providing somewhere for the tenant to sign to indicate they have read the details and agree or disagree.

Sometimes, a landlord may wish to re-use a tenant’s personal data at a later stage for another purpose. In this case, the landlord should provide a further or updated privacy notice with a space for the tenant to indicate his or her explicit consent to the processing of the personal data for this new purpose. This will be particularly important where the personal data is of the sensitive kind because the tenant’s explicit consent may be needed for the processing of this kind of data.

\(^{16}\) Under Principle 1 of the DPA; \(^{17}\) At Schedule 2

---

Privacy Notice: should contain the ‘fair processing’ information required to be given to data subjects i.e.

- the identity of the data controller
- the purpose of purposes for which the data are intended to be processed
- any other information that is necessary to enable the processing to be fair to the data subject
  - e.g.
  - the identities of others with whom the landlord may share (i.e. disclose) the tenant’s personal data
- sources from which landlords may obtain the tenant’s personal data
- how it will be kept securely
- how individuals may exercise their rights

The ICO has published on its website a ‘Privacy Notices Code of Practice’ which provides a useful guide to the content and format of privacy notices and provides examples of good (and bad) privacy notices.
It is beyond the scope of this Guide to provide an exhaustive list of processing situations in which each ground may apply. However, there are two points which need to be made clear before we consider the grounds:

(i) Landlords need to ensure that the ground(s) upon which they rely for any processing activity is/are the most appropriate to the circumstances. The grounds have specific legal meanings and so legal advice may need to be sought. However, whichever ground(s) is/are applied, there is a still a requirement to provide the fair processing information as described above

(ii) Where a landlord can find no appropriate ground(s) for the processing in question, this should prompt the questions:
• “Why do we need this personal data? Should we be processing this information at all?”
• “Can we use anonymised data instead?”

2.5.1 The legal grounds for processing tenants’ personal data

The following grounds, set out within Schedules 2 and 3 of the DPA, apply to any processing of personal data and apply to all data subjects not just tenants. The landlord, as data controller, must first decide whether or not the data to be processed is sensitive personal data, as defined under the DPA.

Data subject:
the living individual whose personal data is processed by either the data controller or data processor or both. In the case of social landlords, possible data subjects will include:
• tenants
• relatives of tenants (where their personal details are held by the landlord)
• the landlord’s own staff
• individuals employed by suppliers or third parties who provide outsourced services e.g. payroll or secure waste disposal, for example:
  • consultants
  • individuals who fall in to the above category but who have ‘moved on’ e.g. ex-tenants or staff) who are still living but whose personal data is still held by the landlord

Where an item of data is not sensitive, only a Schedule 2 ground is required. Where the item is sensitive (such as health/disability personal data), a Schedule 3 ground will be required in addition to a Schedule 2 ground.

The ‘Schedule 2’ grounds for the processing of non-sensitive personal data:
• consent – freely given, fully informed, specific to circumstances, positive indication of wishes, capable of withdrawal at any time
• necessary to perform a contract with the data subject or taking steps at his/her request with a view to entering into a contract (i.e. such as the tenancy agreement)
• necessary to comply with a non-contractual legal obligation (e.g. data sharing with local authorities under the Care Act 2014 in relation to vulnerable individuals)
• necessary to protect data subject’s vital interests (life/death situations)
• necessary for administering justice, or for exercising statutory, governmental, or other public functions (for example where the landlord wishes to collect personal data to fulfil a statutory duty)
• necessary for the legitimate interests of the landlord (data controller) or person to whom the data is disclosed, unless the processing is unwarranted because it prejudices the rights and freedoms, or legitimate interests, of the tenants (data subject). This ground could also be used to legitimise the processing involving the installation of CCTV in the public areas of a block of flats where there has been a recent spate of crime as it would be in the landlord’s legitimate interests to want to try to keep tenants safe.
Wherever a landlord is collecting a tenant’s sensitive personal data, this will, in most cases, require the explicit consent of the tenant for the processing of this kind of personal data.

However, it will not be appropriate for the landlord to ask for a tenant’s consent in situations where:

- the processing applies to ‘vital interests’: a life or death situation where consent cannot be gained e.g. because the tenant is unconscious
- the personal data is necessary for a contract that the tenant is entering into with the landlord e.g. for the provision of a new service from the landlord
- the ‘legitimate interests’ ground applies: e.g. installation of CCTV to protect the interests of both the landlord and the tenants where it would be difficult to get consent of everyone who might be filmed and if any individual said ‘no’ the landlord would not be able to prevent them from being filmed. Plenty of clear signs should be provided to warn people about the filming and reasons for it
- the landlord has a statutory duty to fulfil and the processing of the personal data is for that purpose

Consent

In some situations, there may be a number of legal grounds open to the landlord with regard to the processing in question. This may or may not include consent. However, in order to maintain the best possible relationship of trust with tenants, consent should be sought as ‘good practice’ wherever this is appropriate and possible.

Vulnerable tenants – and the need for their consent

Some tenants will require more assistance in order to maintain their tenancies. Where landlords are providing additional services to vulnerable tenants they are likely to be processing much more sensitive personal data relating to social services data, health data or probation service data, for example. This is an example of a situation in which the processing of tenants’ personal data will require the explicit consent of those individuals.

Developing and maintaining the trust of such tenants will be vitally important in obtaining such consent which will, in turn, enable the landlord to provide housing management and support services which are geared towards their needs. In addition, providing tenants the opportunity to provide their fully informed consent in such cases is also more likely to lead to a relationship with their landlord which is built on trust.

19. It is important to note that the new GDPR makes it clear that granular consents will be required in future: “consent should cover all processing activities carried out for the same purpose of purposes. When the processing has multiple purposes, consent should be given for all of them.”

20. The Data Protection (Processing of Sensitive Personal Data) Order 2000 provides a number of quite limited and specific situations in which an individual’s explicit consent will not be required for the processing of their sensitive personal data.
2.6 CHECKLIST: QUESTIONS FOR LANDLORDS

- how effectively do we monitor and execute our obligations under the DPA?
- have we carried out a data protection (DP) Audit, where necessary?
- have we carried out a risk analysis in relation to the DPA as part of our business planning process?
- have we carried out a Privacy Impact Assessment21 for each new data project we are implementing or where we are carrying out processing which is particularly risky to tenants?22
- are we clear about what tenants’ personal data we want to collect?
- are we clear about the legal grounds that are appropriate to the collection and further use of personal data?
- if sensitive personal data of tenants needs to be collected and used, are we clear about why and have we considered whether the DPA requires us to seek their explicit consent to the processing?
- why do we need this information and what will we do with it?
- in using this data, are there any benefits for tenants and if so, how can they be demonstrated?
- how are we going to communicate our organisation’s data protection policy to tenants, staff and other individuals?
- how do we provide the necessary fair processing information to tenants for the collection and use of their personal data?
- have we agreed clear policies and procedures to demonstrate our ethical values and to maintain and build tenant trust?
- what would be the consequences of a loss of customer trust?

WARNING

A ‘blanket approach’ should not be taken in the application of any of the grounds. Landlords should ensure that the processing ground applied is the most appropriate to the circumstances in any particular case.

3.1 THE BASIS OF TENANTS’ LEGAL RIGHTS

The DPA protects the personal information of individuals and prevents their personal details being used without their consent or in ways of which they are not aware.23

The DPA does not prevent a tenant’s personal information from being shared with others – for instance, in situations where it is for their benefit or necessary to protect the tenant’s ‘vital interests’ or where it is in the public interest to do so, for example to prevent crime/apprehend offenders, collect tax or to maintain national security.

3.2 SPECIFIC RIGHTS FOR TENANTS UNDER THE DPA

Tenants have the right to see their own personal data held by their landlord but they cannot see personal data that relates to anyone else, unless there is a legal ground which allows the tenant to do so - e.g. that person has provided their consent to that specific tenant seeing the information.

Tenants have the following rights under the DPA24, in relation to their own personal data held by their landlord:

(i) Right of access to personal data

This is the right, under section 7 of the DPA, which gives tenants a right to make a request in writing (including via email or social media) to obtain a copy of all of their personal data. This is called a ‘subject access request’.

Landlords can charge a maximum fee of £10 for this and must respond, supplying the information requested, within 40 calendar days25 from the date of receipt of the required fee. However, if it is not clear what information is sought or where it may be located within the landlord’s systems, the landlord may request further information (e.g. such as dates of emails or times/dates of telephone calls) from requesters to enable the data to be located. The 40 day ‘clock’ would then start upon receipt of this further information.

This right allows tenants to be:
- informed whether any personal data is held
- given a description of the personal data26
- informed as to why the information is being processed and whether it will be given to any third parties
- advised as to whether any information has been supplied to third parties

21. See Chapter 6: 6.6.22. i.e. in terms of possible harm to tenants. The risk increases if the personal data being processed is particularly sensitive, for example.

23. It supplements an individual’s right under Article 8 of the Human Rights Act 1998.24. Under the GDPR, tenants’ rights are expanded with new rights such as the ‘right to be forgotten’.

25. This right is subject to a fee of £10, with no fees for subsequent requests in any 12-month period.

26. Note that individuals are not entitled to copies of actual documents, although in practice, often, it is easier for administrative purposes for landlords to supply copies of documents containing the relevant tenant personal data - with third party details and/or information redacted/removed. Other personal data may be withheld where an exemption is applied (e.g. if it relates to on-going investigation by the Police or HMRC, for example.)
Sometimes third parties may wish to make a subject access request for a tenant’s personal data on the tenant’s behalf. This may happen, for example, where a tenant has instructed a friend or relative to obtain their personal data. In this case, at the time of making the request, the landlord would be advised to require the third party to produce:

- evidence of their own identity
- a clear and original signed authority from the tenant in question authorising the third party to seek the information on their behalf
- clear details of exactly what information is requested

Where there is a doubt as to the mental capacity of a tenant or where a third party makes a request on behalf of a tenant who clearly lacks mental capacity, landlords should seek evidence of legal authority for a third party to make a subject access request in these circumstances. This could include an original or certified copy of a power of attorney or an original or certified copy of a Court of Protection Deputyship Order which clearly provides authority for the third party to make such a request on the tenant’s behalf.

There are also a number of exemptions under the DPA that would allow a landlord to withhold certain personal data in response to a subject access request. One of these exemptions includes ‘legal professional privilege’ which protects the communications between lawyer and client.

(ii) A right (under section 10 of the DPA) to object to processing that causes, or is likely to cause, substantial and unwarranted damage/distress

In order to exercise this right, the tenant must write to the landlord explaining clearly which particular processing is objected to and why it is causing or likely to cause substantial damage and/or distress to the tenant or another person and why that processing would be unwarranted.

Upon receipt of the notice (often called a ‘section 10 notice’), the landlord has 21 days to respond and explain whether they agree with the objection and if so set out what steps they are going to take to comply with the request within a reasonable time.

A section 10 complaint cannot be made if the processing objected to is:

- personal data that is essential to the granting and continuation of the tenancy and/or essential to enable the landlord to fulfill their obligations in relation to the continuation of the tenancy
- personal data processed by a landlord to protect a tenant’s ‘vital interests’ (i.e. a life/death matter), or
- personal data which the landlord must process in accordance with a legal requirement. Chapter 4 provides information on such circumstances

Where the processing of a tenant’s personal data is based upon the tenant’s consent, the tenant may withdraw their consent if at any point afterwards they object to the processing – see section 3.3.

How can tenants find out how their personal data is being used?

- the landlord will make this clear in the Privacy Notice that the tenant will receive when they submit their data
- the landlord should have easily accessible information on its policy relating to the use of tenant data and how this policy is executed in practical terms
- a third party makes contact with the tenant regarding the disclosed data. This third party might, for example, be the police or a contractor seeking access to the tenant’s home to undertake repairs or gas or carbon monoxide safety checks

Tenants may become aware that their data has been misused if:

- the landlord voluntarily reports a data breach to the ICO – the landlord may be required to inform all persons affected by the data breach
- the ICO launches its own investigation into a landlord which results in official action, publicised on its website
- the tenant receives direct marketing communications from the landlord or other third party which he or she has not consented to receiving

If, at any point, a tenant is concerned about the use of personal data submitted to a landlord – or who it is being disclosed to – they can make a subject access request to the landlord in order to find out exactly how the data is being processed and what third parties it is being shared with.

If the tenant is unhappy with the response (or lack of one) by the landlord, they can formally object to the landlord about the use of their data. If following this objection, the tenant is still unhappy, other remedies are available.

These issues are explained in more detail in this Chapter 3 of this guide.
Tenants’ rights under the Data Protection Act 1998

NOTE
A section 10 objection is only available to the tenant where the processing complained of by the landlord is based upon the statutory processing or legitimate interests grounds.27

(iii) A right to object to processing that involves a landlord making a decision about a tenant based solely on automatic means

This right does not prevent the landlord making the decision – it simply provides the tenant with a right to require the landlord to have the decision reviewed by a human being rather than by computer. This right is also subject to certain exceptions.

(iv) A right to object to the landlord using personal data for direct marketing purposes

‘Direct marketing’ under the DPA has a very wide meaning and does not bear the ordinary everyday interpretation i.e. it does not just relate to marketing with a commercial implication or with the sale of a product or service in mind. It includes all promotional or advertising material aimed at particular individuals and intended to promote the ethos, aims or beliefs of a particular organisation.

Thus, for example, if a landlord writes to a tenant personally inviting them to participate in an event designed to promote public awareness of work done by the organisation this would count as ‘direct marketing’ for the purposes of the DPA. Where such communication is made by email, text message, telephone or social media, the rules relating to direct marketing under other regulations (Privacy and Electronic Communications Regulations 2003) will also apply.

Individuals have a very strong right to object to the use of their personal data for a direct marketing purpose. The right can be exercised by the tenant in writing to the landlord and asking for the processing for direct marketing to cease. No reason need be given and the landlord must stop within a reasonable time.28

The ICO has published guidance on its website regarding the direct marketing rules and has also produced specific guidance for organisations where the direct marketing is to be carried out by electronic means.29

Direct marketing material will not include communications from the landlord to the tenant in connection with the tenancy and in order for the landlord to fulfil its obligations to the tenant in connection with the tenancy.

27. See page 22 above for the legal ‘grounds’ for processing personal data under Schedule 2 of the DPA. 28. The ICO recommend that electronic means of direct marketing cease within 28 days and postal marketing within 2 months. 29. Direct marketing by electronic means falls within the scope of the Privacy and Electronic Communications Regulations 2003 (PECR), also regulated by the ICO.

(v) The right for individuals to take action against the landlord for compensation through the civil courts

Where damage or distress has been suffered by the tenant as a result of the landlord breaching any of the requirements of the DPA, the tenant can take action against the landlord for compensation.30 The court also has the power to make an order requiring the landlord to rectify, block, erase or destroy inaccurate personal data.

3.3 THE RIGHT TO SAY ‘NO’ AND ‘STOP’ WHERE THE PROCESSING OF THE TENANT’S PERSONAL DATA IS BASED ON CONSENT

As explained in Chapter 2, landlords have obligations and duties under the DPA to make sure they have legal grounds for processing tenants’ data – the tenant’s consent being one such ground. It has already been explained that for consent to be valid it must be freely given, specific to the circumstances and capable of withdrawal at any time.

Therefore, where a landlord decides that consent is the most appropriate ground for processing a tenant’s personal data, that tenant has a clear right to say ‘no’ at any stage if they wish to change their mind and withdraw the permission which they have provided.

3.4 THE RIGHT TO COMPLAIN

If a tenant believes their landlord has failed to meet any of its duties or obligations to them under the DPA in relation to their personal data, the tenant has a right to make a complaint to the ICO if they wish to do so.

30. There is a defence for the landlord if it can prove that it had taken reasonable care to comply with the DPA.
3.5 PUTTING RIGHTS INTO PRACTICE

If tenants feel their rights have not been adhered to by the landlord, and/or they consider that they have been unfairly affected by the use of their personal data, they can:

- complain to the landlord – utilising the landlord’s formal complaints procedure
- complain to the ICO and request an investigation – this should be done if the complaint has not been resolved to the tenant’s satisfaction following a complaint to the landlord
- commence proceedings through the civil courts for compensation where they have suffered harm as a result of a breach of the Act. Again, tenants should complain to their landlord before considering legal action. Legal advice is strongly recommended if litigation is contemplated.

Tenants should make a request in writing (this can also be done by email) in order to exercise any of their rights under the DPA. However, it may be reasonable in some circumstances for landlords to accept requests made verbally e.g. if the request is made by a disabled person unable to make a written request or if the making of a written request would place the individual concerned at substantial disadvantage if they had to do so.

Landlords should have in place a written policy or procedure for dealing with subject access requests, including the situation where a tenant’s personal data is processed by a third party (data processor) on the landlord’s behalf. Landlords may encourage tenants to make the subject access request on their own prescribed form, for ease of administration, although they cannot be compelled to use such a form.

3.6 CHECKLIST: QUESTIONS FOR TENANTS

- What personal data about me has my landlord already got?
- How can I see my personal data?
- Why is my landlord holding this data and what will they do with it?
- Who else will be able to see this data?
- How do I get a copy of my data?
- What other information does the landlord want to collect?
- How might the processing of this information affect me and other tenants?
- Am I happy to agree to whatever processing my landlord wants to do?
- Can I refuse to let my landlord have the information being asked for?
- What are the legal grounds for processing my personal data (if not strictly needed for my tenancy)?
- If I have provided consent to the use of my data, how can I later withdraw my consent?
- What has been done with my data?
- How long will my data be kept and how will it be stored?
- What will happen to my data after it is no longer needed?
In this chapter we address the legal requirements that landlords need to be aware of before taking the decision to share any personal data. The ICO has published a statutory Data Sharing Code of Practice, (the Code) available here. It is very important that landlords that are proposing to share personal data, pay close attention to the advice in this Code. Not only does it provide extensive guidance on the DPA rules relating to the disclosures of personal data but, in the event of a data breach, the ICO is likely to enquire into the extent to which the Code was followed.

The term ‘data sharing’ covers a wide range of situations in which personal data may be transferred from one organisation to another. It includes instances where there is one-way movement of personal data or where there is two-way exchange between organisations. The sharing may take the form of a ‘one-off’ sharing or there may be on-going or regular sharing of personal data.

4.1 SHARING DATA WITH THIRD PARTIES: LANDLORD OBLIGATIONS

A landlord may either receive a request from a third party or it may decide it wishes to share personal data with that third party. The information shared could be that relating to any individual whose personal data is held by the landlord e.g. a tenant, member of staff of the landlord or a contractor or a business contact of the landlord.

In some cases, the landlord will be required by law to share individuals’ personal data and sometimes sharing can be essential to protecting a tenant from harm. In other cases, personal data is shared to gain insight into that data, for the benefit of the housing sector and/or society in general.

Sharing with third parties: examples  (NB: This is not an exhaustive list)

- local authorities, the police and other public bodies for the purposes of crime prevention/reduction
- HMRC for the assessment and collection of tax in relation to the landlord’s employees
- contractors, for example for the purposes of repairs to a landlord’s housing stock
- debt collection agencies and tracing agents, for the purposes of collecting unpaid rent from tenants who have vacated the landlord's property without paying rent due
- Department of Work and Pensions (DWP) and local authorities for the purposes of universal credit claims
- local Safeguarding Authorities, for the purposes of making a safeguarding alert where there is a concern regarding the safety of a child or vulnerable adult

The landlord should, first of all, consider the capacity (under the DPA) in which the recipient of the shared personal data is to receive the information. If the other party is a data processor, i.e. processing only on the landlord’s instructions and at its direction, this has quite significant legal implications, as discussed in Chapters 2 and 7.

The key points for the landlord to consider are:

(i) the landlord will be legally responsible, not only for its own breaches of the DPA, but also for any breaches caused by the actions (or inactions) of its data processor
(ii) the sharing of personal data with its data processor will not, of itself, require specific legal grounds under the DPA in the same way as ‘data controller to data controller’ sharing. The landlord would, however, need to ensure that it has the legal grounds to process the personal data in the first place – in the way that it would need to have grounds for its own staff to process the information

In the next section we consider how the above may apply in practice.
### 4.2 DATA SHARING WITH CONTRACTORS: EXAMPLES

**Example 1: External contractor providing a secure paper shredding/confidential waste destruction service**

A third party contractor carrying out the above service and acting only on the instructions and at the direction of the landlord data controller will be a data processor for the purposes of the DPA.

Shredding or destroying personal data is a processing activity and therefore the processing must be done in accordance with the Data Protection Principles. It would be the data controller landlord’s responsibility to ensure that this is the case.

There must be a contract in place with the company providing the service and this contract must include specific data protection clauses. As the secure shredding company is a data processor, the landlord will be accountable to the ICO and any data subjects for any breach of the DPA, including any breach caused by the waste disposal company.

Thus it is important for landlords to ensure that the company has adequate technical and organisational security measures in place to ensure that the risk of any breach is minimised. There have been cases in the media in recent years where organisations employing companies offering this kind of service have received large monetary penalty notices from the ICO where papers containing very sensitive personal data have been ‘dumped’ in public recycling bins.

**Example 2: Landlord employs the services of a third party tracing agent or debt collection agency to collect unpaid rent**

A landlord is unable to contact a tenant who has moved to a new address, owing money under the tenancy agreement. The tenant has not notified the landlord of his new address and therefore the landlord has decided to appoint a debt collection agency to locate the tenant and seek repayment of the debt.

In order to do this the landlord will have to disclose the tenant’s personal data to the debt collection agency, even though the tenant has not consented to this disclosure.

The key difference between this example and the first one is that whereas the external waste disposal company would be regarded as a data processor, in this second example, the tracing agent/debt collection agency would be likely to be acting as a data controller, as it would have to process the tenant’s personal data for its own purposes (as a debt collection agency/tracing agent) in order to carry out the service for the landlord.

The sharing of any personal data between the landlord and the debt collection agency will be a ‘disclosure’ of personal data from data controller to data controller and therefore a legal ground under the DPA will need to be identified in order for the sharing or disclosure to go ahead – unlike the sharing of personal data between landlord and its own staff or between landlord and its data processor.

In this case, obtaining the consent of the departed tenant for the processing of his or her name and address so that the landlord can track him/her down in order to ask for the unpaid rent is not going to be possible for obvious reasons. The landlord may be able to rely upon the ‘legitimate interests’ ground for the processing:

> “the processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.”

This ground requires that the landlord’s interests must be balanced against the interests of the tenant in this case. If the disclosure of the tenant’s personal data to the debt collection agency is ‘unwarranted’ because of its prejudicial effect on the rights and freedoms or legitimate interests of the tenant, then the disclosure should not be made and to do so would represent a breach of the DPA.

However, as the ICO has pointed out, the landlord’s legitimate interests do not have to be ‘in harmony with’ those of the tenant. It is only where there is a ‘serious mismatch between competing interests’ that the tenant’s interests would come first in this particular situation.

In this example, it is easy to see that there are very different interests between those of landlord and tenant i.e. the tenant may well be very interested in not paying their debt. However, the disclosure of the tenant’s personal data in this situation would not be ‘unwarranted’ as it would clearly be a legitimate interest of the landlord to seek the payment of the debt.

The processing described above must still meet all of the Data Protection Principles, in that the landlord must ensure that the personal data passed to the debt collection agency is:

- accurate (in terms of the details which are known about the tenant)
- up-to-date (in terms of the amount outstanding and the tenant’s last address, which the landlord will clearly know)
- not excessive – the debt collection agency should only be given as much personal data as is relevant and necessary for the purpose of finding the tenant and recovering the debt.
4.3 REQUESTS FOR DISCLOSURE BY THIRD PARTIES

We have considered situations where a landlord may need to share personal data with a third party contractor for the landlord’s own legitimate business purposes.

However, a landlord may receive a request for the sharing of personal data (e.g. that of tenant or member of staff) from a completely separate external body (either public or private) with which it does not have an existing relationship. It may involve a one-way disclosure from the landlord to third party or a mutual exchange of personal data.

In data protection terms, this kind of sharing is likely to be a ‘data controller to data controller’ disclosure of personal data, if both landlord and third party are using the personal data shared for their own legitimate purposes and not simply acting on the instructions of the other party with regard to how the personal data is to be used.

The landlord will need to consider:

1. What powers it has to share the information
   - Most public sector body powers derive from Acts of Parliament and so they will have to ascertain whether the relevant statutes provide them with the ability to share the information requested.
   - Private sector landlords should check their Articles of Association in respect of any particular data sharing powers.

2. What does the landlord’s privacy notice say about the sharing?
   - It is important that any privacy notice provided to the individual whose personal data is to be shared, whether it be a tenant or member of staff, for example, contains information about this sharing at the time of collection of their personal data (e.g. in the tenancy application form) particularly if it is not the kind of sharing that the tenant might expect.

Example 3: Security company providing CCTV surveillance for the purposes of crime reduction/prevention

A housing association has suffered a spate of crime in a particular area. The landlord decides to employ a third party security company to monitor communal areas in a block of flats, where there have been particular problems, using CCTV.

The security company is acting on the instructions and at the direction of the landlord and so there should be a data processing contract in place with the company—setting out the data protection assurances for the landlord data controller, as described in Chapter 7.

The landlord will need to ensure that there is clear signage in the vicinity of the cameras in order to ensure that the requisite fair processing information has been provided to potential data subjects who are caught on camera. The data subjects captured on film could, for example, be tenants, individuals visiting the tenant, or the landlord’s or contractor’s staff or other tenants. Each of these data subjects will have the rights set out above, under the DPA, as such the right of subject access, in relation to the landlord data controller.

The landlord would be able to make use of the non-consent-based ‘legitimate interests’ condition in relation to this processing carried out by the data processor contractor, but the collection of personal data must also be carried out in accordance with all of the Data Protection Principles as discussed above. In particular, the cameras should be situated in areas which will not represent a risk to the ‘rights, freedoms or legitimate interests’ of the individuals who might be captured on the footage. For example, cameras should not be situated in areas such as toilets, or in a tenant’s home.

If potentially criminal activity is captured on film, showing the suspected offender, this footage could be legitimately disclosed to the police, applying the crime prevention/detection exemption, without the knowledge of the potential offender in the footage, if failure to do so would prejudice the crime prevention purpose.

Other examples of contractors who may provide a service to the landlord which involves processing of tenants’ personal data:

- external researchers
- independent tenant participation advisers
- maintenance contractors
- builders and major works contractors
- managing agents
- external auditors

The ICO has stated that the need to actively communicate a privacy notice is strongest where:

- you are sharing sensitive personal data or
- the data sharing is likely to be unexpected or objectionable or
- the sharing is particularly widespread, involving organisations individuals might not expect or
- the sharing is being carried out for a range of different purposes
(iii) What legal grounds, under the DPA, will apply to the disclosure?

For example, is tenant consent going to be required or will another ground (such as the ‘legitimate interests’ ground discussed above in the example of the debt collection agency) be the most suitable ground?36 This depends on what kind of personal data is being requested and by whom and for what purposes.

In determining the legal grounds which may apply under the DPA, the landlord will also need to consider whether the sharing would fall into the category of a mandatory disclosure required by law or a discretionary disclosure where the law allows data to be shared but does not require it.

4.4 MANDATORY LEGAL DISCLOSURES

In this situation landlords have no choice but to comply, otherwise they risk breaking the law.

Where a third party makes a request under a mandatory legal ground it is important that landlords seek clarification as to the specific statutory requirement by asking the requester to provide the name of the relevant legislation and the specific section/clause relied upon. Where a court order is served on a landlord this should provide clear evidence of the need to comply.37 However, landlords should seek legal advice if they are uncertain as to whether any particular legal provision relied upon by the requester does indeed oblige the landlord to provide the information sought.

Where a mandatory legal disclosure is required, the appropriate legal ground, under the DPA, which allows the landlord to disclose this information,38 would be the following:

- the processing is, “necessary for the compliance with a legal obligation to which the data controller is subject, other than an obligation imposed by contract.”

There is also an exemption39 which may be applied by the landlord to any disclosure or sharing of personal data under this ground (disclosures required by law), which means that:

- the disclosure would be exempt from many of the Data Protection Principles, to the extent to which the application of the Principles would prejudice the disclosure
- the individual whose personal data has been disclosed would not need to be provided with a privacy notice in respect of the disclosure (if it do so would prejudice the disclosure)
- the individual whose information is disclosed would not be able to object to or block the disclosure of his/her personal data.

Examples of where landlords may be compelled by law to provide personal data of tenants to third parties include:

- under the Care Act 2014: to provide details to local authorities in relation to vulnerable individuals at risk, for safeguarding purposes
- water companies with properties ‘wholly or mainly in Wales’ have a new power (as from 2015) to obtain certain details relating to the occupiers of premises in the area for which they provide the water supply40
- HMRC requires the disclosure of financial personal data of employees in connection with the assessment and collection of tax
- to protect national security
- when served with a court order to disclose

4.5 DISCRETIONARY DISCLOSURES (where there is a legal power, as opposed to a requirement to share data)

In certain circumstances, landlords may be asked to disclose personal data in situations where a separate Act of Parliament or legal rule provides the power to share personal data but it is not a mandatory legal requirement.

For example, under the Crime and Disorder Act 1998, landlords are able to share personal data with local authorities, the police, probation committees and health authorities, such as where this is necessary or expedient for the purposes of the above Act (i.e. linked to crime reduction strategies).

There is also a statutory gateway which permits the sharing of tenants’ personal data between DWP, local authorities, social landlords and a number of other partners for the purposes of universal credit claims – under the Welfare Reform Act 2012 and related regulations.

---

36 In deciding which legal ground applies, legal advice may need to be sought if it is not clear. Where sensitive personal data is to be shared, it is likely that data subjects’ explicit consent will be needed. Landlords should apply the non-consent based grounds with caution. 37 It is important to check the wording of the court order carefully. 38 DPA Schedule 2, para 3. 39 Under section 35(1) of the DPA. 40 The Water Industry (Undertakers Wholly or Mainly in Wales) (Information about Non-owner Occupiers) Regulations 2014. These changes, which affect landlords, letting agents and Local Authorities, came into effect on 1 January 2015 and require landlords to inform the water supplier about tenants in their properties within 21 days of the tenants moving into the property. If this is not done, the landlord can become jointly and severally liable with the tenant for any outstanding water and sewage charges.
(i) Disclosures to the police

Where the police contact a landlord requesting disclosure of a tenant’s personal data, this kind of disclosure can be made at the discretion of the landlord unless, for example, the police produce a court order for the disclosure, whereupon the disclosure will be mandatory (see above).

Where the request comes as part of a police investigation and the police state that the disclosure is required in connection with the prevention and/or detection of crime or the apprehension or prosecution of offenders, an exemption under the DPA means that, if landlords choose to make the disclosure and apply this exemption, they do not need to inform tenants and the disclosure is exempt from many of the other data protection principles, but only to the extent to which adhering to the DPA principles (e.g. informing the tenant) would prejudice the police investigation. In addition, tenants would not be able to exercise their subject access right to obtain details of what was passed to the police, if this might prejudice the police investigation.

It is important for landlords to bear in mind that they have a choice as to whether to make such a disclosure and whether they wish to apply the exemption. The exemption must be applied on a case by case basis and the use of the exemption requires the landlord to weigh up the possible risk of prejudice to the tenant’s rights against the risk of prejudice to the police investigation if the disclosure is made. Tenants cannot object to this kind of processing.

As with the application of all exemptions, landlords are strongly advised to document carefully their reasons for the application of the exemption to this disclosure.

(i) Disclosures for the purposes of the assessment of collection of tax or similar duty

A similar exemption applies to organisations such as HMRC or local councils that request personal data in connection with the assessment or collection of any tax or similar duty – income tax, national insurance contributions or council tax, for example.

4.6 OTHER TYPES OF DATA SHARING

There are a range of circumstances in which landlords will identify a clear business need or a direct benefit to tenants in sharing tenants’ data with other data controllers.

Example: Landlord holds sensitive personal data and discloses to third party to save tenant’s life: application of the ‘vital interests’ condition

A tenant with disabilities has health problems associated with her particular physical disability. This information has been collected by the landlord from the tenant in her tenancy application form and is collected in order to provide suitable accommodation for the tenant and (ii) to monitor the effectiveness of the landlord’s Equality and Diversity Policy.

The landlord has the explicit consent of the tenant for the use of their health and disability information for the purposes of providing suitable accommodation and in relation to the equality monitoring, there is an appropriate non-consent-based ground available to the landlord to collect this disability information for the purpose of equality of opportunity monitoring.

The tenant is found unconscious on the ground outside the door to her flat by the landlord’s local housing officer. The local housing officer immediately calls the emergency services and upon arrival, provides the paramedics with information held by the landlord in relation to the tenant’s health/disability. The tenant is then provided with the appropriate treatment and her life is saved.

This is a ‘life and death’ situation and an example of a situation where the ‘vital interests’ ground (under both Schedules 2 and 3) of the DPA can be applied to disclose very sensitive personal data without the tenant’s consent.

The other Data Protection Principles would apply which would mean that the housing officer should only provide personal data which is adequate, relevant and not excessive for this purpose i.e. the health data and not information relating to the tenant’s trades union membership or sexual orientation, for example.
4.7 REGULAR AND ON-GOING DATA SHARING

It is very important that when landlords decide to carry out any kind of data sharing, that they comply with the ICO's Statutory Data Sharing Code mentioned above.

For regular sharing, a data sharing protocol is strongly recommended, with the appropriate legal grounds for sharing (under the DPA) identified. Such a protocol should address how the data controller organisations involved in the sharing project are going to ensure that they comply with the eight Data Protection Principles, as each will be liable in their own right under the DPA, but where they work closely together as joint data controllers, a breach by one organisation could, in certain circumstances, mean that either one or both are liable for any harm caused to data subjects, or subject to enforcement action by the ICO. The ICO, for instance, may look at how they agreed to apportion their duties and obligations under the DPA in any data sharing protocol.

A Privacy Impact Assessment (PIA) is strongly recommended (see Section 6.6) before undertaking any risky processing and in particular, where new projects involving personal data are used. The more sensitive the personal data and the greater the risk of potential harm to the individuals involved, the greater the need for a PIA. This should be carried out in the early planning stages of any new project involving tenants' personal data.

Examples are discussed below in relation to the use of 'Digital Inclusion' and projects to help financially excluded tenants. 'Sharing' may involve the one-way disclosure of personal data from landlords to a third party or it may involve a mutual exchange of personal data.

i) Data from rental payment records and use of credit reference agencies

There are frequent instances where, in order to gain access to services and products, individuals need a 'credit identity' or 'credit score'. Many tenants have no such identity or score, so a group of people who are often already disadvantaged are doubly disadvantaged by being unable to access these services or products. Some credit reference agencies provide a simple mechanism to enable tenants to establish such an identity or credit score - they may then be able to gain access to goods and services such as mobile phone contracts and credit cards at more favourable rates.

ii) Helping financially-excluded tenants

Many social landlords have been working on different projects to help financially excluded or disadvantaged tenants, including providing money advice services and setting up credit unions.

Data analysis can help the landlord identify the circumstances in which tenants may need help and advice. The business case for the landlord would be that by helping tenants to manage their finances and budgeting better, they would be better able to pay their rent on time.

iii) Digital inclusion

Many social housing landlords have been working on ways to help tenants get access to the web and online services. The business case for the landlord is that the tenants can access their rent accounts, report repairs, and look for transfers and exchanges online by themselves. The advantage for the tenant is that they can access online services such as banking or cheaper deals and, if they struggle to get out of their home or to reach shops, they can order goods online.

From a DPA compliance perspective, it would be important when undertaking any new project, such as those listed above, that the Data Protection Principles above are followed.
The Information Commissioner’s Office (ICO) is responsible for enforcement action in relation to the DPA. A breach of the DPA can be brought to the attention of the ICO in a number of ways by anyone including a tenant or the landlord:

• a complaint from anyone who believes that their personal data has been processed in a way that does not comply with the DPA and requests an investigation
• a complaint by a third party (i.e. whose personal data is not held by the landlord) who believes that a landlord is processing in breach of the DPA
• media reports which indicate an apparent likelihood of a breach
• a landlord self-reporting a serious breach of the DPA that has come to its attention

5.1: REPORTING A BREACH OF THE DPA TO THE ICO

The ICO does not expect all breaches to be reported – only those that are serious enough to involve significant harm to affected individuals. Landlords can find helpful guidance on the ICO website, available here, which explains when and how to report a breach. The ICO will focus on the risk of potential harm to the individual(s) concerned.

Factors that landlords should take into account when assessing whether to report a breach are, in general terms:

• the amount of personal data that is involved in the possible breach
• how sensitive the personal data is (is it sensitive personal data as defined under the DPA or is it sensitive in some other way e.g. bank account details?)
• the seriousness of the harm to the individual(s) concerned

Landlords should also notify tenants or any other affected individuals who may suffer harm as a result of any breach so that they may take steps to protect themselves.44

43. Dated 2012. 44. Landlords may need to notify other official bodies (such as the Police or local authority) in appropriate cases.
5.2 ENFORCEMENT BY THE ICO

The ICO may investigate and issue a warning or take official enforcement action if it believes that there has been a serious breach of the DPA. The ICO may start by asking for further information relating to the circumstances of the suspected breach. If this investigation reveals a contravention of the Data Protection Principles, the organisation at fault may be issued with an Enforcement Notice requiring it to take specified steps to rectify the contravention or refrain from processing specified personal data.

For serious breaches, a fine (monetary penalty notice) of up to £500,000 can be imposed. In less serious cases, the ICO will accept an undertaking (a kind of legal promise) to improve, which, if breached, can lead to further investigation by the ICO which could, in turn, lead to an enforcement notice or fine (monetary penalty notice) being imposed if there has been a breach of any of the Data Protection Principles.

In certain circumstances, the ICO may decide to prosecute either an individual or an organisation that has breached the DPA. Examples of criminal offences include failure to respond to enforcement notices, or failure to register with the ICO or to notify the ICO of any changes to the way data is processed.

It is also a criminal offence for an individual to obtain or disclose personal data held by an organisation without the consent of that organisation. This offence could be committed, for example, by an employee of a landlord accessing personal data of a tenant without line manager approval. Where a criminal offence under the DPA is due to the ‘neglect, connivance or consent’ of a director or senior office holder of a company, the director or senior office holder may also be prosecuted.

Punishments for any of the above offences include a fine of up to £5,000 in a magistrates’ court or an unlimited fine in Crown Court. The ICO is keen to introduce prison sentences for the most serious criminal offences under the DPA, although these have not yet been brought into force.

All of the above can, of course, result in attendant adverse publicity and reputational damage. The ICO publishes all official enforcement activity on its website.

5.3 CHECKLIST: AVOIDING ENFORCEMENT ACTION BY THE ICO

Landlords should be aware that, where it is investigating a breach and determining what enforcement action to adopt, the ICO looks much more favourably upon organisations that actively demonstrate their commitment to data protection compliance by:

- Ensuring an appropriate level of technical security for all personal data processed, particularly with regard to sensitive personal data of staff and tenants
- Providing regular and ongoing training in data protection so that all staff understand their duties and responsibilities in handling personal data
- Fostering a culture of compliance, with the development of transparent privacy notices and appropriate data protection policies and procedures, including a policy clearly setting out what is to be done in the event of a data breach
- Dealing proactively with data breaches, taking immediate steps to mitigate loss or harm to individuals, and working cooperatively and in a transparent manner with the ICO
6.1 TRANSPARENCY AND THE BUSINESS CASE FOR ETHICAL BEHAVIOUR

There are good business reasons for adopting an ethical (open, honest, accountable) approach to the processing of the personal data of individuals such as tenants and employees. Being seen as a responsible and trustworthy custodian of customer data could give a business advantage to the landlord. Other organisations are more likely to enter into data sharing initiatives with landlords who demonstrate sound compliance as it is less of a business risk to them.

By working with tenants to be open and honest in relation to obtaining and using tenants’ data and by putting in place mechanisms to enable tenants to hold the landlord to account (for example via scrutiny panels) the risks in relation to falling foul of data protection and privacy law and regulations should be mitigated.

Tenants can help the landlord make sure information provided meets tenants’ needs and is provided in an understandable and accessible form. By working together with tenants, landlords can make sure they maintain tenants’ trust and confidence.

If the landlord’s Data Protection and Privacy Policy has been developed with input from tenants it is more likely to be effective in addressing tenants’ needs - as well as protecting the landlord’s interests.

6.2 INVOLVING TENANTS

Any landlord wanting to make use of and/or share tenants’ data should involve tenants from the outset in defining what is going to be done, why, and how, and what information tenants need to have to enable them to understand what is happening and to provide their informed consent.

It is vital that the landlord explains why the collection of the personal data is either mandatory in law or will help the landlord to deliver better services or protect the vital interests of tenants. Landlords should also explain in what circumstances data will be supplied to third parties.

Tenants may not wish their landlord to know about personal details such as specific health, relationship or financial problems, or about their income. They may feel that if they did not have to give any of this information when they were granted their tenancy and if they have managed to pay their rent and maintain their tenancy without causing nuisance or annoyance to their neighbours, why should their landlord have such information?

However, there may be a good ‘business case’ for the landlord to have this information and it may be of benefit to the tenant to provide it to their landlord. It may be possible for the landlord to ensure help and support is provided to a tenant facing personal difficulties. The challenge for the landlord is how to enable the tenant to understand the potential benefits of the landlord collecting personal information without the tenant feeling their privacy has been violated.

Many landlords work in partnership with their tenants as part of normal day-to-day good working practice. Tenants’ representatives are the ideal people to help their landlord identify the best message and methods of communication to gain tenants’ confidence and trust. Whether a landlord has a formal arrangement to work with a landlord-wide tenant group such as a scrutiny panel or other recognised tenants’ body, or a less formal consultative arrangement, involving tenants in data protection and privacy is critical to achieving the benefits and avoiding the pitfalls.48

48. There is a risk of excessive amounts of personal data being collected (in breach of Principle 3) and there is risk of personal data being used for a different purpose than that for which it was originally collected, in breach of Principle 2. It is also important to ensure that the processing is transparent and that individuals are aware of exactly how their personal data is to be used. Where possible, anonymised data should be used.
6.3 ACCOUNTABILITY AND TENANT CONSENT

By being open, honest, transparent, and accountable to tenants in relation to how their data is obtained and used, landlords will go a long way towards ensuring that the way they use the data complies with all aspects of data protection law.

As we have already explained in Chapter 2 ‘Landlord’s Obligations’, landlords must provide tenants with clear information about who wants to do what with their data and why they want to do it.

Providing that this information is clear, in plain language and easily accessible, tenants will be able to understand what is being done and can hold their landlord to account by asking questions and challenging anything with which they do not agree or which they believe undermines their rights to data privacy.

It is often the case that landlords need to collect information of a sensitive nature (e.g. relating to health and disabilities) in order to demonstrate compliance with their own duties under other legislation and to ensure that they are able to meet the requirements of tenants with particular needs. If this kind of information is not provided by tenants it may mean that landlords may not be able to provide the most suitable accommodation (it may even make it very difficult to grant the tenancy at all) and if this is the case, it should be made clear to the tenant so that he or she is fully informed and feels confident that they are providing information which will assist the landlord in providing the best possible service to them.

Although there are instances where landlords may have to obtain and use a tenant’s data whether the tenant agrees or not (see 2.5.1 and Schedules 2 & 3) there are likely to be many circumstances where the landlord could decide that the most appropriate ground for a particular data processing activity is ‘tenant consent’.

Where a landlord has a commitment to being accountable and working in partnership with their tenants, their Data Protection and Data Privacy Policy should say consent will be sought wherever possible and appropriate. However, landlords must guard against adopting a ‘blanket’ approach. There are likely to be circumstances where this consent will not be the most appropriate ground and using the ‘legitimate interests’ condition may be in the best interests of both the landlord and the tenant.49

NOTE

The loss of customer trust is something landlords should consider, as it may result in:

- tenants no longer turning to the landlord for help
- tenants no longer volunteering information to the landlord
- active tenants publicising their loss of trust/critical views about the landlord in social media
- tenants making a challenge to the landlord’s use of personal data
- tenants complaining to the ICO – potentially resulting in large fines for the landlord if the processing is shown to be in breach of the DPA and has resulted in substantial harm or distress to tenants

6.4 TRANSPARENCY AND FAIRNESS

Landlords committed to an ethical approach in relation to data protection and privacy should seek to be as open, honest, fair and transparent as possible when collecting, using, or re-using both personal data and sensitive personal data. This means making clear to tenants exactly what data is being collected, why, what will be done with it, and what rights tenants have in relation to giving and withdrawing consent and what rights of access they have to their own data.

As public concern about misuse of personal data increases, fuelled by the continuation of scandals involving misuse of private information such as we have seen in recent years, commercial organisations are taking action. They are seeking to maximise the benefits of Big Data by actively seeking to expand the instances where they can be ‘up front’ with individuals about how their personal data will be used and by giving assurances that it will be processed correctly, securely, and in accordance with the DPA.

Whilst this approach may initially involve greater administrative activity and expense, the benefits should outweigh these initial disadvantages, especially in relation to maintaining customer trust. Being fair and transparent can:

- reduce the risk of non-compliance under the DPA
- reduce the risk of ICO fines or tenant legal challenge
- align with increasing commercial sector recognition of the benefits of customer trust
- reinforce the landlord’s ethical values and avoids brand damage and loss of customer trust

49. See Chapter 2: 2.5.1
6.6 PRIVACY IMPACT ASSESSMENTS (PIAs) 53

This is a type of risk assessment which is carried out prior to the commencement of any type of processing which may be regarded as particularly risky in terms of the potential harm to the data subjects involved. PIAs are not mandatory under the DPA.54 However, the ICO does ask organisations if one has been carried out, particularly where concerns have been raised over their processing activities. It is an effective means of demonstrating that the organisation is compliant with the DPA.

Moreover, there are significant benefits to conducting a PIA as the ICO has explained in its helpful guide, Conducting Privacy Impact Assessments Code of Practice (2014).

“The first benefit to individuals will be that they can be reassured that the organisations which use their information have followed best practice. A project which has been subject to a PIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A second benefit to individuals is that a PIA should improve transparency and make it easier for them to understand how and why their information is being used.

Organisations that conduct effective PIAs should also benefit. The process of conducting the assessment will improve how they use information which impacts on individual privacy. This should in turn reduce the likelihood of the organisation failing to meet its legal obligations under the DPA and of a breach of the legislation occurring.

Conducting and publicising a PIA will help an organisation to build trust with the people using their services. The actions taken during and after the PIA process can improve an organisation’s understanding of their customers.

There can be financial benefits to conducting a PIA. Identifying a problem early will generally require a simpler and less costly solution. A PIA can also reduce the ongoing costs of a project by minimising the amount of information being collected or used, where this is possible, and devising more straightforward processes for staff.

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within an organisation and ensure that all relevant staff involved in designing projects think about privacy at the early stages of a project.”

50. See dedicated page of ICO’s website which can also be found here.
51. This is approach is also adopted in the new EU General Data Protection Regulation, alongside certification schemes and ‘privacy by default’ which allate organisations to demonstrate their compliance to regulate standards of EU compliance. 52. The Government Data Programme has developed a Data Sharing Impact Compliance, to help organisations understand the benefits and risks of using personal data when developing policy. The Framework can be a useful tool if you are working on a project involving data science. Big data or analytics. If you are doing a PIA, the framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.” ICO Code of Practice on PIAs

Example

Some organisations, including some social landlords, are now providing a customer portal, accessed through a secure log-in on their website which allows tenants or customers to view their accounts and pay bills.

The tenant/customer may update their contact details and correct any inaccuracies in the data.

Some telecoms providers also provide customers access to a full log with transcripts of all conversations with staff, including dates and times of those conversations. Customers are able to leave messages for staff with whom they have had direct contact either over the phone or electronically, and receive replies from staff.

The customer portal allows the organisation to keep customers abreast of changes and update fair processing notices where necessary.

In addition, a ‘privacy by design’ approach has as its central theme the concept of ‘data minimisation’. By adopting this approach, organisations design their systems and procedures with the objective of collecting only the minimum necessary personal data they need in accordance with the purpose for which it is collected and made clear to data subjects. Such an approach demonstrates clear adherence to the principles of the Data Protection Act which require the data processed to be ‘adequate, relevant and not excessive,’ “only processed with declared purposes,” and ‘accurate and up to date’.

Conducting a Privacy Impact Assessment (PIA) is integral to a Privacy by Design approach to processing.

6.5 PRIVACY BY DESIGN

The ICO states that, “Privacy by Design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.”

Although not a mandatory requirement of the DPA, the ICO is keen to see this approach adopted as it is an effective means of ensuring and demonstrating DPA compliance.53

The ICO recommends that organisations build data protection compliance into the early stages of a project and then throughout its life cycle e.g. when

• building new IT systems for storing or accessing personal data
• developing legislation, policy or strategies that have privacy implications
• embarking on a data sharing initiative, or
• using data for new purposes

Such an approach may be costly and time-consuming to set up, but the longer term potential commercial gains can far outweigh the initial cost of resourcing.

53. Rebranded as Data Protection Impact Assessments under the new EU General Data Protection Regulation. 54. Under the new Regulation, Data Protection Impact Assessments will be mandatory where high risk processing is contemplated.
The ICO advises organisations that they should consider the following questions in order to determine whether or not they need to carry out such an assessment in advance of any particular processing activity:

- will the project involve the collection of new information about individuals?
- will the project compel individuals to provide information about themselves?
- will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition
- will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private
- will the project require you to contact individuals in ways which they may find intrusive?

The following are given as examples of situations in which a PIA might be undertaken:

- the introduction of a new IT system for storing and accessing personal data
- a data sharing initiative where two or more organisations seek to pool or link sets of personal data
- a proposal to identify people in a particular group or demographic and initiate a course of action
- using existing data for a new and unexpected or more intrusive purpose
- a new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding automatic number plate recognition capabilities to existing CCTV)
- a new database which consolidates information held by separate parts of an organisation
- legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring

The ICO states, in its Code of Practice on Anonymisation, that as more potentially ‘matchable’ information becomes publicly available and data linkage and computing power develops in our society, the risk of someone being able to combine information to produce personal data increases. "It is worth stressing that the risk of re-identification through data linkage is essentially unpredictable because it can never be assessed with certainty what data is already available or what data may be released in the future."

### 6.7 USING ANONYMISED DATA

We have seen that for information to be defined as personal data under the DPA, the information must relate to a living individual and that living individual must be identifiable from the information. The need for compliance with the DPA falls away at the point at which the personal data is anonymised and is therefore no longer personal data.

If it is possible to say with absolute certainty that no living individual can be identified from a set of data (i.e. 100% anonymisation), that data will not fall within the definition of personal data under the DPA and does not have to be processed in accordance with the DPA Principles.

However, it is not always possible in every scenario to guarantee 100% anonymisation. Difficulties arise where there is some degree of risk of re-identification from a set of data. If there is information on the Internet for example, which would allow re-identification of a living individual, then the data may fall within the definition of ‘personal data’ under the DPA.

The ICO advises organisations that they should consider the following questions in order to determine whether or not they need to carry out such an assessment in advance of any particular processing activity:

- legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring
- monitoring compliance of the data controller with the DPA
- providing advice in relation to particular processing situations e.g. disclosures to third parties
- providing advice in relation to carrying out PIAs
- dealing with data breaches and liaising with the ICO
- training staff
- drafting policies and privacy notices and other data protection paperwork

**DATA PROTECTION OFFICER**

A Data Protection Officer may carry out tasks including:

- monitoring compliance of the data controller with the DPA
- providing advice in relation to particular processing situations e.g. disclosures to third parties
- providing advice in relation to carrying out PIAs
- dealing with data breaches and liaising with the ICO
- training staff
- drafting policies and privacy notices and other data protection paperwork

57. This is not an exhaustive list — merely a guide.
58. The DPO role will be mandatory under the new General Data Protection Regulation where the processing is carried out by a public body (this will affect ALMOs) or where the landlord is processing sensitive personal data on a large scale. Under the GDPR, the DPO will be required to “report to the highest management level of the controller or processor.” Due to the much increased compliance burdens and more detailed records of processing which data controllers and data processors will need to keep under the GDPR, larger organisations may well find that they need to employ someone full-time in this role.
It is very important, therefore, that where landlords are considering using anonymised data of tenants (for example for research purposes) great care is taken to carry out a thorough risk assessment prior to the implementation of any new project. This risk assessment should involve attempting to ascertain the degree of risk of individuals being re-identified at a later stage.

As part of an initial risk assessment, landlords need to be aware of publicly available data, such as the electoral roll and information which could be easily retrieved from a web search. Could such information be put together with the ‘anonymised’ data to establish an identity? This does not necessarily mean that this would result in an individual being named but, as the ICO has suggested, “it would be enough to establish a reliable connection between particular data and a known individual.”

The ‘Motivated Intruder’ test

In its Anonymisation Code of Practice, the ICO refers to the ‘Motivated Intruder’ as someone who has no prior knowledge but who wishes to attempt to identify an individual from a set of data which has been anonymised. This approach assumes the intruder is:

- reasonably competent
- has access to resources such as the internet, libraries, and all public documents
- would employ investigative techniques such as making enquiries of people who may have additional knowledge of the identity of the data subject or advertising for anyone with information to come forward

The ‘Motivated Intruder’ is not assumed to have any specialist knowledge such as computer hacking skills, or to have access to specialist equipment or to resort to criminality such as burglary, to gain access to data that is kept securely.

How high must the risk of re-identification be before the anonymised data falls within the definition of personal data for the purposes of the DPA?

The ICO has stated that “you must be able to mitigate the risk of identification until it is remote.”

ICO Guidance

The ICO has suggested that the following factors should be taken into consideration when assessing the degree of likely success of the motivated intruder:

- what is the risk of jigsaw attack? i.e. piecing different bits of information together to create a more complete picture of someone?
- does the information have the characteristics needed to facilitate data linkage – e.g. is the same code number used to refer to the same individual in different datasets?
- what other ‘linkable’ information is available publicly or easily?
- what technical measures might be used to achieve re-identification?
- how much weight should be given to individuals’ personal knowledge?

The ICO also suggests that organisations could carry out a ‘penetration test’ in order to assess re-identification vulnerabilities and:

- use the electoral register and local library resources/local council information to try to link anonymised data to someone’s identity
- carry out a web search to discover whether a combination of date of birth and postcode data can be used to reveal a particular individual’s identity
- search the archives of national or local newspaper to see whether it is possible to associate a victim’s name with crime map data
- use social networking to see if it is possible to link anonymised data to a user’s profile

59. A Privacy Impact Assessment should be carried out prior to any new risky processing (the risk being defined in terms of the risk to the privacy of the individuals whose personal data are processed).
The tenancy application form

In this form, tenants typically provide a very wide range of personal data. Some of it will be personal data in the form of name and contact details. Other information may fall into the category of sensitive personal data e.g. information relating to health or disabilities, ethnicity and religion.

It is likely that where non-sensitive personal data is collected and is essential to the granting of the tenancy (such that if it wasn’t provided, the tenancy could not be granted), then the collection of this kind of information could be legitimised on the basis of the ‘contractual necessity’ ground (i.e. tenant consent not needed – and not appropriate as any consent for this type of processing would not be ‘true’ consent).

With regard to sensitive personal data collected from tenants, landlords collect this kind of information for a variety of legitimate reasons including, for example, the need to ensure that they provide accommodation which is suitable for tenants’ needs or to demonstrate compliance with statutory obligations. Where such sensitive personal data is collected in order to comply with a statutory duty, or a legal obligation, the DPA provides a legitimising ground for the collection and processing of this kind of personal data in this context.

Where a landlord needs to collect sensitive personal data from a tenant at the application stage and this information is not needed in order to comply with a statutory duty or legal requirement, the other legal grounds for processing which are available under the DPA will need to be examined.

If, after considering the grounds which are available, the most applicable one is that based upon the tenant’s explicit consent, then that consent should clearly be sought from the tenant. This could be achieved by providing the appropriate ‘privacy statement/consent’ section in the tenancy application form to explain to the tenant why that particular information is needed from them and how it will be used and providing a space for signature by the tenant for the tenant to indicate their explicit consent to this processing.

Landlords also need to consider carefully whether this information does in fact need to be collected from the tenant at all if the only ground upon which the processing can be legitimised is the ‘explicit consent’ ground.

However, it is necessary to point out that even where tenant consent is not actually needed in relation to the collection and further processing of any particular item of sensitive or non-sensitive personal data, it is very important that landlords ensure that they provide the fair processing information which would be given either in a privacy notice or statement with the tenancy application form when the information is first collected from the tenant i.e. it is explained clearly to the tenant why the information is needed and how it will be used.

Collecting personal data from tenants

Wherever landlords collect personal data from tenants for the first time it is important to pay careful attention to the following questions:

1. Are you clear about exactly what items of personal data and sensitive personal data are needed (either now or in the future)?
2. Are you clear about exactly why you need these items of information? You must have a ‘real’ reason for collecting information and for its further use and these should be defined at the outset.
3. Are you likely to want to use the data again for something else? If you know it is highly likely that specific items of tenants’ personal data will be needed later on for a slightly different reason, then include it and explain clearly why it is needed.
4. Are you clear about the legal grounds for the collection and further use of the tenants’ data?
5. Where the ground of ‘consent’ is to be used, have you provided clear details to enable tenants to give informed consent?
6. Have you provided all the required fair processing information in a suitable privacy statement within the form where the information is collected? Does it clearly explain why information is being collected, how it will be further used and with whom it might be shared?
Re-use of tenants’ personal data at a later stage for a purpose other than the granting of the tenancy

We have discussed the importance of a landlord designing the tenancy application form, or any forms on which personal data is initially collected, very carefully with appropriate thought given to whether any of the personal data collected may be needed for other purposes, for example for research, direct marketing, or in the implementation of new products and services for tenants.

Ideally, these additional purposes should be specified clearly in the initial collection form (in the privacy statement section) and specific/explicit consents sought where needed at this point. Where, however, this has not been done and the new purpose is not covered in the initial privacy statement or notice, then this exercise will have to be carried out at the later stage. This will mean notifying tenants of the new purpose(s) and where appropriate to do so, obtaining their consent for example by sending out a new privacy notice/consent form.

If the type of processing contemplated is to be done with the explicit consent of the tenant (this is going to be much more likely where the data required to be used is sensitive personal data) then the privacy notice to be sent to tenants should include a means of collecting consent e.g. the tenant’s signature.

If this ground is used, it is important that the consent provided is ‘true consent’ and that tenants have the facility to withdraw consent for this processing at a later stage, if required.

6.8 LANDLORD CHECKLIST: GETTING IT RIGHT

- Have we put in place a clear policy, with clear guidelines, in relation to data protection and privacy and made it publicly available?
- Have we consulted and involved staff and tenants in developing our policy and guidelines?
- Have we developed, and are we providing, a comprehensive programme of training for staff and our tenant representatives?
- Have we designed our systems and procedures to collect only the minimum necessary personal data needed?
- Are we being as open, honest, fair and transparent as possible to tenants when collecting, using or re-using both personal and sensitive personal data?
- Do we seek specific consent from tenants for the use of their data wherever it is possible and appropriate to do so?
- Are all staff clear that tenants have the power to withdraw such consent and have we made sure tenants understand this?
- Have we arranged to issue tenants with a Privacy Notice each time data is collected, or where we want to use the data in a manner not previously specified?
- Do we monitor and review whether or not the terms and conditions of our Privacy Notice been fulfilled?
- Do we explain clearly to tenants what benefits we hope to gain from processing their data?
- Have we made sure tenants know they have a right to see their data and have we put arrangements in place to ensure tenants can have easy access to their data?
- If personal data is being collected are we using it to identify general trends or to make decisions that affect individuals?
- Have we checked how collecting and analysing this data might affect our tenants? Could there be any ‘unintended consequences’?
- Are we regularly monitoring and reviewing how this data might affect our tenants?
- Are we clear about how long the data will be kept, how it will be securely stored and have we explained this to tenants?
Under the DPA, there is a requirement (under Principle 7) for data controllers to ensure that they have an appropriate level of technical and organisational security to protect any personal data they process against accidental loss, destruction or damage.

The vast majority of data breaches for which enforcement action is taken by the ICO result from a breach of this security principle. Landlords need to ensure that the level of security they have in place is adequate with regard to the type of personal data processed – the more sensitive the personal data, the tighter the security will need to be.

The key risk upon which to focus is that posed to the data subject – for example, is there a risk of individuals having their identities or money stolen or their vulnerabilities exploited? There have been many instances, published on the ICO website and highlighted in the press in recent years, where paper files or unencrypted laptops or other portable media containing very sensitive personal data of vulnerable individuals have been accidentally left in public places. Other examples include contractors (data processors), employed to shred sensitive papers or destroy old IT equipment, dumping paperwork in recycling bins or attempting to sell-on the IT equipment without consent and without removing personal data.

Other breaches of Principle 7 occur where staff inadvertently (or sometimes intentionally) disclose personal data without legal authority or where emails or faxes containing personal data are sent to the wrong email address or fax number by mistake.

**Technical and organisational security**

There are two limbs to Principle 7:

- **technical security** which relates, for example, to the implementation of appropriate security software and the use of encryption (see below)
- **organisational security** which refers to data protection policies and procedures, premises access controls and staff training, for example

Examples: data breaches – the following are all examples of how a breach of the 7th principle (security) could occur:

- A member of staff leaves the office in the evening with files, ready for an early morning visit the next day. He leaves the documentation in his bag in the car whilst he visits the gym. His car is broken into and the bag containing the paperwork is stolen
- A member of staff prints rent statements on the photocopier. The employee is distracted and the papers are left there overnight. There are lots of staff around (whose role does not necessarily require them to have sight of the documentation). The office is cleaned overnight and the papers removed
- A tenant fills in a mutual exchange form and drops it in to the office. They obtain a receipt but the application goes missing
- An email is sent internally with a spreadsheet with income and expenditure details of applicants. A staff member only looks at the first tab and decides it is safe to forward to a resident – it isn’t as the other tabs contain highly sensitive information relating to other residents

The seventh data protection principle requires landlords to take into account organisational (e.g. staff training) as well as technical measures when assessing security.

Questions to consider include:

- to what extent do staff receive regular and on-going training in data protection?
- do they understand how to handle personal data, including sensitive personal data?
- do front-line staff understand tenants’ rights under the DPA (including subject access)?
- is there a data protection policy and are all staff familiar with it?

Landlords may need to consider the provision of separate policies on data retention and deletion, IT and organisational security, and procedures relating to circumstances in which tenants may wish to exercise their rights under the DPA (including subject access).
7.1 KEY SECURITY ISSUES FOR SOCIAL LANDLORDS

The ICO has published a report, *Findings from ICO advisory visits to social housing organisations* (2014), available on its website which sets out some of the most important data protection issues, including security, which social landlords should address. In terms of security, the ICO highlights the importance of the following:

- encryption of portable electronic devices\(^{65}\)
- the development of a homeworking policy for staff, which should amongst other things, stipulate technical controls for the security of personal data used
- secure printing
- end point controls e.g. locking down use of USB ports and DVD/CD drives to reduce the risk of data loss ‘on a massive scale’
- restrictions on systems access – e.g. role based access to tenants’ records, particularly where they contain sensitive personal data
- monitoring – of policies and procedures, including those relating to security
- implementation of secure password requirements, including forcing regular changes
- fax machines – although increasingly less common, they represent a ‘significant risk’ to organisations. The ICO strongly recommends a fax usage policy or, preferably, removal of such machines and replacement with secure electronic transfer solutions
- staff training – viewed as crucially important by the ICO and therefore discussed separately in the next section

The ICO has further information on its website offering guidance and practical tips on IT security, including its guidance entitled, ‘IT Security Top Tips’.

7.2 STAFF TRAINING

The ICO has reported\(^{66}\) “varying levels of data protection training in housing organisations” and that “training is a key tool for any organisation in ensuring that staff are aware of their responsibility for data protection.”

The ICO recommends the following as the most important aspects of good practice for data protection training:

- “mandatory induction training that ideally takes place before allowing staff to access personal data
- mandatory annual refresher training
- annual reviews of data protection training content to ensure that it is up to date and remains relevant to the housing organisation’s needs
- specialised training for key roles, for example those dealing with requests for personal data, information security, or records management
- training records that record completed data protection training, and
- procedures to ensure that incomplete training is chased up and resolved"

In the event of a data breach, the ICO will enquire into the extent of ongoing and role-appropriate staff training and the extent to which the organisation’s data protection policies and procedures have been followed.
7.3 APPOINTMENT OF DATA PROCESSORS

In Chapters 2 and 5 we discussed the need for particular compliance measures where landlords appoint data processors. This is a very important aspect of the 7th security principle as data processors can, very often, form the ‘weak link in the chain’ in terms of the landlord’s security measures.

We have already discussed the requirement, under the DPA, for there to be a contract in writing between a data controller and any data processor employed by the controller.

However, the DPA also states that:67

“where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle:
(a) Choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
(b) Take reasonable steps to ensure compliance with those measures.”

What should the data controller consider when conducting its due diligence in appointing a data processor and what should be included within the contract?

The contract must, as a minimum:

- include wording to the effect that the data processor will act only on the instructions from the data controller, and
- require the data processor to provide a level of security commensurate to that which would be imposed on the landlord by the DPA if the landlord was processing the personal data directly.

The landlord should also consider negotiating the following (non mandatory) clauses in order to ensure that it is able to comply with its obligations under the other principles and thereby meet its DPA obligations to tenants:

- a clause requiring the data processor to co-operate with the landlord where the landlord receives a subject access request from a tenant
- a clause permitting the landlord to audit the data processor’s premises or processes in order to provide assurance with regard to security.

In addition, the landlord should consider protecting itself in the event that there is a breach of the DPA caused by the data processors handling of the landlord’s personal data. A suitable indemnity clause allowing the landlord to recover its losses from the data processor could be included.

7.4 CLOUD PROCESSING AND INTERNATIONAL TRANSFERS OF PERSONAL DATA

Where landlords store personal data of any living individual (tenants or members of staff in HR systems, for example) in the ‘cloud’, the location of the cloud provider’s computer servers will be crucial. The DPA states that transfers of personal data outside the European Economic Area (EEA) are prohibited unless the country of destination provides an adequate level of protection for the rights of data subjects (Principle 8).

Cloud providers usually act as data processors and so a written contract will be required containing the security guarantee and other clauses required for Principle 7 of the DPA, described earlier. It is important that landlords conduct due diligence with regard to organisations providing the cloud service in advance of any data processing and that they enquire into the location of storage of personal data and the security measures in place to protect it in transit and while stored by the cloud provider. If this is outside the EEA, landlords will need to ensure that the cloud provider’s contract also meets the requirements of Principle 8. Legal advice may need to be sought in this regard.

In all cases where a transfer of personal data outside the EEA is anticipated or likely, landlords should ensure that their registration or notification with the ICO is updated, that privacy notices advise individuals that their personal data may be transferred outside the EEA, and that the appropriate level of security is in place to protect such transfers.

7.5 CHECKLIST: SECURITY

Landlords should check:

- Physical security of premises where you process data and where staff work
- Security of your IT systems and systems and audit and monitoring of these
- Whether you only allow staff to access data on a ‘need-to-know’ basis
- Whether your staff have the requisite qualifications and integrity for them to access data, or if they should be carefully supervised or given only limited access
- The frequency and adequacy of data protection training for all of your staff: this should be role-appropriate and is particularly important for ‘front-line’ staff in order to ensure that they understand their responsibilities in handling personal data, including recognising and dealing with subject access requests and appropriate handling of third party requests for disclosure of personal data
- How and where paper and electronic data and media are stored and disposed
- The need for policies aimed at preventing simple frauds, such as clear desks and appropriate telephone call handling
- How securely electronic and paper data are transmitted/moved from place to place e.g. by post, email or file sharing or on electronic media such as USB sticks. The ICO strongly recommends that all portable media containing personal data should be encrypted
DATA LANDLORDS CAN LEGITIMATELY REQUEST FROM TENANTS

The following are examples of personal data that can be held by landlords:

- age
- title
- full name
- other name(s) may be known by
- marital status
- current and previous addresses
- alternative contact address
- landline/mobile phone contact details
- email address
- national insurance number
- nationality
- immigration / residential status
- ethnicity
- religious belief
- gender identification
- sexual orientation
- disability details – nature of disability, disabled access requirements
- aids and adaptations requirements
- medical information – physical and mental health
- vulnerabilities – e.g. sight, hearing impairments, drug/alcohol dependency issues
- employment status
- housing history
- household type
- economic status
- income details – wages and/or benefits
- financial commitments (expenditure and debts)
- bank details
- allowances, benefits and grants
- details of support being received or required from external agencies (name of support worker, name of external agency)
- unspent criminal convictions
- third-party authority and information (name, address, date of birth, contact details, nature of relationship to tenant)

Landlords can also collect personal data in the form of certain opinions and intentions, such as:

- staff case notes on tenants, including support worker diaries
- staff opinions on tenants in neighbour nuisance cases and their intentions on how to deal with tenants in such cases

In addition, landlords might hold social service department case notes or information supplied by the DWP in relation to universal credit entitlement.

Summary of personal data that may be collected by landlords directly from third parties

A landlord may obtain information about the tenant(s) from a third party, which may include information from social services, mental health agencies, benefit services such as the local council’s housing benefit service, the job centre or DWP, money advice agencies, GP, hospital, support worker and/or external support services.

Information obtained may include:

- details of medical conditions, both physical and psychiatric
- details of medication and/or treatment
- hospital number
- name
- address
- national insurance number
- DWP reference number (universal credit)
- housing benefit claim number
- income details of tenant and family members (this information can be included on housing benefit entitlement notification letters or benefit letters)
- benefit entitlement information – this may include confirmation of the amount of benefit entitlement, the periods the benefit relates to, any backdated payment of benefits and periods it relates to.

Details of child protection, care or residency arrangements

Details of tenant(s)/household members’ vulnerabilities

Types of forms used by landlords

- housing application form
- pre-tenancy assessment form
- housing interview form
- sign-up form
- equality and diversity monitoring form
- income and expenditure / financial assessment form

Types of documents obtained by landlords

- proof of benefit letter (job seekers’ allowance, employment support allowance, disability living allowance now in some instances referred to as personal independent payments)
- proof of income (wage slips, P60, child tax credit notifications)
- bank statement – for the purposes of proof of income for housing benefit claim or calculation
- ID and proof of residence documents for tenant and family members (passport, driving licence, visa, immigration documents)
- housing benefit entitlement notification letters
- letters from DWP notifying of universal credit application or entitlement
- letters from DWP notifying of changes to income (money advice purposes)
- council tax notifications – ID, money advice purposes or income and expenditure to consider rent arrears payment arrangement
- ID and proof of residence documents for tenant and family members (passport, driving licence, visa, immigration documents)
- housing benefit entitlement notification letters
- letters to tenant(s) about a spouse, partner, children, and/or relatives that will be residing with the tenant at the property or may come to reside with the tenant at some stage during the tenancy:
  - title
  - full name
  - date of birth / age
  - relationship to the tenant
  - medical difficulties
  - disability details
  - vulnerabilities
  - income details (employment income and/or benefit income) – this may be obtained for the purposes of completing housing benefit entitlement calculations and/or proof to be sent to the benefit services to process a housing benefit claim.
  - bank statement – for the purposes of proof of income for housing benefit claim or calculation

Other information

This is information a landlord may obtain from the tenant(s) about a spouse, partner, children, and/or relatives that will be residing with the tenant at the property or may come to reside with the tenant at some stage during the tenancy:

- title
- full name
- date of birth / age
- relationship to the tenant
- medical difficulties
- disability details
- vulnerabilities
- income details (employment income and/or benefit income) – this may be obtained for the purposes of completing housing benefit entitlement calculations and/or proof to be sent to the benefit services to process a housing benefit claim.
- bank statement – for the purposes of proof of income for housing benefit claim or calculation.