LEWIS SILKIN

Data Protection

Inside

Why is data protection important?

Personal information collected by organisations in the housing sector, especially by Registered Providers (RPs), is often extremely sensitive. Therefore, the sector must be particularly scrupulous when it comes to data handling.

Alerted by the findings of its visits to RPs, the UK's data protection watchdog, the Information Commissioner's Office (ICO) has repeatedly warned the housing sector of its powers to fine and punish organisations that breach data protection rules.

Serious breaches of the data protection laws can see organisations facing a fine of up to £500,000 – and potentially, in future, a fine of up to 5% of turnover, if proposed new EU laws get the go-ahead.

If your organisation doesn't understand and follow the data protection rules, you could be at risk, not only in monetary terms, but also in terms of reputation.

What is 'personal data'?

Data protection laws are designed to strike a balance between safeguarding peoples' privacy and allowing organisations to collect, keep and use data for the purposes of running their businesses.

The current law is set out in the Data Protection Act 1998 (DPA 1998).

The DPA 1998 includes all the key definitions of technical terms that you and your staff will need to know in order to keep to the rules on sharing, securing and processing information relating to tenants and homebuyers, employees and contractors, or suppliers and contacts (who are all potential "data subjects" under the DPA 1998, i.e. individuals identified by the data).

The DPA 1998 applies whenever a data controller processes personal data. But what do these technical terms actually mean? "Data" means information processed and held on a computer or recorded on paper in a structured filing system. "Personal data" means data relating to a living individual (including expressions of opinion), who can be identified from those data or from those data together with other information in your organisation's possession.

Tighter rules apply to so-called "sensitive personal data". This means data about a person's ethnic background, political opinions, religious beliefs, health or criminal records. The law expects organisations to treat this type of personal data with greater care, as it is likely to be more private and could be used to discriminate against people.

The demands and duties relating to "sensitive personal data" are especially relevant to RPs, considering that they often process delicate information about their tenants, including their background, disabilities, ages and vulnerability.

Who is responsible?

So, who is responsible for observing the obligations and duties set out in that Act? The DPA 1998 places those duties on those organisations who decide how and why such personal data is processed.

Those organisations are known as "data controllers" and will include RPs, ALMOs, or developers. It's the data controllers' responsibility to comply with the DPA 1998 and failure to do so could see them face enforcement action, prosecution or a compensation claim.

In contrast, "data processors", (those who process data on behalf of the data controller) are not directly subject to the rules. For example, when a developer uses another company to carry out a survey of its recent home buying customers, on its behalf, and the survey company has access to the developer's customer records. The survey company in this case is the data processor. The developer will remain responsible for ensuring the survey company's processing complies with the data protection rules. They will therefore need to put in place an appropriate written contract with the data processor.

What are the data protection principles?

The DPA 1998 is constructed around a structure of eight relatively straightforward data protection principles that all organisations dealing with data must follow.

In summary, personal data must:

1. Be processed fairly and lawfully;
2. Be obtained only for specified and lawful purposes;
3. Be adequate, relevant and not excessive;

4. Be accurate and kept up to date;
5. Not be kept for longer than is necessary;
6. Be processed in accordance with the rights of data subjects under the DPA 1998;
7. Be kept secure (specifically, appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data); and
8. Not be transferred outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data subjects.

What do the data protection law say about security?

The 7th principle requires organisations to manage the security of the personal data in their possession.

This means that RPs and developers should ensure that only authorised people can access, alter, disclose or destroy personal data. In practice, this could mean having a staffed foyer/reception area; dedicating zones or areas to meet confidentially with tenants or prospective homebuyers; or deploying swipe card access to records and server rooms. As well as adopting physical security measures, registered providers and developers should look at restricting access to tenant and customer records according to staff roles.

In addition, data controllers need to ensure they have appropriate policies in place for dealing with data breaches – for when it's gone wrong – and all staff are trained to know what to do in such situations.

How can data be shared with other organisations?

RPs often share personal data with other organisations which then use the personal data for their own reasons (and become data controllers too). For example, personal data will be shared when sending a tenant's details to a government agency.

Before deciding to share any personal data with other organisations, you should identify what you are attempting to achieve and consider the potential benefits and risks of sharing the personal data. Think carefully about whether you can just share specific data rather than an entire record, or if you can achieve the same aim through the anonymisation of the data.

All RPs should put in place data sharing agreements with those organisations with which they regularly share personal data.

The ICO has issued guidance in the Data Sharing Code of Practice covering: when personal data can be shared; the security measures that need to be in place; and state who in each organisation is allowed to approve data sharing. You should also look to spell out procedures for handling data subject access requests.

What are data subject access requests?

Data subjects have a number the rights under the DPA of which probably the most important is the right to request access to personal data held about you. This right is commonly known as a data subject access request or 'SAR'. Any person can exercise this right simply by making a written request. Organisations may require payment of a fee for dealing with the request, up to a maximum of £10.

A SAR is most often used by tenants to who want to see the information a RP holds about them. If a RP receives such a request from a tenant, the registered RP must respond promptly and in any event within 40 days of receiving the request.

Dealing with such requests may be a challenge, especially if there is large amount of personal data or if the personal data is held in a way that makes it difficult to locate, access and extract. However you should put in place suitable procedures to help identify the relevant personal data.

If you only remember five things, remember these five things...

1. Serious breaches of the data protection laws can see organisations face a fine of up to £500,000.
2. "Personal data" means information (including

expressions of opinion) relating to a living individual who can be identified from those data or from those data together with other information in your organisation's possession.

3. Tighter rules apply to so-called "sensitive personal data".
4. Data controllers need to have contracts in place with their data processors, and when they share personal data with other data controllers.
5. "Data subjects" have the right to access their personal data.(e.g. own it) – even if only temporarily.

Funny fact

In 2011, Vince Cable, the business secretary, was forced to apologise for dumping confidential documents in bins outside his constituency office. The Daily Telegraph reported at the time, that unshredded paperwork, including letters from ministers and containing personal details of constituents, were found discarded outside Mr Cable's HQ. Mr Cable admitted it was an "unacceptable breach of privacy" and said the ICO had been notified.

…little bits of law

This is one in a series of leaflets published by Lewis Silkin LLP, providing information on a range of legal issues that face our developer clients. Other topics discussed range from boundaries to wildlife.

Professional advice should be obtained before applying the information in this client guide to particular circumstances.

For a full list of available leaflets please visit our website or contact patrick.brown@lewissilkin.com.

For more information please contact:

Patrick Brown at
patrick.brown@lewissilkin.com or

Patrick Brown
patrick.brown@
lewissilkin.com

Simon Morrissey
simon.morrissey@
lewissilkin.com

Classified
classified@
lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | F +44 (0)20 7864 1200
www.lewissilkin.com