Findings from ICO advisory visits to residential sales and lettings organisations

January 2016

Version 1.0, 28 January 2016

Executive summary

The Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the Data Protection Act 1998 (DPA) and for promoting good practice in information handling. The DPA consists of eight principles with which all organisations processing personal data must comply.

During 2014/15, we visited a number of residential sales and lettings organisations across the UK to understand the information risks and challenges that they are facing. We also conducted an online survey in conjunction with the National Association of Estate Agents (NAEA) and Association of Residential Letting Agents (ARLA) and completed by numerous residential sales and lettings organisations.

Our analysis identified common themes and challenges faced by residential sales and lettings organisations in complying with the DPA.

Summary of findings

- There was little in the way of formal policies and procedures in place for data protection in the organisations visited.
- There was little if any formal training for data protection.
- There was a lack of awareness whether written contracts were in place containing information security clauses.
- There was a lack of awareness about the importance of using technical security controls such as encryption to protect personal data if devices are lost or stolen.
- The use of generic accounts to gain access to IT systems is widespread.
- Where system access was password protected these were seldom complex. Passwords were also not changed regularly.
- There was a lack of security in place for manual records containing personal data.

- Where CCTV was used, the organisations were not displaying adequate notices to inform individuals that CCTV is in operation on the premises and had rarely included this purpose in their registration.

- Adequate information for individuals about how the organisations were going to process their personal data was not always supplied.

- Personal information was kept for longer than necessary as retention schedules were seldom in place.

Recommendations

Policies and procedures

Finding

Only one organisation we visited had a data protection policy in place. None of the agencies who permitted staff to work from home had a home or remote working policy outlining staff responsibilities towards personal data in these circumstances, and no guidance for staff on how paper documents and mobile devices should be stored off site or secured during transit.

The survey results showed a different picture with 71% of respondents reporting that they did have written policies in place detailing how client/customer information is secured and managed.

Recommendation

It is essential to have written data protection policies and procedures in place to ensure compliance and promote good information handling. Organisations should:

- ensure policies consider the additional security risks associated with home / remote working where applicable, as well as staff working within the office environment;

- ensure policies are approved by a director or senior manager, have a clearly identified owner and version number;

- store policies on the organisation's intranet or a shared network drive and communicate to all staff; and

- review policies on a periodic basis and update when necessary.

Data protection training

Finding

Most of the organisations visited and 35% of survey respondents did not provide data protection, confidentiality or information security training for their staff. Of the two organisations visited who did provide training, only one refreshed this on an annual basis.

Recommendation

Training is a key tool for ensuring staff awareness of data protection obligations, confidentiality and the security of personal data. Good practice in training should include:

- data protection training as part of the induction process for all staff;
- annual data protection refresher training for staff who have access to personal data; and
- maintaining a record of training completed and reminding staff when their training is due.

Third party contractors

Finding

Services such as IT support, archiving IT hardware and confidential waste were carried out by third party contractors in a number of organisations visited. 57% of survey respondents did not have contracts in place with contractors and although in most organisations visited written contracts were in place with third parties it was unclear whether the contracts contained appropriate information security clauses.

Recommendation

To improve compliance with the DPA organisations must have a contract in place with any third party who processes or has access to personal data on their behalf. Organisations should:

- be satisfied third parties provide sufficient guarantees about security measures implemented to protect any personal data it is processing for you;
- take reasonable steps to check that those security measures are being put into practice;
- have a written contract setting out what the third party is allowed to do with the personal data including security measures outlined above; and
- where applicable ensure certificates of destruction are received from reputable third parties detailing safe destruction of confidential waste and IT equipment.

Technical security controls including encryption and endpoint control

Finding

In general there was a lack of awareness about the use of technical security controls to protect networks, computers and mobile devices such as encryption, anti-virus, anti-malware and firewalls. For instance many organisations were unaware of the risks associated with using unencrypted devices such as laptops, USB memory sticks and portable hard drives. The majority of the organisations visited had not disabled USB ports and DVD/CD drives which poses a significant risk to the security of personal data.

Survey responses reflected this finding with only 12% of organisations having controls in place to prevent portable media being connected to their computers. 78% reported using unencrypted devices or didn't know whether they were encrypted.

Recommendation

Organisations should:

- ensure appropriate anti-virus, anti-malware, and firewalls are installed on their systems and portable devices all of which should be automatically updated on a regular basis;
- use approved encryption software to ensure the information remains protected in the event of a device being lost or stolen;

- lock down ports and drives to limit the risk of unauthorised removal of personal data and the introduction of malware and viruses to the network;
- provide staff with encrypted memory sticks where there is a business need and allow a designated open USB port to be used only in such circumstances where authorisation from a manager or designated member of staff has been obtained; and
- keep a log of all portable media devices and the names of the individual owners.

System access and password requirements

Finding

Only half of the organisations visited and those responding to the survey had controls in place to limit access to personal data according to job role. 'Needs-based access' should restrict staff's access to electronic data held on systems, and in some cases manual data, to only those who require it to perform their role. It was not clear in all cases whether system access was amended when employees changed role and revoked promptly when they left the organisation.

94% of survey respondents and the majority of organisations visited provided their staff with individual accounts and passwords to access the network and systems containing personal data. However in most cases controls were weak regarding password complexity with 53% not requiring complex passwords to be used and the frequency with which they were required to change, as 45% never change their network passwords and 55% never change their passwords for databases and applications.

Recommendation

In order to reduce the risk that personal data may be accessed inappropriately, organisations processing personal data electronically on systems should:

- have controls in place to restrict access to systems;
- review access on a regular basis and update when staff change roles within the organisation; and

- ensure system access procedures include prompt removal of access for all leavers and in cases where staff are suspended or away from the office for a prolonged period of time such as long term sickness or maternity leave.

Passwords provide a way in which organisations can restrict access to their systems. However, when password controls are not robust, organisations are at risk of unauthorised access to information, system intrusion and they are less likely to have a record of who has accessed or amended data and when this may have happened. Organisations should implement password controls including:

- outline password rules in a written policy and ensure all staff are aware of their responsibilities;
- issue all staff with unique usernames and passwords for the network and systems containing personal data;
- do not keep a list of employee passwords;
- do not allow users to share passwords with their colleagues;
- enforce changing temporary passwords when users log on for the first time;
- create rules regarding the complexity of passwords such as at least eight characters long including a combination of upper and lower case numbers, letters and symbol characters; and
- prompt regular password changes at least every 90 days and restrict the number of failed logon attempts before a user's account is locked and needs re-setting.

Storage of manual records and locked screens

Finding

A large proportion of organisations visited and 25% of survey respondents did not have adequate security in place for manual records containing personal data. In some cases files containing personal data were stored on desks, in trays, on open shelving or in unlocked cabinets overnight. This was due to a combination of lack of secure storage cabinets, failure to lock these cabinets or lack of secure storage for the keys to those cabinets.

Those organisations where staff were encouraged to clear any personal data from their desks when not occupied, did not have this requirement documented in a policy and did not conduct regular checks to monitor compliance.

Screens were also observed to be left unlocked whilst staff were away from their desks.

Recommendation

The open layout of many agents' offices means that there is a high risk that anyone who enters the premises could view or even remove personal data left on desks or visible on unlocked screens. Therefore organisations should:

- ensure security controls in relation to the storage of manual records such as securing personal data in lockable filing cabinets when not in use and at the end of the day are implemented, enforced included in the data protection or equivalent policy;
- introduce mandatory clear desk and locked screen procedures using 'Ctrl-alt-delete', formalise in policy and take steps to ensure they are being adhered to by staff.

Fair processing, including CCTV

Finding

Half of the organisations visited and 91% of survey respondents did not have a fair processing notice on their website to provide clients and customers with information explaining how their personal data may be used or disclosed.

Some organisations provided such information verbally and in writing on application forms and agreements. This wasn't happening in all cases with 33% of respondents reporting that they did not provide customers with information regarding how their organisation will use and secure their data, and 31% not providing their customers with any information explaining how their data will be shared with third parties.

Where organisations used CCTV cameras for security purposes, fair processing notices were not always used or fit for purpose and in some cases organisations had not informed the ICO about this purpose for processing personal data during the notification process.

Recommendation

Organisations who process individual's personal data should:

- create an appropriately detailed fair processing notice outlining how they may use or share a customer or client's information, including the circumstances in which this may occur;
- share the notice with clients and customers in writing, before obtaining their personal data;
- make the notice available in a reasonably prominent place on their website;
- obtain consent prior to sharing personal data with any third parties unless a valid exemption applies;
- ensure customers and staff are made aware if CCTV recording is used on the premises by use of appropriately-sized notices containing contact details and explained to staff in a policy;
- ensure the retention period for CCTV data is documented in a written schedule; and
- ensure CCTV recording is reflected in the company's notification details to the ICO. This can be done by calling the Registration helpline on 0303 123 1113 or by emailing the Registration team at Registration@ico.org.uk.

Retention of personal data

Finding

The majority of the organisations did not have a written retention schedule covering all manual and electronic records including emails.

Survey results showed 39% of businesses were keeping electronic information relating to residential lettings indefinitely while the figure for residential sales was 25%. Although a significant number of respondents reported disposing of paper records relating to sales and lettings, still 10% were keeping this information indefinitely.

Recommendation

Organisations should review the personal data they hold and identify how long it needs to be retained for based on why it was obtained. Agreed

timeframes for each category of data should be documented in a retention schedule to help safeguard against holding the personal data indefinitely which would be a breach of the Act.

When creating a retention schedule, organisations should consider the following:

- identify all categories/ types of personal data held by the organisation;
- any additional legal and statutory requirements;
- standard industry practice;
- whether the whole record needs to be retained to meet a business requirement or just a specific section of it;
- identifying secure appropriate disposal methods for both electronic and manual data;
- who will be responsible for periodic weeding and destruction of records and how compliance of this is to be monitored.

Further actions

The ICO has produced a range of guidance for organisations to use to better manage and secure their personal information. The information can be found on our website ico.org.uk, with particular small business guidance at ico.org.uk/business.

Other useful ICO guidance:

- Data protection guidance
- A practical guide to IT security
- Employment code of practice – quick guide
- CCTV code of practice
- Privacy notices code of practice
- Encryption guidance

Useful guidance produced by other organisations:

- Getsafeonline

Advice and assistance

The ICO's helpline can answer queries about data protection compliance and can be contacted on 0303 123 1113.

The ICO also has offices in Scotland, Wales and Northern Ireland which can answer questions specific to those legislation and regulations in those areas.

The Scottish office can be contacted on 0131 244 9001.

The Welsh office can be contacted on 029 2067 8400.

The Northern Irish office can be contacted on 028 9027 8757 or 0303 123 1114.

Appendix 1 – Background

The Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the Act and has a remit for promoting good practice in information handling. The Act consists of eight principles of good information handling that all organisations processing personal data have to comply with.

In 2014/15 we undertook 10 advisory visits at residential estate and letting agents in England, Scotland and Wales and conducted an online survey with 51 respondents in conjunction with the National Association of Estate Agents (NAEA) and Association of Residential Letting Agents (ARLA). The objective was to gain a better understanding of the data handling practices, information risks and challenges facing organisations in this sector and the circumstances they operate in.

Whilst this only constitutes a tiny fraction of the number of residential estate and letting agents in the UK there were a number of common themes and challenges faced in managing information.

Advisory visits are a one day informal visit to look at how an organisation handles personal information where we provide practical advice and guidance on site and a short report after the visit. The visits typically cover information security, records management and requests for information.

Find out more about our advisory visits and read summaries of advisory visits we've carried out.

As of June 2015, the number of people working in the real estate sector in the UK stands at 547,000, with 2000 leaving the industry over the last year according to the Office for National Statistics.

Appendix 2 – Typical processing of personal data by residential sales and lettings agents.

Around half of the organisations visited and those who responded to the survey cover both residential sales and lettings, with the remaining covering either sales or lettings. Organisations operating within this sector do not tend to process sensitive personal data.

The information processed is in both paper and electronic form with a significant amount of electronic data stored on externally hosted customer relationship management (CRM) databases. Estate and letting agent specific software facilitates the management of property marketing, preparing property particulars and viewings along with storing information relating to the requirements of customers and clients.

In the main these businesses hold a mixture of electronic and manual records relating to vendors (property sellers) and property buyers for residential sales agents, landlords, as well as tenants' information for residential letting agents and employee information. The details held include names, contact details including home, email addresses and telephone numbers, bank details, tenant references, proof of identification such as passports, driving licences and utility bills, credit check documentation and standard employee data, including medical information where relevant.