A matter of record

Thousands of agents are not complying with the Data Protection Act 1998, risking fines of up to £500,000. Lawyer Stephanie Pritchett advises

Estate agents and letting agents are among organisations which, because they process personal information electronically, have a statutory duty to notify the Information Commissioner's Office. Yet the duty, under the Data Protection Act 1998, is being largely ignored by agents, and the ICO has launched a campaign to get them to comply. It did so after noticing that just 3,734 estate agents and 1,416 letting agents were registered with it.

Should you care? Well, on April 6, new penalties of up to £500,000 were brought into force for serious contraventions of the Act. These include data security breaches, which are dangerously widespread.

Sales and letting agents are particularly at risk. Self-evidently, any business which holds or processes customers' details is potentially at risk of data protection breaches. The particular area of concern for property agents is the ability to cause 'serious harm and distress' with its data protection breaches.

By way of example, agents will keep files on prospective tenants or purchasers, with details of the properties they are seeking and many other details, including financial or budgetary constraints. It is all too easy to add notes to a file which could unfairly affect that customer's ability to buy or rent a home, such as 'indecisive' or 'punching above their weight'.

A comment could find its way on to someone's file that suggests the purchaser is in a stronger financial position than they actually are. In such cases, a simple file note could mean the purchaser ends up paying more than they needed to for a property as a result of that inaccurate information.

Many agents are probably not routinely informing their customers that they have a right to have a copy of their personal information and to correct it where it is inaccurate, and this could easily lead to breaches of data protection law leading to serious harm or distress. This is dangerous territory.

Beware, too, of disgruntled employees who are moving on to a rival estate agent taking your data with them. There are agents who know, to their cost, that this does happen. Data protection and data security breaches are mainstream news. At times, it can be hard to pick up a newspaper without a headline about sensitive information left in skips or missing laptops and memory sticks containing data about thousands of customers.

The recession has also meant greater temptation for businesses to cut corners and a greater desire to exploit databases and information assets. Put this together with compliance cuts, and there is a recipe for unmanageable and dangerous business risks.

Stephanie Pritchett is a lawyer practising in data protection, freedom of information and privacy law as well as information management

It's personal!

On average, according to research, each UK citizen has personal information on them stored on over 700 different databases by different organisations.

Information about an individual (including name, address, date of birth, credit card details, expiry date and sort code) can be sold on the information black market for just £1. A database with details about 100,000 individuals can therefore be worth £100,000.

Slick Willie Sutton, the prolific US bank robber, famously said he robbed banks "because that's where the money is". Are databases the new banks?

It is also worth bearing in mind the theory of Moore's Law, which postulates that computers get twice as fast every two years. It has, therefore, never been easier for organisations to store, use, lose and misuse personal data they hold.

Many agents are probably aware of instances where customers' details are passed on, without the their consent, to mortgage brokers, insurance companies or solicitors during or after a transaction as a way of earning an extra commission or payment. A few alarm bells should be ringing because this should absolutely not be happening.

Big fines

In order to impose a fine, the Information Commissioner (who is the UK

regulator of the Act) must be satisfied:

- That there has been a serious breach of the Act;
- That this contravention would be likely to cause serious harm or distress; and
- That the contravention was either deliberate, or that the agent should have known about the risk of the breach and failed to take reasonable steps to prevent it.

Selling on or passing on customers' details for marketing purposes may well be viewed as a deliberate breach, and would be likely to attract unwelcome interest from the Information Commissioner.

It is important to remember, however, that fines can be imposed where breach of the Act (such as a loss of customer data) was accidental, but where the agent failed to take reasonable steps to prevent this accidental breach.

For instance, failing to:

- encrypt laptops or memory sticks which were then lost or stolen; or to
- properly protect (or limit access to) customer details, which are then passed or sold to a competitor by a disgruntled employee,

would be failures which could result in enforcement action if they were shown to lead to a data protection breach.

Justice Minister in the last Labour Government, Jack Straw, said of the new penalties: "They will ensure the Information Commissioner is able to impose robust sanctions on those who commit serious contraventions of the data protection principles.Most data controllers do comply with the principles, but since misuse of even small amounts of personal data can have very serious consequences, it is vital that we do all we can to prevent non-compliance. Penalties of up to £500,000 will act as a strong deterrent."

The Information Commissioner has previously been criticised as toothless. However, the current UK commissioner, Christopher Graham, was appointed a year ago and has a determined mindset. He also has increased powers to fine and to spot-check public sector bodies, with similar 'dawn raid' powers for private sector bodies likely to follow. Personal criminal liability for directors and increased funding mean that enforcement is set to increase.

Data protection law, one of the most expensive for organisations to comply with, is here to stay. Those teeth are sharpening. Don't let your agency business fall foul of this legislation.

As Christopher Graham says: "No organisation can neglect to protect people's privacy. Not only is it the law, but there is also a hard-headed business imperative." ■

DATA PROTECTION – A QUICK GUIDE

The Data Protection Act applies to all businesses that use personal information, with very few exemptions. It also gives individuals certain rights, including the right to see the information that is held about them. For example, a candidate who has failed a job interview might want to see the notes that were taken. By law, you will need to notify the Information Commissioner you are processing information. Failure to notify is a criminal offence. You will have to pay for this notification – the fee will be £35. For large organisations, it will be £500 if you have more than 250 staff and a turnover of more than £25.9m.

Compliance means data must be lawfully processed, and for limited purposes; it must be adequate, relevant and not excessive; it must be accurate; not kept longer than necessary; processed in accordance with the individual's rights; and not transferred to other countries without adequate protection.

You stand to be prosecuted and fined if you use or disclose information about other people without their consent. The only real exception is the police, who can ask to see records.

The Act covers computer records and some manual records. Most computer records should be disclosed on request, with any third party information removed. Manual records need to be properly filed so that information can be easily found.

You and your staff should take special care when using email or the internet. Take particular care with data about ethnicity, disabilities, sex life, trade union membership, religion, etc. General good guidelines to observe are: do not leave people's information lying around on desks unless it is actually being used; keep filing cabinets locked; do not leave data displayed on screen; do not leave computers logged on if they are unattended; never send an email that you would not put on the back of a postcard; encrypt computers, including laptops and portable devices.

There are some companies offering to register your business and carry out notifications for you. They usually want about £95. You do not need to use them and it may not be wise.

TOP DATA PROTECTION COMPLIANCE TIPS

- Review your agency's compliance in light of the increased risks of a £500,000 penalty for a breach of the Act.
- Ensure data protection moves up the corporate compliance agenda. It must be taken seriously at a senior level in your agency.
- A health check of your data protection policies and procedures should include: your website; client-facing privacy policies; data collection forms; internal data protection policies; monitoring; communications; data retention and destruction policies; and any outsourcing procedures.
- Review your Information Commissioners Office notification to ensure it is accurate and up to date. Many people rely on ICO templates and renew their annual notification without making changes. However, failure to notify new data processing activities within 28 days is a criminal offence.
- Have a robust subject access request procedure in place: failure to fully comply with requests for information from individuals is the top reason for complaints to the ICO.
- Ensure marketing team practices are compliant with the Act and the Privacy Regulations, via appropriate use of customer databases, opt-ins, opt-outs, unsubscribe requests etc.
- Ensure all arrangements with third parties who process data on your behalf (e.g. mailhouses and marketing companies) are in writing and contain the legally required data protection clauses. (Stephanie Pritchett's firm, Pritchetts, have free sample clauses, worth £500, available to readers: www.pritchettslaw.com for more details.)
- Have a data security and security breach policy in place.
- If you use security cameras or other devices, ensure CCTV policies are legally compliant.
- Carry out staff data protection awareness training and stay abreast of legal developments in this area. Pritchetts produces free newsletters, which you can sign up to on the website.