Andrew Dyson discusses the issues of patient data protection and security under the terms of the Data Protection Act 1988

Protect and survive

When HM Revenue and Customs admitted to losing discs containing details of 25 million child benefit claimants, there was a public outcry. In the wrong hands, the records would provide sophisticated criminals with a valuable tool to steal the identity of millions of innocent victims – to open bank accounts, get credit cards, loans, state benefits and generate passports and driving licences.

In an age where face-to-face transactions are no longer the norm and paper records increasingly obsolete, maintaining confidence in the way personal information is handled is essential best practice in business. Organisations cannot and must not take good security for granted – the stakes are simply too high for getting it wrong. HMRC found this out to its cost.

Within hours of the announcement that it had lost child benefit discs there was a massive public outcry, the chairman resigned, questions were being asked in Parliament and the Information Commissioner's Office (ICO) commenced formal investigations under the Data Protection Act 1998.

Here we explore the importance of managing personal information properly, outline the legal responsibilities organisations have to protect personal information, the consequences of failing to comply with those responsibilities and practical steps to avoid some of the most damaging pitfalls.

Taking care of personal data

The well-publicised problems suffered by HMRC highlight the risks of failing to properly protect personal information. Sadly, the case is not unique.

Earlier in the year, Nationwide Building Society was fined a record £1m for failing to take proper steps when a laptop containing 11 million customer records was stolen from an employee's car and a further 11 banks and building societies were 'named and shamed' for the reckless way in which they discarded customer records on the high street.

These incidents damage confidence, erode hard-won reputations and ultimately lose businesses money. High-profile security blunders in the US and continental Europe have seen companies lose millions of dollars off stock market values and massive payouts to blighted consumers and vexed regulators. UK companies who fail to protect privacy face similar risk and should be prepared to manage the adverse consequences.

Complying with the DPA

Taking proper care of personal information is not just sound commercial practice, it is a legal requirement.

Any organisation responsible for the collection and use of personal information must comply with the Data Protection Act 1998.

The DPA establishes a legal framework which 'data controllers' must follow when 'processing' personal information.

All data controllers have a duty to keep personal information within their control secure against unauthorised or unlawful use. This is a specific requirement within the DPA and requires organisations to ensure:

- Personal information is held within secure IT systems
- Appropriate physical and technical controls are in place to limit access to personal information held within the organisation on a 'need to know' basis
- Personnel who have access to personal information are subject to appropriate security vetting and confidentiality agreements
- Everyone within the organisation is aware of their role in managing information security
- Policies and procedures are in place to manage security risk and effectively deal with any breaches
- Penetration tests and audits are regularly conducted to validate and enhance these procedures
- Where personal information is provided to a third party, a security risk assessment is carried out on that organisation before any personal information is handed over and the basis on which the information will be used is clearly delineated in a 'data processor' contract.

Information security is only one aspect of the legal responsibilities set out in the DPA. The legislation also sets out broad responsibilities to manage personal information in a fair and lawful manner. Compliance with these additional requirements means:

- Formally notifying the ICO about the types of personal information

collected and used by the organisation. This notification is published in a public register of 'data controllers'

- Issuing 'privacy policies' to staff, customers and the like which explain in clear English the personal information held by the organisation and how this is used
- Only using personal information for purposes which are 'fair' in all the circumstances, having regard for the individual's expectation of privacy. It will generally only be fair to use personal information:
  - Where necessary to fulfil a legitimate business activity which does not harm the individual (for example, where necessary to fulfil a specific transaction with the individual)
  - Where necessary to comply with a specific legal responsibility, or
  - Where the individual has specifically authorised their information to be used in a particular way
- Ensuring the purpose for which information is to be used is as clearly explained to the individual in the relevant privacy policy and justifiable on one of the above mentioned grounds. It is often tempting to use information collected for one purpose at one time, for something else later on, or to pass it on to a third party. This may not be possible – so always confirm what is permissible before authorising such activity
- Limiting the amount of personal information used to fulfil a particular activity, to the data actually necessary to complete that task
- Taking care to update records which become out of date or obsolete
- Allowing individuals the right to access a copy of the personal information on demand
- Allowing individuals the right to 'opt out' from any direct marketing activity
- Not transferring any personal information outside the European Economic Area without securing additional protections.

Enforcement under the DPA

The ICO regulates compliance with the DPA. It is required to investigate and rule on complaints received from members of the public on alleged breaches of the legislation. It wields significant power to carry out formal inquiries and enforcement action.

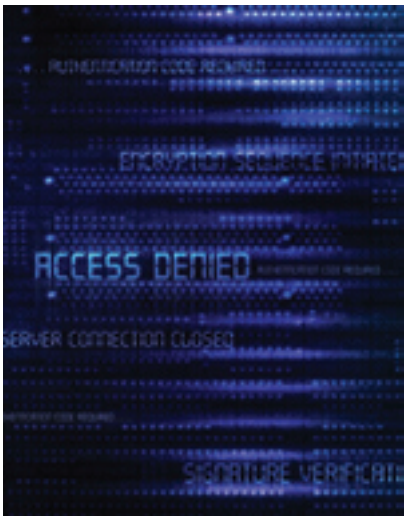
Organisations who find themselves under investigation from the ICO are likely to be exposed to adverse publicity once those investigations are complete – the ICO has a deliberate policy of raising awareness of data protection through publicising poor working practices.

If systemic failures are identified, there is the additional risk of a fine of up to £5,000 in a Magistrates Court or an unlimited fine in a Crown Court. Further, if individual members of staff are found to be involved in making unauthorised disclosures of personal information they personally face the prospect of a custodial sentence.

Steps to take to ensure compliance

Establishing a clear regime of information governance will ensure compliance with the rules and limit the risk of things going wrong. As a basic checkpoint, make sure these simple processes are in place:

- Have a clear understanding about the personal information collected and used within the practice
- Ensure the way in which personal information is used remains consistent with the expectation of the individuals concerned – be satisfied that staff or customers would not be surprised to learn about the way in which their private details are used
- Have a data retention policy which ensures records are regularly updated and deleted when obsolete
- Have a security policy which sets out a clear process for maintaining the integrity of data, prevents unauthorised access to information and has effective procedures for managing breaches
- Ensure IT infrastructure supports effective security controls and data management
- Carry out regular data protection compliance audits
- Nominate a senior officer with overall responsibility for management of data protection and security compliance.



What to do if things go wrong

If an information security breach occurs, the temptation may be to keep quiet and hope the problem passes by unnoticed. This is usually a recipe for more trouble. The ICO is quite clear that if things go wrong there is an overriding duty to protect the individuals' concerned as quickly and effectively as possible.

At a minimum, this is likely to mean issuing a clear communication to those affected, explaining what has happened; explaining any risks that they may be exposed to as a result of the problem – for example, any enhanced risk of identity theft and steps they can take to minimise that risk; notifying the ICO, so that they can provide appropriate additional advice and guidance; carrying out immediate remedial action to prevent a recurrence of the problem; and conducting an investigation to understand any systemic organisational failures which should be rectified.

For the future

The ICO has just been given the power to audit and inspect those government organisations that hold and process personal information without first having to gain permission. Similar powers are being sought for businesses.

Further, Section 55 of the DPA relates to the illegal buying and selling of personal information. Presently, it carries a criminal penalty of up to £5,000 in a Magistrates Court or an unlimited fine in a Crown Court. But going through Parliament as part of Criminal Justice and Immigration Bill is a proposal to add a two-year prison sentence. Also, the ICO wants reckless breaches of the Act to become a criminal offence. Only Section 55 breaches and breaches of an enforcement notices are criminal offences under the present law.

Conclusions

People expect their personal information to be properly protected at all times, whether held by the public or private sector. Organisations who fail to put in place appropriate measures to secure information risk alienating their customers, upsetting regulators and undermining their commercial viability. These risks are real and substantive. If not already in place, commit now the appropriate resource and attention needed to ensure secure effective information governance.

● **Andrew Dyson** is a partner at DLA Piper. He specialises in information law and data protection issues