



## **Information Commissioner's Office Powers: A Guide to Compliant Security in the UK from Network Box**

Legislation on protecting data in the UK – such as the Data Protection Act 1998 (revisions, that take effect in April 2010, were introduced to the Act in 2009) and PCI DSS – have made good security even more important for businesses. Since the introduction of the Data Protection Act in 1998, a company breaching data security rules could be served an enforcement notice by the Information Commissioner and made to clean up its act. In January this year, the Information Commissioner was given greater powers of enforcement, and the ability to fine companies breaching data security up to £500,000.

Organisations keep more data, and for longer, than ever before. Much of this data – customer records, financial information or personal identity details – has a real value to cyber-criminals, and any organisation that holds data is a potential target for a hacker. Whether it's stealing an identity, launching a phishing campaign, or cloning credit card information, consumer data has intrinsic value to cyber-criminals, so must be kept secure.

This guide is designed to give guidance to companies on best security practice to avoid a security breach. It is not designed to replace legal advice on compliance; and we advise companies to seek the advice of compliance law experts where appropriate. For the purposes of this guide, we have enlisted the help of [James Pickering](#), a commercial litigation barrister. His full opinion on the legal aspects of compliance can be read [here](#).

### **1. The background to current security requirements**

Recent years have seen some shocking data breaches from major organisations across the public and private sectors. In January this year, the [ICO publicly criticised the Southampton University Hospitals NHS Trust](#) for failing to meet data security standards of the Data Protection Act, and allowing a laptop to be stolen which contained 33,000 (password protected) patient records. It also [named and shamed Zurich Insurance](#) for losing an unencrypted back up tape that contained the financial details of 46,000 policy holders. Gwent Police recently [hit the headlines](#) after a file was emailed to the Register that contained details of criminal record checks on more than 10,000 people who were either in jobs or applying for jobs that require a CRB (Criminal Record Bureau) check.

Any organisation that holds personal data has a responsibility to secure it. Mistakes will always happen, particularly (as in the cases above) when the primary fault is either human error or a direct attack on physical security. But there is much that can be done to protect data and to lessen the impact of human error.

### **2. What are the principles of the Data Protection Act?**

The Data Protection Act has at its heart eight 'data protection principles'. These are listed on the [direct.gov website](#):

These principles require any organisation, corporation or governmental body that collects personal information to handle it safely. Anyone collecting personal information must:

- fairly and lawfully process it
- process it only for limited, specifically stated purposes
- use the information in a way that is adequate, relevant and not excessive
- use the information accurately
- keep the information on file no longer than absolutely necessary
- process the information in accordance with your legal rights
- keep the information secure
- never transfer the information outside the UK without adequate protection

All organisations collecting and using personal information are legally required to comply with these principles.

The law provides stronger protection for more sensitive information - such as your ethnic background, political opinions, religious beliefs, health, sexual life or any criminal history.

[James Pickering](#), a commercial litigation barrister, explains the purpose of the Data Protection Act:

“The basic purpose of the DPA 1998 is to regulate those who possess and control personal data relating to individuals. In general terms, it does this in 2 main ways. The first is to give individuals whose data is being held certain rights to obtain information about the nature and content of the relevant data being held in relation to themselves. The second is to create statutory obligations on the part of those holding the data to deal with such data in what can be broadly described as a “fair” way.”

Pickering examines the concept of the data protection principles:

Part I of the DPA 1998 introduces the concept of the “data protection principles”. These are 8 principles which in broad terms set out the way in which a person who controls data (a data controller) is required to deal with that data.

The above “data protection principles” are set out in Part I of Schedule 1 to the DPA 1998.<sup>1</sup> For present purposes, the relevant principle is the seventh which provides:

*“7. Appropriate technical and organisational measures shall be taken against unauthorised processing of personal data and against accidental loss or destruction of, or damage to, personal data.”*

Perhaps the most important provision of the DPA 1998 as originally enacted is section 4(4). That section provides that, subject to certain exceptions:

---

<sup>1</sup> DPA 1998, section 4(1), (2).

*“...it shall be the duty of a data controller to comply with the data protection principles in relation to all person data with respect to which he is the data controller.”*

In short, therefore, the net effect of the above is that a person who controls data is under a statutory obligation (note the use of the words “it shall be the duty of...”) pursuant to section 4(4) of the DPA 1998 to comply with the “data protection principles” including in particular the 7th principle which requires data controllers to take “appropriate technical and organisational measures” against, amongst other things, “accidental loss or destruction of...personal data”.

### **3. What are the penalties for failing to comply with the act?**

The original Data Protection Act of 1998 states that: “A person must not knowingly or recklessly, without the consent of the data controller – (a) obtain or disclose personal data or the information contained in personal data, or (b) procure the disclosure to another person of the information contained in personal data.” Contravening this was to commit a criminal offence.

The 2008 Criminal Justice and Immigration Act 2008 introduced some significant amendments to the act, which took effect on 6 April 2010. The key points from this are:

- increased powers of the Secretary of State to punish non-compliance
- the addition of five new sections introducing the concept of a ‘monetary penalty notice’ (a fine).

So:

“(1)The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that—

- (a) there has been a serious contravention of section 4(4) by the data controller,
- (b) the contravention was of a kind likely to cause substantial damage or substantial distress, and
- (c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller—

(a) knew or ought to have known—

- (i) that there was a risk that the contravention would occur, and
- (ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(d) failed to take reasonable steps to prevent the contravention.”

*James Pickering, Enterprise Chambers*

In Pickering’s words:

“A wholly innocent contravention will not be punished; but an intentional, reckless or negligent contravention will be.

“The greater the level of appropriate security application in place, the less chance there is of the Information Commissioner and/or a court concluding that any such contravention was deliberate or reckless.”

#### 4. What should businesses do?

In broad terms, a company that controls data has to comply with the data protection principles. This involves taking

‘appropriate technical and organisational measures...against unauthorised processing of personal data and against accidental loss or destruction of, or damage to, personal data.’

How, in practice, can businesses apply this principle? According to Pickering:

“What constitutes ‘appropriate technical and organisational measures’ will vary from organisation to organisation and will depend on the significance and impact of the data – and in particular the harm which might result from accidental loss - as well as the available technology and the cost of implementing the same. Ultimately, therefore, whether or not a particular step ought to be implemented will be a matter of judgment – with the more important the data, the greater the obligation on the data controller to provide effective security. In short, therefore, a commercial security application which is suitable for a business which controls low impact data may not necessarily be suitable for a business which controls data of greater importance and significance.”

#### 5. What do we recommend as best practice?

Pickering says:

“There is no single or absolute test of “best practice” with there instead being the somewhat nebulous standard as set out in the data protection principles. In short, what is best practice will vary from business to business depending on factors such as the nature of the data and the cost of appropriate security. Further practical guidance as to what is likely to be considered best practice within particular industries and sectors is contained in the Information Commissioners website at:

[http://www.ico.gov.uk/what\\_we\\_cover/data\\_protection/guidance/good\\_practice\\_notes.aspx](http://www.ico.gov.uk/what_we_cover/data_protection/guidance/good_practice_notes.aspx).”

Data breaches can come from any source: a lost data stick; a hack through a network vulnerability; or an insider either mistakenly or maliciously transferring data out of the organisation.

While there are no absolutes (and each company will have slightly different requirements), there are simple steps that each company can take to minimise the chances of a security breach. Please note: we always recommend that companies seek legal advice on compliance (and this is not designed to replace that advice).

##### 5.1. Avoid human error.

Most data breaches are caused by human error. This covers a multitude of sins: from an employee falling victim to a phishing attack; to leaving a laptop on a train with unencrypted data on it. Good security management can significantly reduce the risk of human error causing a breach. This doesn't just apply to the end user, but also to the

IT department. You can have the best security systems in the world in place, but if you don't keep them updated, or misconfigure the firewall, or change an application without checking the impact that has on security, then your systems may be rendered useless. For more information, see our [guide to updating systems](#).

**5.2. Plan for a breach.** Ensure that individual systems are redundant, so the impact of a breach is minimised. Have a plan ready to implement the minute a breach is identified. This should include a breach notification plan (voluntary at the moment, but [likely to become mandatory within the next two years](#)).

**5.3. Review any third-party suppliers that host data** such as CRM systems or financial systems providers (including web or mobile payment providers); and ensure that they are [PCI DSS compliant](#).

**5.4. Encrypt any data that has to be moved,** and ensure mobile devices and laptops are securely password protected. Where possible, use multi-factor authentication (our [guide to authentication](#) for more information).

**5.5. Check all data leaving the building,** in the same way that you check data that comes in (via any communication channel, such as IM or email). This will help prevent unauthorised transfer of data that could lead to compromised security.

**5.6. Remember that security is about more than just email.** In 2009, we saw a clear move by cyber-criminals towards focusing on exploiting vulnerabilities in applications, web browsers and servers, rather than just mailing executable code. As a result, you should integrate anti-spam, anti-virus and firewall to other critical protection, including intrusion detection and prevention (IDP), application security, VPN, and content filtering.

**5.7. Review what applications and systems are used across the organisation as part of your ISO9001 meetings or about once per quarter.** The security team must work to ensure they are aware of vulnerabilities in all systems from Internet facing routers to new web applications. Set clear user access rights and guidelines to ensure that all users understand what they should and shouldn't be using. For more information, see our [guide to monitoring applications](#).

**5.8. Ensure that all data is routed through the appropriate channels and that nothing bypasses security systems** (this is one of the most common causes of vulnerabilities). For more information, see our [guide to routing](#).

**5.9. Educate employees.** Hold security training at least once a year for each employee, to review security procedures and to make sure that all employees understand their role in keeping an organisation secure. Limit access rights so that only employees who really need access to certain applications or platforms have it.

**5.10. Use a secure VPN for home workers.** With more of us working from home at least some of the time, the risks of a security breach increase (for example, if the computer used is also used by other family members). Consider issuing a work computer to regular home workers that is configured to the organisation's security standards. Data carried between work and home on memory sticks or mobile devices can get lost in transit. Far better to allow access only via a secure VPN. See our [guide to remote working](#) for more information.

**5.11. Don't allow employees to download anything that isn't approved by the security team** – particularly P2P software or platforms, that can open up a clear route through the organisation's security. Even commonly-used platforms such as IM must be checked to ensure that it is routed via the right secure channels and updated regularly, to avoid leaving a 'back door' open to a hacker.

## 6. Conclusion

As Pickering says:

“What is considered “appropriate” will depend on all the circumstances of the case, but there can be no doubt that the greater the level of commercial security application in place, the less chance that any particular business will be seen to have not taken sufficient or appropriate steps. Similarly, the greater the level of advice taken by a data controller from entities such as Network Box, the greater the prospects of that business being able to show that any contravention was neither deliberate nor reckless and therefore outside the ambit of section 55A of the DPA 1998.”

Whether a company complies with the Data Protection Act will largely depend on the specific circumstances of each company. But a data breach could carry a larger cost than simply the risk of a fine from the Information Commissioner. The cost – both in monetary and reputational terms - of cleaning up after a data breach can be enormous. The cost of avoiding that breach is minimal.

**To talk to a security expert about data security and compliance, contact Simon Heron or James Mackie on 0800 107 6098, or email [nbuk@network-box.co.uk](mailto:nbuk@network-box.co.uk).**

For legal advice on compliance, contact

[James Pickering](#)

Enterprise Chambers

9 Old Square

Lincoln's Inn

London WC2A 3SR

### **About Network Box:**

Network Box Limited (NBL) is an international managed security services company, specialising in unified threat management (UTM). It continuously defends the networks of its customers using PUSH technology to instantaneously update protection, from 12 Security Operations Centres spread around the globe. NBL's customers in Asia, Australia, North America and Europe include companies such as BMW, Nintendo and Toyota, as well as banks, utilities companies and government organisations.

For more information on the latest security issues, see <http://www.network-box.co.uk>, or visit Simon Heron's blog at: <http://blog.network-box.co.uk>, or follow Simon on Twitter: <http://twitter.com/networkbox>.