

## Legal and Regulatory Compliance for UK IT Professionals

IT professionals in the UK have to ensure their organisations comply with an increasingly complex web of statute, regulation and foreign legal requirements. On top of this, they have to meet contractual obligations and protect the confidentiality, availability and integrity of corporate information.

### *Complex web of UK regulation*

The Data Protection Act ('DPA') is at the heart of these obligations, and there are key intersections between this law and the requirements of the PCI DSS (Payment Card Industry Data Security Standard), the EU Privacy Directive, the Human Rights Act ('HRA'), the Regulation of Investigatory Powers Act ('RIPA') and, for public sector organisations, the Freedom of Information Act.

### *Foreign laws*

There are also a number of foreign laws that may affect UK companies: California's SB1386, which deals with data breaches, appears to include companies worldwide in its scope, although the law has not yet been used against a non-Californian company. US anti-spam (the CAN-SPAM Act) and copyright (the Digital Millennium Copyright Act) may also affect UK companies. Even SOX, the US corporate governance law, has an impact on the IT departments of many UK subsidiaries of US-listed organisations.

## Legal and Regulatory Compliance for UK IT Professionals

UK companies trading in Europe may also be affected by local versions of EU directives or laws which go further than those applicable in the UK.

Ignorance of the law is no defence and can cost a business millions if it proceeds against an employer or alleged attacker without due process, and without having made the correct initial arrangements. It could even put an employer or information security professional in the dock and let the guilty party off the hook. It is an increasingly complex area, and one in which expert and up-to-date legal advice is essential!

### **The Data Protection Act**

The DPA is the most important UK IT law. The DPA applies to any organization (called a ‘data controller’) that processes personal data – data about living human beings (called ‘data subjects’), not about corporations. It is a principles-based law: it sets out eight general principles, rather than detailed requirements. Data controllers have to determine for themselves how best to comply with its principles, and the website of the Information Commissioner ([www.ico.gov.uk](http://www.ico.gov.uk)) contains substantial compliance guidance; certification to ISO/IEC 27001 is usually recognised as evidence that an organisation has taken adequate steps to meet its DPA compliance obligations.

Essential Reading - Data Breaches Report: [www.itgovernance.co.uk/products/1615](http://www.itgovernance.co.uk/products/1615)

### **The Data Protection Act - Details**

The eight principles of the DPA are that personal data must be:

## Legal and Regulatory Compliance for UK IT Professionals

1. fairly and lawfully processed;
2. processed for the specified purposes;
3. adequate, relevant and not excessive;
4. accurate and up-to-date;
5. kept no longer than necessary;
6. processed in accordance with the data subject's rights;
7. secure ('appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'); and
8. not transferred to countries that do not provide adequate protection for the data (ie, protection to at least the level required in the EU).

The DPA covers 'structured' data storage, and applies to both electronic and paper records.

The Information Commissioner is the only statutory authority for administering and maintaining the public register of data controllers. The DPA's reach includes CCTV records, websites and internet activity, recruitment and selection of staff, employment records, staff monitoring (including, for example, checking telephone records or internet use) and information about workers' health.

The DPA places restrictions on transferring personal data to countries that are not within the EU. This restriction is particularly important for organizations 'offshoring' any part of their customer support or other operations, or consolidating in a single location

## Legal and Regulatory Compliance for UK IT Professionals

services previously delivered from multiple jurisdictions, or having personal data stored or processed elsewhere. The EU Safe Harbor arrangements were devised to enable US companies to handle the data of EU residents in spite of the fact that the US does not meet the DPA requirements; not many US companies do.

A data subject is entitled to make a written request, called a Subject Access Request, to the data controller (accompanied by a minimal set fee) and to be given, within 40 days, a copy of all information held about them. This usually occasions a huge diversion of IT effort to trawl email archives as well as distributed file storage.

Data subjects have a number of other rights, such as having inaccurate data about them amended or deleted; preventing processing that is likely to cause them damage or distress and to sue for compensation if damage or distress has been caused, and preventing processing for direct marketing purposes, which means that they can stop the arrival of personalized junk mail by writing to the data controller.

Read more about the DPA in this handy pocket guide: [Data Protection Compliance in the UK](#)

### **BS10012**

BS10012 is the new British Standard that provides a specification for a Personal Information Management System against which an organisation can be externally audited and which will provide evidence of compliance with the DPA.

## Legal and Regulatory Compliance for UK IT Professionals

Obtain your own copies of BS10012 from [www.itgovernance.co.uk/products/2542](http://www.itgovernance.co.uk/products/2542).

The penalty for non-compliance with DPA was, from the outset, derisory, with the result that compliance has (at best) been inconsistent. Data Protection has, however, been in the news recently and, following a number of high profile data breaches (HMRC and many others), the Information Commissioner has been given the power to levy ‘substantial’ fines where he considers an organisation to have been recklessly negligent in its compliance with the DPA. As a minimum, any laptops or other portable media that contain personal data should be encrypted to FIPS 140.

The ‘tariff’ of fines for non-compliance is being devised at the moment, and the first fines might be expected before the year end – so sensible IT professionals should take action now to ensure they’re not going to land their companies in trouble.

### **FREEDOM OF INFORMATION AND THE ENVIRONMENT**

The DPA intersects with the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations.

Read: Data Protection vs Freedom of Information [www.itgovernance.co.uk/products/2088](http://www.itgovernance.co.uk/products/2088)

The FOIA provides a general right of access to all types of information held by public authorities and those providing services for them. There is a long list of information types that do not have to be provided and this list is growing. Information about private

## Legal and Regulatory Compliance for UK IT Professionals

companies that is contained in any tender documents is not automatically excluded.

The Information Commissioner is responsible for the DPA, the FOIA and the Environmental Information Regulations, which enable people to access environmental information held by or on behalf of public authorities and those bodies carrying out a public function.

Part of the information requested under either the FOIA or the Environmental Regulations might also be personal information, and as such information may not be disclosed, public sector organisations need to be clear about how they classify, maintain and archive these different types of information.

### **HUMAN RIGHTS AND INVESTIGATORY POWERS**

A person's rights under HRA, which incorporates into UK law the principles of the European Convention for the Protection of Human Rights and Fundamental Freedoms, are extensive. Most of the rights within this Convention are qualified, insofar as they are subject to limitations if the employer can show necessity to protect the rights and freedom of others. In particular, an employee could argue in a court or tribunal that the employer monitoring or tapping the employee's work telephone or email or Internet activity was a breach of her/his rights under HRA.

RIPA deals with the same issues. It makes it unlawful to intentionally intercept communications over a public or private telecommunications network 'without lawful authority'. Interception could be legal if both parties consented to the interception or,

## Legal and Regulatory Compliance for UK IT Professionals

where an employee has not given express consent, if the monitoring is to record evidence of business transactions; ensure compliance with regulatory or self-regulatory guidelines; maintain the effective operation of the employer's systems; monitor standards of training and service; prevent or detect criminal activity; or prevent the unauthorized use of computer or telephone systems (ensuring that the employer's policies are not breached). The interception of personal electronic communications will almost certainly also be covered by the DPA.

While there will certainly be a series of court and tribunal cases over the next few years that deal with the conflicts between the HRA, and the RIPA, employers need to introduce (with due process) an Acceptable Use Policy if they wish to be able to take legal or disciplinary action in respect of inappropriate employee behaviour.

### **PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS 2003**

The Information Commissioner is also responsible for enforcing these regulations, which cover use, by telecommunication network and service providers, and individuals, of any publicly available electronic communications network for direct marketing purposes, and any unsolicited direct marketing activity by telephone, fax, electronic mail (which includes text/video/picture messaging, SMS and email) and by automated telephone calling systems.

The key right conferred both on individuals and on corporate entities is the right to register their objection to receiving unsolicited direct marketing material, and these regulations provide a mechanism

## Legal and Regulatory Compliance for UK IT Professionals

for doing this. A number of requirements, including in some circumstances the obligation to obtain the prior consent of the person to whom marketing messages are to be directed, are imposed on direct marketers and these will intersect with obligations under the DPA; organizations have to ensure that they comply with both and systems, therefore, have to be designed to make this possible.

### **COMMERCIAL LAW**

There is also a number of IT-related regulations that impact how organisations carry out their business. The first of these is the Companies Act 2006, which consolidated and replaced all previous UK company law. This Act contains many provisions that recognise the electronic nature of today's commercial world. Its provisions include the requirement that organisations identify themselves clearly in all their email and on their websites; it allows for email to be used to form contracts and to be evidence in a court; and it sets out in detail the conditions under which public companies can use websites and email for the whole range of shareholder communication.

The Electronic Communications Act had already started to tackle the issue of electronic signatures and this Act was designed to regulate the usage of cryptography and to make provision for appropriately authenticated electronic signatures to be used in electronic commerce and for them to be admitted as evidence in court.

## Legal and Regulatory Compliance for UK IT Professionals

### **E-Commerce and distance selling**

Organizations selling goods and services through e-commerce must also be aware of a growing range of distance selling regulations. The Financial Services (Distance Marketing) Regulations set out rules about information that must be supplied to consumers when financial services are sold at a distance (eg electronically); the Consumer Protection (Distance Selling) Regulations describe information that all consumers (not businesses) are entitled to receive from suppliers, and their rights to cancel a transaction; and the Electronic Commerce Regulations, which contain specific requirements covering (inter alia) information to be provided by e-commerce businesses, how prices should be presented, and how unsolicited email should be identified. Again, system, website and sales process design (and customer information) has to take these various requirements into account.

There is clearly an intersection between all these regulations, the DPA and, for organizations that accept payment cards, the requirements of the PCI DSS.

### **COMPUTER MISUSE ACT 1990 ('CMA')**

The CMA is of renewed importance to UK IT professionals. It is designed to provide for securing computer material against unauthorized access or modification and outlaws, within the UK, hacking and the introduction of computer viruses. It hasn't been entirely successful in doing so.

Its implications, though, are far reaching: anyone using someone else's user name without proper

## Legal and Regulatory Compliance for UK IT Professionals

authorization is potentially committing an offence. Anyone copying data who is not specifically authorized to do so is potentially committing an offence. It also has relevance for organizations whose employees may be using organizational facilities to hack other sites or otherwise commit offences identified under the Act.

Organizations could use the RIPA to ensure that staff are complying with the law; they would certainly need to have explicit user authorizations and acceptable use policies in place, or any disciplinary action based on the CMA would almost certainly fail – and fail expensively, given the intersection between CMA, RIPA and HRA.

### ***Police and Justice Act 2006 (the ‘PJA’)***

The Police and Justice Act 2006 (which deals with many other issues) also amended the CMA, and increased the maximum sentence for ‘unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc’ (aimed primarily at denial of service attacks, but with a far wider effect) from five to ten years.

## **INTELLECTUAL PROPERTY**

Information is, by any standard, intellectual property or IP; the Internet starting point for organizations that want detailed advice on intellectual property is the website of the UK Patent Office (which, since April 2007, has been operating as the UK Intellectual Property Office): [www.ipo.gov.uk](http://www.ipo.gov.uk). The principal legislation on copyright can be found in the Copyright Designs and Patents Act 1988. It has been amended a number of times and there is no official

## Legal and Regulatory Compliance for UK IT Professionals

consolidation of it. Copyright issues include both paper and electronic documents, as well as patents, trademarks and designs.

### **Software copyright**

A most important issue in dealing with copyright is for the organization to ensure that it is not infringing the copyright of its software suppliers. Any software that is running on the organization's network is potentially subject to copyright restrictions and it is essential that the organization ensure that it has the correct type and number of licences for this software.

### **SAFEGUARDING OF ORGANIZATIONAL RECORDS**

Records must be protected from loss, destruction or falsification. Some records must be retained to meet statutory or regulatory requirements, while others may be needed to provide adequate defence against potential civil or criminal action or to prove the financial status of the organization to the range of potential interested parties, including shareholders, tax authorities and auditors, or to meet contractual liabilities.

All forms of record are included: paper, electronic documents and emails. Electronic mailbox policies that delegate responsibility to individuals to destroy email records may be in breach of these requirements.

Due consideration should be given to the possible degradation of media over time and any manufacturer's recommendations for storage should be followed. Similarly, system upgrades and changes

## Legal and Regulatory Compliance for UK IT Professionals

must allow for archived electronic data to remain accessible throughout its retention period.

Records should be destroyed once they have reached the end of their retention period

### **What's the deal with PCI-DSS?**

There's a lot of interest in PCI – and rightly so because it has real teeth. Or does it? Ever changing deadlines and lack of clarity and education has made it difficult to understand.

Target dates for compliance with the PCI DSS have all long since passed. Many organisations - particularly those that fall below the top tier of payment card transaction volumes - are not yet compliant.

The latest version (1.2) outlaws the use of WEP in wireless networks and was available from 1 October 2008. The PCI Security Standards Council (<https://www.pcisecuritystandards.org>) has also recently issued standards for Pin Entry Devices and for online Shopping Carts applications.

Key facts about PCI:

1. PCI DSS has no legal status: it is not a law. Enforcement can only be carried out by contractual means.
2. Enforcement is through the commercial banks that have the merchants as customers. Thousands of banks are involved, many with more pressing challenges than policing PCI. The enforcement of PCI compliance is nationally and internationally inconsistent.

## Legal and Regulatory Compliance for UK IT Professionals

3. PCI DSS is a prescriptive standard with one-size-fits-all approach to information security requirements.

Non-compliance, though, is a short-sighted and highly risk stance to adopt - rather like assuming that your business has no exposure to acts of nature or IT failure and doesn't, therefore, require a business or IT service continuity plan.

All businesses that accept payment cards are prey for hackers and criminal gangs that seek to steal payment card and individual identity details. Many attacks are highly automated, seeking out website and payment card system vulnerabilities remotely, using increasingly sophisticated tools and techniques. Once a vulnerability has been discovered, an attack can start - without management or staff of the target company having a clue.

When the attack is exposed - perhaps through a victim disputing fraudulent credit card charges - the target company will be exposed to a harsh and expensive set of repercussions. These will range from customer desertion and brand damage to significant penalties and operating requirements imposed by their acquiring bank, which will include a future level of monitoring at a level normal only applicable to the very largest of merchants.

Breach of PCI can be expensive. TJX, Inc (the owner of the TK Maxx clothing chain) took a \$118 million earnings hit in 2007 to cover the fines, penalties and other costs that resulted from a widely-reported wireless security breach that may have affected 100 million cardholders worldwide. They also had to divert significant management time and money to

## Legal and Regulatory Compliance for UK IT Professionals

handle multiple legal suits and class actions, and have belatedly had to comply with PCI DSS anyway.

PCI DSS is designed to ensure that merchants are effectively protecting card holder data. It recognises that not all merchants may have the technical understanding to identify for themselves the steps necessary to achieve this and short-circuits that danger by providing explicit and detailed requirements. All merchants, and their service providers, should get in line with PCI DSS, and ensure that they stay compliant.

For more information on PCI DSS, and for critical tools, resources and practical compliance guidance, see [www.itgovernance.co.uk/pci\\_dss.aspx](http://www.itgovernance.co.uk/pci_dss.aspx)

### **DISABILITY DISCRIMINATION ACT ('DDA')**

Last, but not least, the IT professional also needs to be aware of the DDA, which made it unlawful to discriminate against any person in respect of their access to, or use of, a means of communication, information services or the services of any profession or trade, or any local or other public authority.

The DDA clearly includes websites and on-screen or browser-based communication methodologies within its scope.

The Act does not require a service provider to adopt one way of meeting its obligations rather than another. The focus of the Act is on results. Where there is a physical or electronic barrier, the service provider's aim should be to make its services accessible to disabled people.

## Legal and Regulatory Compliance for UK IT Professionals

### ***Critical Reading***

- BS10012  
[www.itgovernance.co.uk/products/2542](http://www.itgovernance.co.uk/products/2542)
- Cyberwar, Cyberterror, Cybercrime:  
[www.itgovernance.co.uk/products/1731](http://www.itgovernance.co.uk/products/1731)
- Data Breaches Report – Trends & Best Practice:  
[www.itgovernance.co.uk/products/1615](http://www.itgovernance.co.uk/products/1615)
- DPA PG: [Data Protection Compliance in the UK](http://www.itgovernance.co.uk/products/1615)
- Information Security Law - the Emerging Standard for Corporate Governance:  
[www.itgovernance.co.uk/products/1976](http://www.itgovernance.co.uk/products/1976)
- IT Regulatory Compliance – Set of Pocket Guides: [www.itgovernance.co.uk/products/937](http://www.itgovernance.co.uk/products/937)
- PCI DSS: [www.itgovernance.co.uk/pci\\_dss.aspx](http://www.itgovernance.co.uk/pci_dss.aspx)
- Unified Compliance Framework:  
[www.itgovernance.co.uk/products/1708](http://www.itgovernance.co.uk/products/1708)