Chiene+Tait
CHARTERED ACCOUNTANTS

Do You Know if You Are Data Protection Act or Payment Card Industry Compliant?

The Data Protection Act – what is it and how does it affect you?

The Data Protection Act covers how businesses hold data about a "living and identifiable individual". Individuals can be identified by various means such as their name and address, telephone number or email address. The Act applies to data which is held, or intended to be held, on computers and to data held in a "relevant filing system". If a business fails to adhere to the Act, the reputational affect of a data breach can be considerably more than the monetary fine that may be applied by the Information Commissioners Office. Fines of up to £500,000 or a prison sentence can be imposed on a business in the case of a serious contravention.

Key Principles of the Act

- Data may only be used for the specific purposes for which it was collected e.g. contact details for a job are retained for the period of how long the job runs for only.
- Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information (for example, the prevention or detection of crime). It is an offence for Other Parties to obtain this personal data without authorisation.
- Individuals have a right of access to the information held about them, subject to certain exceptions (for example, information held for the prevention or detection of crime).
- Personal information may be kept for no longer than is necessary and must be kept up to date.
- Personal information may not be sent outside the European Economic Area unless the individual whom it is about has consented or adequate protection is in place.
- Subject to some exceptions for organisations that only do very simple processing (e.g. a diary/ Blackberry or workplan), and for domestic use, all entities that process personal information must register with the Information Commissioner's Office.
- The departments of a company that are holding personal information are required to have adequate security measures in place. Those include technical measures (such as firewalls) and organisational measures (such as staff training).
- Subjects have the right to have *factually incorrect* information corrected.

How Does This Affect You?

In essence the rule of thumb is to treat someone else's data as you would wish your own personal data to be treated. In terms of the 'technical measures' to secure personal data the points below will help you stay on the right track to protect any personal data you may store:

- Password protect your PC/laptop.
- Where possible encrypt your PC/laptop in case of theft.

- Install a firewall on your home/office network (this may already be part of your ADSL/broadband router, if so ensure it is turned on and updated).
- Ensure antivirus is installed on your PC/laptop and updated to prevent virus/malware infection.
- Ensure your operating system (Microsoft Windows or Mac) patches and updates are installed on your PC/laptop in a timely manner, to avoid vulnerability exploitation.

PCI (Payment Card Industry) Data Security Standard Compliance – what is it and how does it affect you?

What is the PCI Security Compliance?

The PCI (Payment Card Industry) data security standard is an information security standard for organisations that handle credit cardholder information for the major debit/credit cards. It was created to reduce credit card fraud by reducing the consumer's exposure to potential risks and threats to security.

How Does This Affect You?

If you take payments by credit card for work and retain the credit card information, you must put steps in place to achieve the PCI data security standard. Smaller businesses and service providers are not required to explicitly comply with each of the controls prescribed by the PCI data security standard. These smaller organisations must still implement all recommended controls, in order to maintain good recordkeeping and avoid potential liability, in the event of fraud associated with theft of the cardholder's data.

Below are the controls that must be put in place to formally comply or informally validate with the standard:

Control Objectives	PCI Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

If a company is employing the services of a third party to process debit/credit card payments, then it is the responsibility of the third party to be PCI compliant as long as no cardholder details are stored locally.

If you have any queries or concerns about the Data Protection Act or credit card payment standards information above, please contact your bank, IT provider or the ICO directly via the ICO helpline on 0303 123 1113. Alternatively, the Chiene + Tait IT team would be happy to assist by contacting Ian Clark, IT Manager on 0131 558 5800 or email ian.clark@chiene.co.uk.