SonicWALL CDP Seminar

Continuous Data Protection Seminar – 15 July 2009

Dr Rosanna Cooper
Telfords Yard, 6/8 The Highway
London, E1W 2BS
Tel: +44 0207 084 5739
Fax: +44 0207 481 4197
Email: enquiries@rtcooperssolicitors.com
Website: www.rtcoopers.com
15 July, 2009

RTC
RT Coopers

Introduction

- Introduction
- Data Protection Act
- Specific Issues Relating to Back-ups/Security
- Data Protection Compliance – Best Practice
- Conclusion

RT Coopers

Introduction

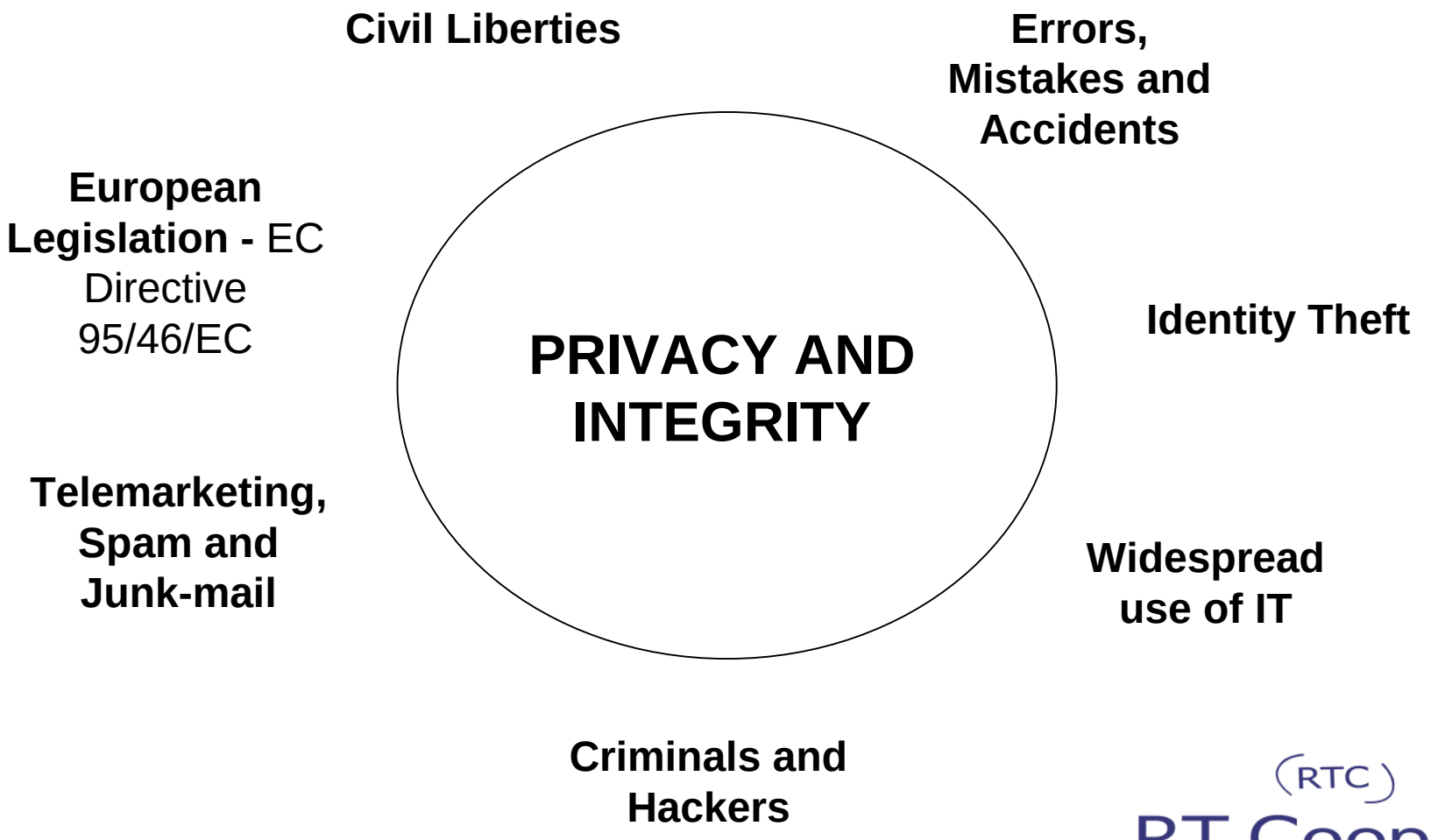
RT Coopers

Introduction

- Information about individuals require **protection**
- **Personal data** includes information about individuals which would be considered private
- An individual's **personal data** must be complete, accurate and up-to-date
- Data Protection legislation covers all market sectors –the need for reliable **data protection procedures and policies**

RTC
RT Coopers

Introduction



RT Coopers

What is Data Protection?

RT Coopers

What is Data Protection?

- Data Protection Act
  - Why is it Relevant?
  - Are you or your Client processing ‘Data’?
  - What Types of ‘Data’?
  - Data Protection Principles
  - Data Controllers and their responsibilities?
  - Data Processors and their responsibilities?

- Specific Issues Relating to:
  - Confidentiality
  - Back-ups
  - Retrieval
  - Security
  - Staff Training

RTC
RT Coopers

What is Data Protection?

- **Data Controller**
  - Is a “person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any **personal data** are, or are to be, processed”.

  - Data Controller has primary responsibility for compliance
    - Personal Data – Data about identifiable living individuals
    - Determine whether processing ‘personal data’
    - Decide how and why personal data are processed
    - Information handling – Compliance with the eight principles of good practice
    - Ensure that Data Processors adhere to the terms of their Data Processing Agreements
    - Acquire “data subjects” consent for processing sensitive data
    - Existing procedures for handling sensitive or personal data?
    - Notification

RTC
RT Coopers

What is Data Protection?

- **Data Controller cont'd**
  - Security measures to safeguard personal data - Responsibility for day-to-day security measures
    - Discussing with senior colleagues what measures should be adopted
    - Writing procedures for staff to follow
    - Organising training for staff - checking whether following procedures and that the measures work
    - Monitoring change

RT Coopers

What is Data Protection?

- **Data Processor**
  - Is “any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller” i.e. Subcontractors, bureaux or agents processing data on behalf of your organisation
  - May require contract between data controller and processor

RT Coopers

What is Data Protection?

- **Personal Data**
  - Is any data about identifiable individuals. It includes:
    - Facts and opinions about individuals
    - Information regarding the intentions of the data controller towards the individuals
- **Data**
  - Means information which is or is intended to be processed electronically, or which forms or is intended to form part of a “relevant filing system”
  - Data in electronic form is defined in section 1(1)(a) of the DPA.
    - Information that is “processed by means of equipment operating automatically in response to instructions given for that purpose” or information that is “recorded with the intention that it should be processed by means of such equipment” is ‘data’
- **Processing**
  - Means “obtaining, recording or holding information or personal data or carrying out any operation or set of operations on the information or data”.
  - The DPA introduces two more types of manual processing of information which, if the information relates to an identifiable individual, will involve processing of ‘personal data’:
    - Processing information as part of an ‘accessible record’; and
    - Processing recorded information held by a public authority

RTC
RT Coopers

What is Data Protection?

- The DPA is concerned with four types of Data which can be broadly referred to as:
  i. Electronic Data;
  ii. Data forming part of a Relevant Filing System;
  iii. Data forming part of an Accessible Record (other than those accessible records falling within (i) or (ii) above); and
  iv. Data recorded by a Public Authority

- 'A relevant filing system':
  - The files are structured or referenced in such a way as clearly to indicate at the outset of the search whether specific information capable of amounting to personal data of an individual requesting is held within the system and, if so, in which file or files it is held; and
  - Which has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria.

RTC
RT Coopers

What is Data Protection?

- '**Personal Data**' must be processed in accordance with the Eight Data Protection Principles
- Processing is wholly or partly by automatic means, or where it is non-automated processing of personal data which forms part of a 'filing system' or is intended to form part of a 'filing system
- Protection may be provided by information security controls including:
  - Technical controls (e.g.: Login ID's and Passwords)
  - Procedural controls (e.g.: Company policy)
  - Legal Controls (e.g.: The Data Protection Act 1998)

RTC
RT Coopers

Data Protection Principles

- There are **8 Data Protection Principles**:

1. Personal Data must be processed fairly and lawfully
2. Personal Data must be obtained only for specified and lawful purposes and must not be processed further in any manner incompatible with those purposes
3. Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they were collected
4. Personal Data must be accurate and, where necessary, kept up to date
5. Personal Data must not be kept longer than is necessary for the purposes for which they were collected
6. Personal Data must be processed in accordance with the rights of data subjects
7. Personal Data **must be kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage**
8. Personal Data must not be transferred to countries outside the European Economic Area unless the country of destination provides an adequate level of data protection for those data

http://www.ico.gov.uk/

RTC
RT Coopers

Specific Issues

RT Coopers

Specific Issues

- Specific Issues Relating To:
  - Confidentiality
  - Back-ups
  - Retrieval
  - Security
  - Staff Training

RTC
RT Coopers

Specific Issues

- Confidentiality
  - Must Keep Data CONFIDENTIAL
  - Confidentiality Agreements
  - Confidentiality Provisions in Employment Contracts

- Personal Data **must be kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage:**

- What constitutes lost, destroyed or damaged data?
  - Data Destroyed - Either accidentally, or deliberately, deleted
  - Data lost - Can no longer be found - Lost
  - Damaged data - Files may become corrupted
  - Best Practice - Clear policy e.g. for back-up of drafts

RTC
RT Coopers

Specific Issues

- **What is the Purpose of Backing-up Data?**
  - By Backing-up Data a Data Controller/Processor is taking steps to:
    - Put adequate measures in place to prevent the unauthorised loss, damage or destruction of Data (7th Principle)
      - Disaster Recovery
      - System Failure - Total loss or corruption of Data

RTC
RT Coopers

Specific Issues

- **For how long should Back-up Data be held?**
  - Dependant on the:
    - Procedures and Policies in place
    - The nature of the organisation processing the data
    - Purpose for which the organisation is processing this Data
    - The nature of the Data
  - Not be kept longer than is necessary (5th Principle)
  - Best Practice – Data are accurate and, where necessary, kept up to date (4th Principle)

RTC
RT Coopers

Specific Issues

- **Security?**
  - An organisation should take into account technological developments when deciding on security measures but no requirement for ‘state of the art’ technology
  - Act specifically allows organisations to take cost into account
  - The measures must be appropriate for the harm that could result and the nature of the information to be processed
  - How valuable, sensitive or confidential is the Data?
  - What damage or distress could be caused to individuals if there was a security breach?
  - What effect would a security breach have on the organisation?
    - In cost?
    - Reputation?
    - Customer trust?
  - If organisation has highly sensitive or confidential personal information e.g. medical records or financial data that could cause damage or distress if unauthorised disclosure:
    - What is the potential threat?
    - Is the organisation’s security measures vulnerable?

RTC
RT Coopers

Specific Issues

- **Security?**
  - How does the organisation manage the operation of its computer systems?
    - Is this done with procedures and by documenting change or is it on ad-hoc basis?
    - Are there checks and balances in the job roles to help prevent unauthorised changes or even fraud?
  - Special security measures for accessing servers, back-up systems
  - Protection against the possible loss of information if the power supply fails?
  - To ensure your equipment is properly maintained to prevent against loss or interruption to your work?
  - Do you control the access to your computer systems? Do staff have their own password and only use the system using their own?

RTC
RT Coopers

Specific Issues

- **Security?**
  - Ensuring Business Continuity:
    - Is the system capable of checking that the data are valid and initiating the production of back-up copies? If so, is full use made of these facilities?
    - Are back-up copies of all the data stored separately from the live files?
    - Is there protection against corruption by viruses or other forms of intrusion?
  - Detecting and dealing with breaches of security:
    - Do systems keep audit trails so that access to personal data is logged and can be attributed to a particular person?
    - Are breaches of security properly investigated and remedied; particularly when damage or distress could be caused to an individual?

RTC
RT Coopers

Specific Issues

- **Security?**
  - Staff Selection and Training:
    - Is proper weight given to the discretion and integrity of staff when they are being considered for employment or promotion or for a move to an area where they will have access to personal data?
    - Are the staff aware of their responsibilities?
    - Have they been given adequate training and is their knowledge kept up to date?
    - Do disciplinary rules and procedures take account of the requirements of the DPA? Are these rules enforced?
    - Does an employee found to be unreliable have his or her access to personal data withdrawn immediately?
    - Are staff made aware that data should only be accessed for business purposes and not for their own private purposes? The Act also requires you to take reasonable steps to ensure the reliability of employees that have access to personal information.
  - Training staff in their responsibilities about the personal information the organisation processes? For example, making it clear Data is confidential and the restrictions on how this should be used?

RTC
RT Coopers

Compliance

RT Coopers

Compliance

- Best Practice
  - In the event the Data Protection Principles and all contractual obligations are adhered to, the organisation is likely to meet the requirements of the DPA1998:
    - Reducing the likelihood of claims being issued against the organisation in respect of Data Protection
    - Impacting on any insurance policy relating to Data Protection
    - Preventing unauthorised use of Personal Data

RTC
RT Coopers

Compliance

- Best Practice
  - Clearly define responsibilities for security between data processor and client
  - Business continuity arrangements that identify how to protect and recover the personal information held by the organisation
  - Check compliance with legal obligations such as copyright or licensing requirements?
  - Periodic checks of your security arrangements to ensure they are still appropriate and up to date?

RTC
RT Coopers

Compliance

- Best Practice
  - The management of any organisation should ensure:
    - Appropriate safeguards are in place to prevent Personal Data being leaked, for example by e-mail, from an organisation's internal databases
    - All Personal Data are appropriately backed up as often as possible to prevent loss
    - Personal Data are not made available to any individual or employee without the authorisation of the Data Controller
    - Set clear directions for its employees to follow
    - Demonstrate support for, and commitment to, data protection through the issue and maintenance of appropriate policies across the organisation

RTC
RT Coopers

Compliance

- Best Practice
  - Using another organisation to process personal information often causes security problems
  - The client has to determine whether the Data Processor has the legal responsibility for processing personal data e.g. security measures in place
  - There are steps laid down in the Act which must be adhered to
    - The Act introduces express obligations upon data controllers when the processing of personal data is carried out by a data processor on behalf of the data controller. In order to comply with the Seventh Principle the Data Controller must:
      - Choose a Data Processor providing sufficient guarantees in respect of the technical and organisational security measures they take
      - Take reasonable steps to ensure compliance with those measures
      - Ensure processing by the Data Processor is carried out under a contract, which is made or evidenced in writing, under which the data processor is to act only on instructions from the Data Controller
        - The contract must require the data processor to comply with obligations equivalent to those imposed on the Data controller by the Seventh Principle. BS 7799 and 1S0/IEC Standard 17799.

RTC
RT Coopers

Compliance

- Best Practice
- Has a risk assessment been carried out?
  - To take account of what Data you need to protect?
  - The type of security problems that could occur?
  - The effectiveness of your current security measures?
  - Does the person with responsibility for security have the standing and resources to ensure the job gets done?
  - Any security manager needs management approval?
  - Is an overall security policy required?
  - Are there security procedures in place for staff to follow?
  - Is there co-ordination between key people in the organisation? For example, the security manager will certainly need to know about the commissioning and disposal of any new IT equipment.
  - Are checks made that people are taking their security responsibilities seriously?
  - Is there a procedure to ensure security incidents are investigated and lessons are learnt?
  - Is access given to anyone outside the organisation, for example, for computer maintenance? Is the organisation clear about what they need access to and why, and what security is needed to have in place to oversee what they do?

RTC
RT Coopers

Compliance

- Best Practice
  - Privacy Policy
  - Terms and Conditions for your Business
  - Terms and Conditions as Data Processor
    - Legal Contract required to set up managed service to backup data remotely on behalf of customers
    - At a minimum contract to be clear about their use and disclosure of the information
    - The contract must also have security measures
    - Client must take reasonable steps to check that the Data Processor is adhering to those security measures
  - Limitation of Liability
  - Consequential losses
  - Service Level Agreements
  - Security Measures
  - Insurance

RTC
RT Coopers

Compliance

- Best Practice
  - Some of the security controls that the data controller:
    - Security management
    - A security policy setting out management commitment to information security within the organisation
    - Reasonability for the organisation's security policy clearly placed on a particular person or department
    - Is there sufficient resources and facilities made available to enable that responsibility to be fulfilled?
  - Controlling access to information:
    - Is access to the building or room controlled or can anybody walk in?
    - Can casual passers-by read information off screens or documents?
    - Are passwords known only to authorised people and are the passwords changed regularly?
    - Do passwords give access to all levels of the system or only to those personal data with which that employee should be concerned?
    - Is there a procedure for cleaning media (such as tapes and disks) before they are reused or are new data merely written over old? In the latter case is there a possibility of the old data reaching somebody who is not authorised to receive it? (e.g. as a result of the disposal of redundant equipment).
    - Is printed material disposed of securely, for example, by shredding?
    - Is there a procedure for authenticating the identity of a person to whom personal data may be disclosed over the telephone prior to the disclosure of the personal data?
    - Is there a procedure covering the temporary removal of personal data from the data controller's premises, for example, for staff to work on at home? What security measures are individual members of staff required to take in such circumstances?

RTC
RT Coopers

Conclusion

RT Coopers

Conclusion

- Data Protection is a **very serious** issue for all organisations that handle personal data.
- Make sure you know what the consequences of your actions are!
- **Professional legal advice is crucial to staying on top of things!**
- **Trouble is easily avoided!**

RTC
RT Coopers

Further Information:

RT Coopers Solicitors

Telfords Yard, 6/8 The Highway
London, E1W 2BS

Tel: +44 0207 084 5739
Fax: +44 0207 481 4197

Email: enquiries@rtcooperssolicitors.com
Website: www.rtcoopers.com

THANK YOU

RT Coopers