Data Protection

PIPA Conference 2012 – 10 July

Dr Rosanna Cooper
Tel: 020 7488 9947
Switchboard 020 7173 6292
Fax: 020 7173 6291
Email: enquiries@rtcooperssolicitors.com
Website: www.rtcoopers.com
10 July, 2012

RT Coopers

PIPA

Introduction

- Introduction
- What is Data Protection?
- Relevance of Data Protection Act?
- Data Protection Issues
- Defined Terms
  - Case Study 1
- Eight Data Protection Principles
  - Case Study 2
- **Specific Issues pertinent to Medical Information and Pharmacovigilance**
  - **Case Study 3**
  - **Case Study 4**
  - **Case Study 5**
- Privacy Policy
- Cookies
- Risk Assessment – Best Practice
- Conclusion

RT Coopers

PIPA

What is Data Protection?

Why is Data Protection Relevant?

- To strike a balance between individuals' rights to privacy and the ability of organisations to use data gathered for the purposes of their business
- Contains the rules governing data protection

When does the Data Protection Act 1998 ('DPA') apply?

- DPA applies whenever a **data controller processes personal data or personal sensitive data**

RT Coopers

PIPA

Why is the DPA needed?

RT Coopers

PIPA

Meaning of Data Protection?

- Information about individuals requires **protection**
- **Personal data** include 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

PIPA

Defined Terms

Who is a 'Data Controller'?

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". E.g. an employer, NHS Trust, GP surgery and pharmaceutical company

- Compliance with DPA
- 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
- Acquire "data subjects" consent for processing personal sensitive data
- Existing procedures for handling personal sensitive or personal data?
- Notification

RTC RT Coopers

PIPA

Defined Terms

What is the Data Controller's primary responsibility for compliance?

- Data controller is responsible for day-to-day security measures to safeguard personal data

Common tasks and responsibilities:

  - Discussing with senior colleagues what measures should be adopted
  - Writing procedures for staff to follow – **Data Protection Policy**
  - Organising training for staff - checking whether following procedures and that the measures work
  - Monitoring change

- A **data protection officer** may be appointed.

RTC RT Coopers

PIPA

Defined Terms – Data Protection Officer

- Most organisations need at least one designated Data Protection Officer (part-time for SMEs)
- Large organisations normally split Data Protection activities into:
  - Routine administrative tasks
  - Management (policy, audits *etc*.)
- Need working links to IT/IT Security, Internal Audit, Legal, Risk Management etc.

RT Coopers

PIPA

Defined Terms - Data Protection Policy

Management should set clear directions and demonstrate support for, and commitment to, data protection through the issue and maintenance of appropriate policies across the organisation

RT Coopers

PIPA

Defined Terms

Who is a 'Data Processor'?

Data Processor = "Any person (other than an employee of the Data Controller) who **processes the data on behalf of the Data Controller**"

E.g. Subcontractors, bureaux or agents processing data on behalf of your organisation

- May require contract between data controller and processor, known as a **data processing agreement**

RTC RT Coopers

PIPA

Defined Terms

What is 'Personal Data'?

Personal Data = Any data about **living individuals** who **can be identified from the data** or from that data and other information which are in the possession of, or are likely to come into the possession, of the data controller.
E.g. names, addresses, dates of birth, telephone numbers, email addresses and gender

- 'Personal data' include
  - Facts and opinions about individuals
  - Information regarding the intentions of the data controller towards the individuals

What is 'Sensitive Personal Data'?

Sensitive Personal Data = Information relating to the racial or ethnic origin of a data subject, his or her political opinions, religious beliefs, trade union membership, sexual life, **physical or mental health or condition**, or criminal offences or record.
E.g. medical history

RTC RT Coopers

PIPA

Defined Terms

What does 'Data' mean?

Data = Information which are or are intended to be processed electronically, or which forms or is intended to form part of a "relevant filing system"

- 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

RT Coopers

PIPA

Defined Terms

What is a 'relevant filing system'?

'Relevant Filing System' = 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

PIPA

Defined Terms

What does 'Processing' mean?

Processing = "**Obtaining, recording** or **holding** information or personal data or carrying out any operation or set of operations on the information or data"

- Processing of 'Personal Data'

(*Michael John Durant v Financial Services Authority [2003]*)

- Broadly defined
- Processed fairly and lawfully
- Certain conditions have to be met
- Data subject must be told the identity of the data controller and why information is or is to be processed

RTC RT Coopers

PIPA

Defined Terms

Latest Development

- Cases
  - *Michael JohnDurrant v Financial Services Authority [2003] EWCA Civ 1746* – Court of Appeal.

  - Subject access requests
  - Relevant filing system is limited to a system "*In which the files forming part of it are structured or referenced in such a way as clearly to indicate at the outset of the search whether specific information capable of amounting personal data of an individual requesting it…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 or information about the applicant can be readily located*"

RT Coopers

PIPA

Defined Terms

Latest Development

- *Michael JohnDurrant v Financial Services Authority [2003] EWCA Civ 1746* – Court of Appeal.

  - Purpose of the subject access provision is " *to enable [an individual] to check whether the data controller's processing… unlawfully infringes his privacy and, if so, to take such steps as the Act provides (i.e. blocking or rectification)…It is not an automatic key to any information, readily accessible or not of matters in which he may be named or involved*."

  "*It is likely in most cases that only information that names or directly refers to [a data subject] will qualify and "not all information retrieved from a computer search against an individual's name or unique identifier is personal data within the Act"*

RT Coopers

PIPA

Defined Terms

Latest Development

- *Michael John Durrant v Financial Services Authority*

- In deciding on a case-by-case basis whether information falls within the Act, two factors are relevant:

1.“..*Whether the information is biographical in a significant sense, that is, going beyond the recording of the putative data subject’s involvement in a matter or event that has no personal connotations…*

2.“…information should have the putative data subject as its focus rather than some other person with whom he may have been involved or some transaction event…In short, it is information that affects his privacy, whether in his personal or family life, business of professional capacity”

Clear warning to litigants that the Act: “*…is not an automatic key to any information, readily accessible or not, of matters of matters in which he may be named or involved. Nor is to assist him…to obtain discovery of documents that may assist him in litigation or complaints against third parties.”*

RT Coopers

PIPA

Case Study 1

A new slimming pill (e.g. Qnexa) has recently undergone Phase I clinical studies. The participants completed a form prior to the study with their details, such as:

- Names, addresses, email addresses, gender, any previous health issues and a brief medical history
- Consent for the company to contact the participant's GP
- Consent to participate in the trial

After 2 weeks, participant A developed serious heart palpitations and suffered anxiety attacks.
Participant A completed an online form on the company's website to disclose the adverse side effects. The company has a structured database which holds details included under Qnexa and are identified according to the type of reaction. The participants' names are recorded under the corresponding reaction.

RTC RT Coopers

PIPA

Case Study 1

Participant A also contacted her local GP by phone and also made an appointment. At the meeting, the GP enters information relating to the adverse side effects into the participant's records held on the computer, as well as written notes, which are stored in participant A's file, in the cabinet. The cabinet is organised alphabetically.

Q

Identify the following:

- Any personal data
- Any sensitive personal data
- The data controller
- The data processor

RTC RT Coopers

PIPA

Data Protection Principles

- 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 form part of a 'filing system' or are intended to form part of a 'filing system

RT Coopers

PIPA

Data Protection Principles

Latest Development

- *Bodil Lindqvist*

- European Court of Justice first ruling – Mrs Lindqvist set up internet pages about the parish church: Held

  -Referring to person on the Internet and identifying them either by name or by other means constitutes processing of personal data by automatic means within the meaning of community law;
  -Exemption for processing carried out by a natural person in the exercise of activities which are exclusively personal or domestic does not apply to the publication of information on the Internet. Internet publication accessible to an infinite number of people;
  -Transfer of data to a third country – does not cover the loading of data onto an Internet page even if such data are accessible to persons in third countries. This is the position regardless of whether the an individual in a third country has accessed the Internet or whether the server is located of that hosting service is physically located in a third country.

RT Coopers

PIPA

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

RT Coopers

PIPA

Data Protection Principles

5. Personal Data must be processed in accordance with the rights of data subjects

6. Personal Data must be kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage

7. Personal Data must not be kept longer than is necessary for the purposes for which they were collected

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

RT Coopers

PIPA

Data Protection Principles

Principle 1

Personal Data must be processed fairly and lawfully

The data controller must justify the **processing** of **personal data** as being fair, by meeting one of the following:

- the data subject has given his **consent** to the processing;
- the processing is **necessary** for the **performance of a contract** or the entering into of a contract to which the data subject is a party;
- the processing is **necessary for compliance with any legal obligation** to which the data controller is subject;
- the processing is **necessary in order to protect the vital interests** of the data subject;
- the processing is **necessary for the administration of justice**; or
- the processing is **necessary for the purposes of legitimate interests** pursued by the data controller provided such processing does not harm the rights and freedoms or legitimate interests of data subjects.

RTC RT Coopers

PIPA

Data Protection Principles

Principle 1

The data controller must satisfy a further condition if **processing personal sensitive data**. Most pertinent conditions are:

- where the data subject has given his **explicit consent**;
- where the processing **is required for the purposes of complying with employment law**;
- where it is **necessary to establish, exercise or defend legal rights**

RT Coopers

PIPA

Data Protection Principles

Principle 1 – Case Study
Q
Is the company that is conducting studies on Qnexa complying with the conditions of Principle 1 in relation to personal data and/or personal sensitive data? If so, which?

Principle 1 – Case Study (Scenario 1)

Participant A's GP relays the information provided about adverse reactions to the company conducting the studies, including participant A's details

Principle 1 – Case Study (Scenario 2)

Participant A's GP relays the information provided about adverse reactions to the company conducting the studies, without including participant A's details
What issues are there, if any, in each scenario?

RTC RT Coopers

PIPA

Data Protection Principles

Principle 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

- A data protection notice is usually provided to data subjects and includes the following information:

  - details of the data controller;
  - the purposes for processing, including any non-obvious purposes (e.g. cross-mailing or host mailing);
  - details of any recipients of the personal data (e.g. other companies within the group) and their purposes;
  - an opt-out / opt-in for marketing, as appropriate.

RTC RT Coopers

PIPA

Data Protection Principles

- a description of the methods to be used for contacting individuals for marketing purposes (e.g. telephone, fax, SMS, email and/or mail); and
- any other information that is necessary to make the processing fair (e.g. whether it is obligatory to provide all the information requested or whether provision of some of that information is optional).

If personal data are kept beyond the specified purpose = breach

- Collection of personal data is important

RTC RT Coopers

PIPA

Data Protection Principles

Principle 3

Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they were collected

Principle 4

Personal Data must be accurate and, where necessary, kept up to date

- There must be a mechanism for ensuring that all personal data held are kept **up-to-date**

RTC RT Coopers

PIPA

Data Protection Principles

Principle 5

Personal Data must not be kept longer than is necessary for the purposes for which they were collected

- There is no specification as to how long to keep personal data

- Should have data protection policy
- Could follow time limit for financial documents
- For longer trials/studies – keep personal data for longer

Principle 6

Personal Data must be processed in accordance with the rights of data subjects

RT Coopers

PIPA

Data Protection Principles

Data Subjects' Rights

- The DPA lists the rights of data subjects:

  - the **right of access** to personal data;
  - the right to object to certain processing causing substantial damage or distress;
  - the right to object to automated decision taking; and
  - the right to object to direct marketing

- Most relevant – **Right of access to personal data**

  - An individual may request access to all personal data of which he or she is the subject and which is being processed by the data controller.
  - Data controller can require a fee
  - Data controller can require that request to be made in writing and to provide enough information to identify and verify the identity of the data subject making the request.

RTC RT Coopers

PIPA

Data Protection Principles

Data Subjects' Rights - The data controller must:

- Respond to request within **40 days**
- Amend personal data if ….
  - –Inaccurate or incomplete
  - –Processed unlawfully
  - –Kept for longer than necessary
- Cease processing if notified – within 21 days (Response) (Data Subject Notice)
- Cease processing – (Direct Marketing Notice)
- Limit decision-based on automated processing on request
- see *Michael John Durant v Financial Services Authority* – Lord Buxton held "think very carefully" before attempting to use the subject access provisions as a weapon of litigation

RTC RT Coopers

PIPA

Data Protection Principles

Data Subjects' Rights

- Any information that is not relevant to the data subject can be **redacted** from the documents that are provided to the data subject as part of a request

RT Coopers

PIPA

Data Protection Principles

Principle 7

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

PIPA

Data Protection Principles

Q

- What would constitute a breach?

- Email with wrong attachment
- Password to computer left susceptible to use
- Key left in cabinet
- Virus attack leading to loss of data
- Dumping unwanted personal data – i.e. not disposing correctly

RTC RT Coopers

PIPA

Data Protection Principles

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?

RT Coopers

PIPA

Data Protection Principles

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

PIPA

Data Protection Principles

- 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

PIPA

Data Protection Principles

- 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

PIPA

Data Protection Principles

Principle 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

Must ensure destination country has data protection laws as robust, if not more so, than UK!

- Transferring data to the US:

Some organisations sign up to the **Safe Harbor Agreement**

- Check whether the organisation to which you are transferring data signs up to the Safe Harbor Agreement
- If so, such organisations adhere to adequately rigorous data protection laws

RTC RT Coopers

PIPA

Data Protection Principles

Principle 8 – Case Study

If the company in Case Study 1 is conducting studies on Qnexa in the UK and sending the results, including data gathered from the participants, to be stored at a data centre in India.

Q
What extra obligations, if any, are there on the company's data controller?

RTC RT Coopers

PIPA

Case Study 2

Company B, based in the UK, decides to conduct Phase I clinical studies on a cutting edge new medicinal product in China. Company B briefly weighed up its options and acknowledged that China may possess a number of companies looking to replicate the product and/or gin access to its results. However, company B settled on China to carry out the studies as it is cheaper than Europe and easier to obtain study participants. The results of the studies are transferred back to the UK for analysis.

Q
What issues should be considered and addressed around the following:

- Data processing - Principle 1?
- The purposes for processing – Principle 2?
- Security – Principle 7?
- Data transfer – Principle 8?
- Anything else?

RTC RT Coopers

PIPA

Case Study 2

A

What issues should be considered and addressed around the following:

- Data processing - Principle 1?
  - Consent
- The purposes for processing – Principle 2?
  - Notification of purpose to participants
  - Adequate information provided?
- Security – Principle 7?
  - Security on site – risk of results going to competitors
  - Limiting access to data
  - Levels of security
  - Making data anonymous before transfer
  - Encryption

RTC RT Coopers

PIPA

Case Study 2

A

What issues should be considered and addressed around the following:

- Data transfer – Principle 8?
  - Checking adequate measures in place in China/adopted and enforced by laboratory used in China
- Anything else?
  - Data processing agreement/Data controller agreement

RT Coopers

PIPA

Specific Issues pertinent to Medical Information and Pharmacovigilance

- Confidentiality
- Back Ups
- Data Sharing
- Data Retention

RTC RT Coopers

PIPA

Specific Issues pertinent to Medical Information and Pharmacovigilance

- Confidentiality

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

- Back Ups

- 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

PIPA

Specific Issues pertinent to Medical Information and Pharmacovigilance

- Back Ups

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

But,

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

PIPA

Specific Issues pertinent to Medical Information and Pharmacovigilance

- Data Sharing

- What is data sharing?

- The Data Sharing Code of Practice
  - Guidance
  - How much weight is given to the Code?

- What is its relevance?
  - Who is the Code addressed to?
  - Especially applicable to Joint Working

  http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.pdf

RTC RT Coopers

PIPA

Specific Issues pertinent to Medical Information and Pharmacovigilance

- Data Retention (Principle 5)

Personal Data must not be kept longer than is necessary for the purposes for which they were collected

RT Coopers

PIPA

Case Study 3

A company is conducting post marketing studies on a medicine to comply with conditions placed on its marketing authorisation by the MHRA.

a. studies are conducted
b. research results are transferred outside the EEA
c. some data are anonoymised
d. researchers keep the results of the participants
e. company does not have a policy in place
f. the information is stored in computer of researchers with no security
g. company has some written procedures in place
h. records are out of date
I. company is notified
j. staff members are unaware of the DPA
l. it has no policies or security measures in place
m. most participants are unaware of the use of their data
n. some data are out of date

What is the likelihood of breach of the DPA?

What advice would you give to the company?

RT Coopers

PIPA

Case Study 4

An organisation involved in enlisting and referring participants for clinical studies, has created a database of participant' details and would like to market and/or sell the information to pharma looking to conduct post studies, including post-marketing studies. The organisation has a number of volunteers working for it as well as temporary and casual workers as well as permanent staff:

a. the database contains email addresses of the participants
b. no other identifiable details of the participants
c. no data protection policy in place
d. data is transferred outside the EEA

Q
What is the likelihood of breach of the DPA?
What advice would you give to the organisation?
Can the organisation sell the database in its current form?

RT Coopers

PIPA

Case Study 5

The organisation from Case Study 4 now has a website and it uses the website to attract new participants.

It keeps a database of all of the participants such as their names, addresses, religion, sex. It has not notified the participants individually that it holds the information, but it has a privacy policy on its website. Participants' records are never deleted, even when they no longer subscribe to the website. The organisation is planning to use the information to collaborate with an organisation in the USA.

What is the likelihood of breach of the DPA? What advice would you give to the organisation? What are the risks surrounding the organisation planning the collaboration?

RT Coopers

PIPA

Privacy Policy

A further consideration for the organisation in Case Study 5, as it operates online and collects participants' personal data, is a **privacy policy**

A **privacy policy** should be located on the organisation's website as it **collects and processes** participant's **personal data**

Purpose of Privacy Policy:

- To explain how personal data are **collected**, **intended to be used** and **stored**
- To explain the procedures in place to safeguard privacy
- Cookies

RTC RT Coopers

PIPA

Cookies

The **privacy policy** should detail whether the organisation's website uses cookies.

- The law on cookies has changed.
- EU Cookie Directive 2009/136/EC:
  - "*It is therefore of paramount importance that users be provided with* ***clear and comprehensive information*** *when engaging in any activity which could result in such storage or gaining of access*."

The crux of the legislation is that **sufficient information is provided to website users and the users have consented to the use of cookies**, **before cookies are used on websites**. In particular, website users should be provided with clear and comprehensive information about what the cookies are doing and what is being stored.

RTC RT Coopers

PIPA

Cookies

- Guidance from Information Commissioner's Office:

"*Consent must involve some form of communication where the **individual knowingly indicates their acceptance**. This may involve clicking an icon, sending an email or subscribing to a service. The crucial consideration is that the individual must fully understand that by the action in question they will giving consent*."

- Possible option – "**opt-in**"
  - Users/participants should provide consent and accept the use of cookies on a website
  - The organisation should state what type of cookies are used

RTC RT Coopers

PIPA

Cookies

- Types of cookies
  - Login cookies
  - Session cookies
  - Google analytics

Practical

Websites may need to be amended. E.g. a **pop-up box** may appear upon entering website seeking the user/participant's agreement to the use of cookies.

- Similar to the requirement to opt-in for marketing purposes, the following can be borne in mind:

- Do not use a "catch-all" phrase without an opt-in box
- There should be a clear line of consent
- Individuals must appreciate what they are consenting to
- Sufficient information should be provided in relation to the cookies

RT Coopers

PIPA

Risk Assessment - Best Practice

- Plan a series of audits/reviews to:
  - -Re/confirm appropriate controls in place
  - –Determine control effectiveness
  - –Identify non-compliances *etc.*
  - –Make useful recommendations
- Obtain clear management support
- Follow-up agreed actions
- Consider independent assessment
- 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.: DPA)

RTC RT Coopers

PIPA

Risk Assessment - Best Practice

- **Best Practice**
  - Making data anonymous before transfer
  - Instructing security expert to stress your security measures
  - Conduct regular audits
  - To have a privacy policy in place
  - Data Processing Agreement
  - Data Controller Agreement
  - Use data for purpose collected
  - Seek consent where appropriate

RTC RT Coopers

PIPA

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!**

RTC
RT Coopers

Further Information

RT Coopers Solicitors

Tel: 020 7488 9947
Switchboard 020 7173 6292
Fax: 020 7481 4197

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

THANK YOU

RTC
RT Coopers