Module: Web Development Issues
Unit: Legal Aspects of Web Development
Lesson: Privacy and Data Protection

Introduction

In this lesson we are going to look at issues concerning privacy - do we even have a "right" to privacy? And what can be done to protect our 'e-privacy' - in other words, our privacy whilst online?

We will see how the Data Protection Act 1998 and European Human Rights Act affect us in this area. We will look at two other important pieces of legislation: the Freedom of Information Act 2000, which gives us access to information held about us, and the Regulation of Investigatory Powers Act 2000, which updates the law on the interception of communications to take account of technological change. There are controversial areas within this Act, which many consider to be an invasion of our e-privacy.

think about it

But why should privacy be a concern to us? Surely only those with something to hide have something to worry about?

Take a look at this fictional online scenario to get you thinking: http://www.aclu.org/pizza (it needs sound).

feedback

Your reaction to the pizza scenario is obviously personal, but it is not too far-fetched to think that your personal information could be used in some similar way - there has been discussion for several years about whether insurance companies should use genetic data to determine the level of health cover they will provide to individuals - if someone is shown to have a genetic disposition towards, say, some form of cancer, the insurance company may choose to increase their premium because of this, or refuse to insure them at all.

This lesson does not seek to give "right" or "wrong" answers to all the questions it raises - but it is important that you think about the issues - as an individual and as a web designer. You will hold certain views, but your users may hold different views, and it is important to consider the issues from all angles.

The "Right" of Privacy

Most people consider that privacy is a fundamental aspect of human life:

"The quest and need for privacy is a natural one, not restricted to man alone, but arising in the biological and social processes of all the higher forms of life..." (Michael, James "*Privacy and human rights: An international and comparative study, with special reference to developments in information technology"* UNESCO publishing 1994).

Michael also states that privacy is generally thought of as a civil or political "right" but should perhaps be thought of as an economic, cultural or social "desire".

Despite this, as recently as the 1990s, English law did not provide a right to privacy. In 1991, Lord Justice Glidewell stated that: *"It is well-known that in English law there is no right to privacy, and accordingly there is no right of action for breach of a person's privacy..."*

In other words, someone could "invade your privacy" and there would not be anything the law could do about it.

Information Privacy

Information privacy is to do with the control of personal information - knowledge and information about ourselves.

Smith et al (1996) identified four major points of concern that members of the public have regarding corporate use of information. These are:

knowledge check

Collection

This refers to the concern that "extensive amounts of personally identifiable data are being collected and stored in databases". In other words, there is too much collection going on.

Unauthorised secondary use

People are concerned that "information is collected for one purpose but is used for another, secondary purpose."

Errors

This is the concern that "protections against deliberate and accidental errors in personal data are inadequate" - not knowing if what is collected is accurate

Improper access

Improper access refers to the concern that "data about individuals are readily available to people not properly authorized to view or work with this data". This would include access through hacking and organisations not restricting data access strictly to those who "need to know".

think about it

What personal information do organisations hold about you? Do you share the concerns listed above?

What would be the consequences for you if you were a victim of over-collection of data, unauthorised secondary use, errors or "improper access"?

feedback

You may have considered things like:

- Bank details, held by your employers, past and present, and by people with whom you have done business.
- Purchasing history at your local supermarket and other stores with loyalty schemes.
- Medical history - held by your doctor, insurance companies
- Credit card details held by companies you have used for mail order or internet shopping
- Information on your opinions and habits collected by organisations doing surveys
- Police records - motoring offences; records of security checks made by potential employers

There are many more examples.

Possible consequences could include, for example:

- Over-collection - increased risk of misuse.
- Unauthorised secondary use - increased "junk mail".
- Errors could result in you being refused credit, a mortgage or loan.
- Improper access - fraud or even identity theft.

There may be worse consequences - could incorrect information result in you being arrested for something you didn't do?

Rights to Information Privacy in Law

Do we have a "right" to privacy of information? Yes, thanks to the Human Rights Act 1998, which enshrines the European Convention on Human Rights in English law. In particular, the incorporation of Article 8 of the Convention creates a general right to respect for privacy which did not previously exist. Article 8 offers general protection for a person's private and family life, home and correspondence from arbitrary interference by the State.

top tips

ARTICLE 8 - RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Note that the right to respect for privacy under Article 8 is qualified. This means that interferences by the State can be permitted, but they must be justified and satisfy certain conditions.

Other protection for our privacy is provided by the 1948 Universal Declaration of Human Rights, Article 12, and to a limited extent in the Data Protection Act 1998, which we will cover later in this lesson. Also, the duty of confidentiality is enshrined in some professions, such as medicine and law.

However, the Regulation of Investigatory Powers Act 2000 could be said to erode these "rights" - more on this later.

Case Study: RFID Tags

An RFID tag is a small electronic device which responds to radio signals sent to it. The device can be made into a "smart tag" or smart label, and attached to an object, typically an item, box or pallet, or even a person. It can then be read remotely (by a "reader") to determine what or where the object is. The data obtained is fed to a host computer. Most RFID tags are passive devices, i.e. they respond to a signal (on the right radio frequency).

More information is available here: http://www.rfidc.com/docs/introductiontorfid_technology.htm

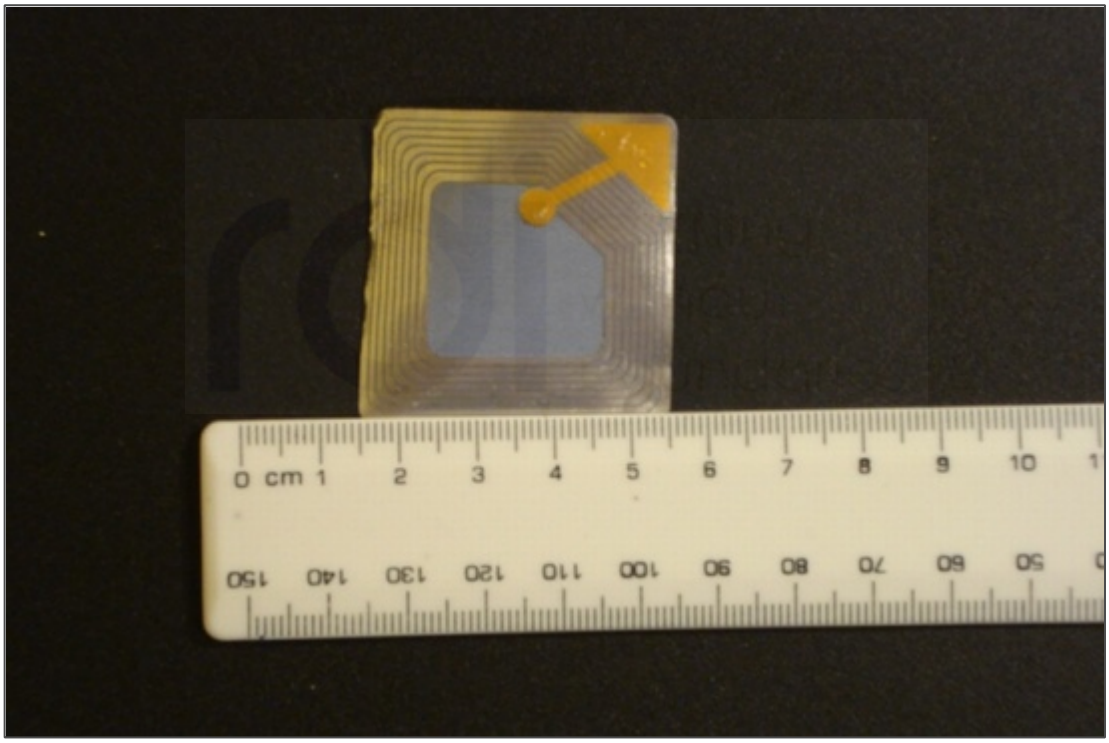

Figure 05.03.01 - RFID Tag

At a first look, RFID tags can be seen to fulfil many of the functions of barcode labels, but with the advantage that the tag can be read remotely, without needing a direct line of sight between the reader and the label. RFID tags are very widely used like this for tracing and monitoring a wide variety objects:

- The US Department of Defence is using RFID to trace military supply shipments,
- They are used by many shops to manage the supply chain.

Some uses, however, have raised concerns about the potential impact on a person's privacy.

- An Australian casino placed 80,000 RFID tags in employees uniforms;
- Michelin tyres plans to put RFID into car tyres linked to the VIN of the vehicle - this is good for tracking thefts, but could also be used to track someone's movements;
- An RFID tag is also to be placed in Euro notes - this could be used to monitor the entire 'journey' of each individual note!

- Delegates at the Chinese Party Congress were required to wear an RFID equipped badge at all times to track their movements.

A company called *Applied Digital Solutions* has designed a RFID tag called the VeriChip that is designed to be implanted under the skin, similar to the microchips sometimes used for pets. The proposed use is for vulnerable people such as children and Alzheimer's patients - but the implication of such technology is huge!

Useful links:

http://news.bbc.co.uk/1/hi/technology/4247275.stm

http://www.privacyrights.org/ar/RFIDposition.htm

think about it

What do you think about the uses given above for RFID tags? What are their good points? Are they all examples of good use of information technology? Shining examples of progress? Or do any of them make you feel uneasy? Can you see potential for misuse, criminal, political or otherwise?

feedback

This is one "Think About It" which cannot be answered here - your reaction will be personal. But it is important to think about it. Perhaps you could discuss this issue on the Discussion Forum.

The University of Washington is engaged in a project to look at the use of RFID tagging. It is testing a system that allows participants to follow others' movements around campus.

"The overarching goal of the project is to inform the community...of the risks, benefits, and challenges of user-centered RFID systems while proposing technological solutions whenever possible - *and to do so before such systems become commonplace*." http://rfid.cs.washington.edu/

Privacy & the Law - The Data Protection Act 1984

The Data Protection Act of 1984 was finally given royal assent in 1984 after twenty years of campaigning.

The Government was forced into passing the Act because of the 1981 European Convention for the Protection of Individuals with regard to Automatic Processing of Data. The adoption of this convention meant that the United Kingdom would not have been able to trade with the EU without some kind of data protection in place. It could therefore be said to be an economic piece of legislation and nothing to do with protection of privacy!

The Act gives protection to personal information or data, rather than privacy in general.

European Union Data Protection Directive, 1995

This directive was formally adopted by the EU Council of Ministers in 1995. It was important for two main reasons.

First, it established a Europe-wide set of legal principles for privacy protection, to be enacted in all EU member states.

Second, it prohibited the transfer of personal data from EU countries to any countries which do not have 'adequate' data protection laws.

The UK Government was not wholly in favour. The Home Secretary at the time, Michael Howard,

"spent much of 1994 lobbying his opposite numbers in Europe to have the new European law derailed. He almost succeeded. The directive passed through the Council of Ministers in February with Britain in opposition" (Davies, Simon "Big Brother: Britain's web of surveillance and the technological order" 1996).

Article 1.1 of the directive states:

"In accordance with this directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".

As we saw in lesson 1 International Aspects, EU law becomes part of UK law. The 1995 Directive led to the 1998 Data Protection Act, which is a modified version of the previous Act, and is an important piece of information legislation.

The Data Protection Act 1998

The new Data Protection Act 1998 came into force on 1st March 2000. The main differences and enhancements to original 1984 Act are:

- Data controllers have to register, and make their registration details public.
- Data security has been tightened: "appropriate technical & organisational measures must be taken to prevent the unauthorised or unlawful processing or disclosure of data."
- Access to information held - you can now find out not only what data is held about you, but also the purposes for which it is being processed, and a description of potential recipients of the information. You also have the right to prevent the processing of data which is likely to cause damage and distress, the right to know the logic behind automated decisions and the right not to have significant decisions based solely on the results of automatic processing - an example of this could be using automatic psychometric testing to make a decision on whether or not to employ someone.
- The Act "considerably extended" the right of an individual to claim compensation for damage caused by any breach of the Act.
- Organisations can only transfer data to non EU member countries if there is an "adequate level of protection".
- Some types of 'manual' data (paper file systems) are now also covered.

my learning space activity

Think about the personal data your organisation keeps, on you and on others.

- What types of information are held?
- What is it used for?
- What safeguards are in place to keep the data secure and ensure it is accurate?

feedback

You may have considered information on employees (past and present) such as name, address, date of birth, qualifications, training and other personnel records. Bank details may be held by payroll, along with national insurance numbers, used for tax and national insurance calculations.

You may also have considered information held on your customers and clients. This would vary depending on the type of organisation, but could include names, addresses, perhaps credit card details, personal preferences, purchase history and so on. Data like this could be used for order processing, marketing and forecasting.

Every organisation will also have its financial records and forecasts.

Typical safeguards include using passwords, virus protection, firewalls and regular back-ups. You may include physical protection such as security locks and alarms, and protection from fire damage. Perhaps you also considered disaster recovery.

The information commissioner's office has a special note about information held on laptops:

"Where the information held on a laptop or other portable device could be used to cause an individual damage or distress, in particular where it contains financial or medical information, they should be encrypted...if it is brought to the Commissioner's attention that laptops that have been lost or stolen have not been protected with suitable encryption he will consider using his enforcement powers." (http://www.ico.gov.uk)

Have you identified any gaps for your organisation?

The Data Protection Act 1998

Three important definitions from the Act:

1. "Data controller" means a person who determines why and how any personal data is processed;
2. "Data subject" means an individual who is the subject of personal data;
3. "Personal data" means data which relate to a living individual who can be identified from the data held.

If you are a "data controller" you must notify the Information Commissioner in order to be placed on the public register. In 2007 it cost £35.00 per year to be placed on the register.

research activity

What are the "Eight Principles" of the Data Protection Act 1998 and what does each one mean?

What are the implications of the eight principles for your own organisation (or one with which you are familiar)?

feedback

The eight principles:

Personal information must be...

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to other countries without adequate protection

More information can be found at the website of the Information Commissioner's Office

http://www.ico.gov.uk

You will have considered the specific implications to your own organisation, but if you are required to comply with the Act, you have a number of legal responsibilities:

- to notify the Information Commissioner you are processing information, unless you are an organisation who has personal information only for:

1. staff administration (including payroll);
2. advertising, marketing and public relations for your own business; or
3. accounts and records (some not-for-profit organisations)

- to process the personal information in accordance with the eight principles of the Act; and

- to answer subject access requests received from individuals.

Data protection principle 7 (the security principle) is particularly important - data must be kept secure (for instance, from loss, damage or theft). This requires organisations to put various measures in place,

Identity theft is a growing problem, and organisations are expected to keep personal data safe and secure.

think about it

What organisational, administrative and technological measures would an organisation need to implement in order to satisfy this principle?

feedback

Appropriate measures could include

1. physical protection (e.g. Locks)
2. access protection (e.g. security codes, password protection)
3. encryption of the data in some cases

This is only a short list of possible measures. There are others possible, depending on the nature of the organisation and the data it holds.

The Durant Case 2003

As always, case law has been used to clarify aspects of the legislation.

The background to this key case concerns a Mr M. J. Durant. In the late 1990s, Mr Durant began litigation against Barclays Bank, alleging he had been the victim of fraud. He was unsuccessful, but referred the matter to Financial Services Authority (FSA). They investigated, but closed the case without taking action against the bank.

Mr Durant then requested access to personal information held by the FSA (Mr Durant wanted to access the FSA files to see whether they contain information concerning the alleged fraud.)

The FSA argued that the information, although personal, was not subject to the right of access. Mr Durant then used section 7 of the DPA to force the FSA to disclose to him information regarding his complaint. The FSA disclosed some of the information requested, refused to disclose other information and "redacted" (censored) other information (in order to protect the right of others who could be identified by this information).

The case went to Court of Appeal. The judge's ruling is important because it clarified:

- What data is "personal" within the meaning of the DPA, and
- What is meant by a "relevant filing system" in relation to manual files

knowledge check

Personal Data

The Court of Appeal concluded that data will relate to an individual if it: "is information that affects" a person's "privacy, whether in his personal or family life, business or professional capacity". They ruled that merely mentioning a person's name in a document does not amount to personal data.

Relevant Filing System

The ruling said that the Act could only apply to manual files if they were organised in a sophisticated and structured manner, to resemble the organisation of a computer file. A rule of thumb test for this would be whether someone with no particular knowledge of an organisation's type of work or the documents they hold would be able to extract specific information about an individual (the "temp test").

Link to the judges' ruling on this important case:

http://www.hmcourts-service.gov.uk/judgmentsfiles/j2136/durant-v-fsa.htm

Regulation of Investigatory Powers Act, 2000

The Regulation of Investigatory Powers Act, (RIP Act) "updates the law on the interception of communications to take account of technological change such as the growth of the Internet."

Critics say the Act is a gross invasion of privacy which will destroy e-commerce in Britain; the government argues it is necessary to crack down on internet crime, terrorism and paedophilia.

The Act is in three parts:

knowledge check

Interception and access to communications data
This section allows law enforcement and security agencies, such as MI5, to monitor internet traffic through the collection of "communications data". This does not mean the actual content of websites or emails, but the "clickstream" left by users - in other words, the websites and chatrooms they visit and the addresses of emails they send and receive. If security services suspect someone of criminal activity, they can request a government warrant to intercept and decode the internet content.

UK internet service providers (ISPs) must "maintain a reasonable intercept capability".

The Home Office has said the Act brings the monitoring of the internet in line with that of telephone calls. However, web addresses also show exactly what people have been looking at and build up detailed profiles of where people go online and who they communicate with, which is not true of telephone records.

Surveillance and covert human intelligence sources
This section regulates the surveillance techniques that have been used for many years. However, it specifically allows security services to keep their surveillance methods secret.

Encryption
This section "provides new powers to help combat the threat posed by rising criminal use of strong encryption." It "requires any person to provide a decryption key or the plain text of specified material in response to an authorised written request". In other words, the RIP Act gives powers to demand decryption of any message or data, whether or not a person is suspected of any crime. This section was only activated in October 2007.

top tips

Encryption means converting information into a form which cannot be understood by anyone except holders of a specific "cryptographic key". Decryption is the inverse of encryption. Encryption is used to prevent unauthorised access to data.

Criticisms of the RIP Act

There have been many criticisms of the Act. Some observers have commented that it was rushed in by a parliament which did not actually understand it. In 2003, Lord Phillips of Sudbury told a Parliamentary meeting that neither backbenchers nor government ministers fully grasped the Regulation of Investigatory Powers Act.

Others have claimed that the act is so badly worded that it is unenforceable. Still others believe it to be a breach of the Human Rights Act and an attack on civil liberties. In the light of the events of September 11th 2001, the government is now pressing for increased use of surveillance, and the RIP Act becomes even more significant.

RIP Act - Areas of Controversy

1. "Black Box" Interception

ISPs have "to maintain a reasonable intercept capability" - in other words, they must install computer technology that allows the monitoring of flow of data i.e. websites & chat rooms visited, addresses of emails sent and received. Critics have said that the legislation was rushed in without proper consultation or consideration of the technological logistics.

2. Reverse Burden of Proof

In English law, the accused is innocent until proven guilty. Some claim that the RIP Act reverses this burden of proof, and requires the accused to prove his innocence.

If communications are encrypted, the Act can force individuals to surrender the encryption key. If they do not, they could receive a two year jail sentence, or up to five if they are suspected of terrorism or paedophilia offences. The implication is that the authorities are assuming that the encrypted material is of an illegal nature.

It is an acceptable defence to have genuinely forgotten the key - but this is clearly very difficult to prove. Individuals can also go to jail if they tell someone else that they have been asked for the encryption key!

This section may not even be particularly effective - some criminals would probably quite happily accept a two year sentence if it is less than that for the crime of which they are suspected.

3. Employers right to intercept employees' email

The Act also allows employers to intercept emails and internet use by their staff, on grounds such as monitoring for computer viruses.

4. Compromise of e-commerce

Some are concerned about the effect of the Act on UK business. A British Chambers of Commerce report estimated the Act could cost business £46bn in the first five years of operation. It is possible that the legislation could dissuade e-business from setting up in the UK.

research activity

Use the internet to research news items about the RIP Act. For instance, what sort of prosecutions has the Act resulted in?

group learning activity

For this activity, you will need to organise yourselves into groups on the discussion forum, to debate a privacy topic.

"**We are sleepwalking into a surveillance society"**

Richard Thomas, UK Information Commissioner (Aug 2004)

This group activity takes the form of an online debate in which you will have to argue either in support of or against the above statement.

Ideally, you will need around 4-6 people in your group. If you were born between January and June, you will be arguing in **support** of the statement. If you were born between July and December, you will argue **against** the statement. It doesn't matter what your real opinions are (for this activity, anyway!) - even if you feel you are arguing for the "wrong" side it will be useful as you will then be able to see both points of view more easily.

Click the appropriate link below to obtain the briefing material for the discussion:

See **Your birthday January-June - You are arguing "for"** at the back of this lesson booklet.

See **Your birthday July-December - You are arguing "against"** at the back of this lesson booklet.

If you really cannot find a group of learners to debate this issue with, then instead, create powerful supporting statements for BOTH points of view, on your own if necessary. Or maybe you could involve your friends and family - privacy affects us all.

Hacking - a threat to privacy?

We considered hacking in lesson 2, defining it there as illegal or unauthorised accessing of a computer system, network or accounts without the permission of the owner of that computer system.

Hackers may include those programmers who say they are acting altruistically - for the wider good - by investigating security loopholes, and "crackers" - those who "crack" (find ways around) security features. They may not be malicious themselves but, in publicising their findings, they may leave a system open to those who are. Then there are those who commit further offences such as credit card fraud and misuse of the telecommunications system.

Hacking can therefore be seen to have implications for privacy. Any system holding personal data is a potential target for hackers. Bainbridge, D (2004) gives a useful analogy:

"In the days before computers, sensitive information was kept locked away in filing cabinets in a locked room...By contrast, information stored on a computer that is linked to a telecommunications system [is like locking the cabinet but leaving it] in a public place. It is just a matter of finding the right key to fit the cabinet."

Those who hack with malicious intent are unlikely to be deterred by strengthening criminal law, so it is essential that those responsible for compute systems do everything possible to make the systems as secure as they can.

Freedom of Information Act, 2000

The Freedom of Information Act deals with access to official information. It aims to address some privacy concerns by giving individuals or organisations the right to request information from any public authority. Under the Act,

(1) Any person making a request for information to a public authority is entitled -

(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and

(b) if that is the case, to have that information communicated to him.

(http://www.ico.gov.uk/what_we_cover/freedom_of_information.aspx)

As always, there are exceptions to what information must be disclosed, and there have been recent moves to exempt Members of Parliament from obligations under the Act, with an amendment to the Act having been debated in Parliament in Spring 2007. One justification for this is to protect the confidentiality of MP's correspondence from their constituents. However, this amendment is now unlikely to go ahead in its current form, with further consultation being planned instead.

There are many implications of the Freedom of Information Act, but in the context of this lesson, it can be seen to allow individuals access to information held about them, which goes some way to addressing the four points of concern identified earlier in the lesson, particularly allowing them to check the amount of data held and its accuracy.

knowledge check

To complete this knowledge check activity, see the Knowledge Check section at the end of this lesson.

knowledge check

To complete this knowledge check activity, see the Knowledge Check section at the end of this lesson.

knowledge check

To complete this knowledge check activity, see the Knowledge Check section at the end of this lesson.

knowledge check

To complete this knowledge check activity, see the Knowledge Check section at the end of this lesson.

Knowledge Checks

Module: Web Development Issues
Unit: Legal Aspects of Web Development
Lesson: Privacy and Data Protection

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

Privacy and Data Protection - Page 14

knowledge check

Which Act incorporated the European Convention on Human Rights into English Law?

- Data Protection Act 1998
- Human Rights Act 1998
- Regulation of Investigatory Powers Act, 2000
- Freedom of Information Act, 2000

Please choose which of the answers above is correct.

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

Privacy and Data Protection - Page 14

knowledge check

What is a "Data Controller"?

- A powerful computer containing personal information
- A government position with responsibility for overseeing data protection
- Someone who has personal data about them stored on a computer
- A person who determines why and how personal data is processed.

Please choose which of the answers above is correct.

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

Privacy and Data Protection - Page 14

knowledge check

Which of the following statements about RFID tags is true?

- They can be implanted under the skin
- They require a battery to power them
- They must be scanned by a laser scanner to read them
- They are too heavy to be worn on clothing

Please choose which of the answers above is correct.

Privacy and Data Protection - Page 14

knowledge check

Which of the following is NOT a way of protecting personal information?

- Password protecting a file
- Using encryption
- Using registered mail to send computer discs through the post
- Keeping back-up tapes in a locked fire safe

Please choose which of the answers above is correct.

Knowledge Checks - Solutions

Module: Web Development Issues
Unit: Legal Aspects of Web Development
Lesson: Privacy and Data Protection

Privacy and Data Protection - Page 14

knowledge check

Which Act incorporated the European Convention on Human Rights into English Law?

- ✗ Data Protection Act 1998
- ✓ Human Rights Act 1998
- ✗ Regulation of Investigatory Powers Act, 2000
- ✗ Freedom of Information Act, 2000

Please choose which of the answers above is correct.

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

Privacy and Data Protection - Page 14

knowledge check

What is a "Data Controller"?

- A powerful computer containing personal information
- A government position with responsibility for overseeing data protection
- Someone who has personal data about them stored on a computer
- A person who determines why and how personal data is processed.

Please choose which of the answers above is correct.

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

Privacy and Data Protection - Page 14

knowledge check

Which of the following statements about RFID tags is true?

- They can be implanted under the skin
- They require a battery to power them
- They must be scanned by a laser scanner to read them
- They are too heavy to be worn on clothing

Please choose which of the answers above is correct.

You can contact us on
02476 765 15700
International: +44 (0) 24 765 15700

Privacy and Data Protection - Page 14

knowledge check

Which of the following is NOT a way of protecting personal information?

- Password protecting a file
- Using encryption
- Using registered mail to send computer discs through the post
- Keeping back-up tapes in a locked fire safe

Please choose which of the answers above is correct.