CAPITA
LEARNING & DEVELOPMENT

Group Risk

Security Awareness Training 2010 – 2011

Data Protection Awareness

CAPITA
LEARNING & DEVELOPMENT

Table of contents

CAPITA
LEARNING & DEVELOPMENT

1. Background

Meet Emma.

“At first, I didn’t really grasp the extent of it … When my credit card company called me to ask me whether it was me who had booked airline tickets over the phone for four flights, it was clear that somehow my credit card had been used without my knowledge. But how? It had never been out of my sight. As the weeks went by, it turned out that someone had my passport, my driving license … Had taken over my bank and savings accounts … and had crashed in my insurance policy. Every day, some other piece of my life seemed to fall apart as I learned of another fraud committed in my name. My whole identity had been hijacked. Of course, I had read about situations such as these, but I had dismissed what I had read. You never really think it could happen to you. But it did happen to me. In fact, it happened to hundreds of others too. And it could just as easily happen to YOU!”

2. Introduction

Emma is a customer services assistant for a retail bank. She has fallen victim to financial crime. A fraudster has spent money on her credit card, taken over her bank, savings and other accounts and stolen her identity. Your task in this learning module is to uncover how the data protection act is designed to protect our personal information. During this module, you will learn that:

- Emma disclosed her personal information when making an on-line purchase
- Personal information has value
- All organisations must tell those about whom it collects personal information why it wants that information and what it proposes to do with it once it has it.

As you walk down the street on the way to the office one morning, the breeze picks up and you notice how much paper is suddenly flying around. Scraps of paper, whole sheets and what looks like documents are flying around in the breeze. A sheet of paper from a jotter falls at your feet. You pick it up and look at its contents: At the top of the paper is your company logo. You realise that leaving this on the street poses two threats. Someone could make purchases using Emma's credit card details and so defraud her; the paper could end up in the hands of a newspaper or TV news show, which could seriously damage your company.

You also find:

- a financial analysis of insurance claims
- candidates' CVs and applications for jobs
- names and salary details of employees.

You decide to take the papers back to the office. You collect as much paper as you can and inform security. You know what you have just discovered is potentially damaging; both to customers and the business.

You can't believe it. You are reminded of so many similar losses of personal information that have been reported in the news in recent months.

3. What's in the news?

For each of the following, decide which you think are true and which are false:

1. **Mortgage company accidentally discloses the records of over 15,000 clients.**

True
In February 2010, a mortgage company disclosed records of more than 15,000 customers, including personal information relating to individuals' arrears or possession proceedings. The database was sent by an employee by email with neither encryption nor password protection. It was intended for a consultant's personal email account but an error on the part of the sender meant that a member of the public with a similar email address to the consultant received the database instead. It is not difficult to see why emails can be mis-sent; the replacement or omission of just one letter in an email address can mean a document goes off to the wrong person. That this database was not encrypted meant that had it fallen into unscrupulous hands, thousands of customers would have been at risk of fraud. Once you've 'hit' send, it's gone! When sending emails containing personal or confidential information, follow the Group Information Security Policy and Dos and Don'ts on Internet and Email. Always ensure such information is encrypted.

2. **Social work records found in second-hand filing cabinet.**

True
In January 2010, duplicates of social work records held in the council's offices were found in a second hand filing cabinet. They had apparently been used by a social worker during active casework duties. The files contained an extensive amount of personal data including information about the ethnicity, religious beliefs and physical or mental health conditions of individuals. In one instance, the data provided an almost complete picture of the individual's life. This is just one of many examples of personal files being left in old filing cabinets and removed from offices during office moves and refurbishments. They typically end up in second-hand office furniture shops. If they are discovered by honest people, they are usually returned, (though sometimes via the media which then causes damage to reputations). It is just as easy for files left in old filing cabinets to end up in unscrupulous hands and for people to be caused distress and financial loss as a result. Copying information in any format increases the risk of it going astray.

3. **Major UK Financial Services firm fined £3.26m for failing to protect customers' personal information.**

True
In July 2009, large volumes of unencrypted customer details and confidential information about customers were sent by this firm via post or courier to third parties. An investigation also revealed that confidential customer information was also left on open shelves or in unlocked cabinets which could have been lost or stolen. Sending confidential information by post if it has not been encrypted is highly risky. Even sending it by recorded delivery only guarantees that it will be signed for if it is delivered. Recorded delivery is not a guarantee of delivery. As you walk around the office, how much confidential information can you see lying on open shelves? Is it customer information? Is it about colleagues? Is it business sensitive, (i.e. that if a visitor saw it, it could subsequently damage the business in some way)?

Follow the Group Information Security Policies and Dos and Don'ts on Office Working and ensure you never leave confidential or sensitive documents unattended, whether on desks, printers or in meeting rooms.

4. **Major UK Building Society fined just under £1m after personal information about thousands of customers was stolen.**

True
In February 2007, thousands of this building society's customers' personal information was stolen from an employee's laptop which he had taken home. The building society was unaware that the stolen laptop contained customers' confidential information until three weeks after the theft, so customers were left at risk for an extended period of time.

A general rule of thumb is that if it cannot be encrypted, it should not be removed from the office, as people are put at risk if that information is lost or stolen. The failure of this building society to discover that customers' confidential information was on the laptop was highlighted by the Financial Services Authority. For three weeks, neither the building society nor its customers did anything to protect those who had inadvertently been put at risk. If personal information about customers or colleagues goes missing, it must be reported immediately. Immediate reporting means that organisations are able to put in place plans to inform customers and to take steps to minimise any risk. Any delay is a fraudster's delight!

5. **British intelligence officer lost a memory stick full of secret information.**

True
In April 2009, a British intelligence officer lost a memory stick full of secret information including the names, code names, addresses and operational details of dozens of intelligence officers and confidential informants that she had downloaded from computer systems at her office. The loss risked the lives of undercover agents and informants who subsequently had to be relocated. As well as the risk to agents' and informants' lives, the total cost of aborted operations was put at £100m. Copying any confidential information to USB sticks or removable drives has become the norm in recent years, rather than the exception. These too easily go missing. As a general rule of thumb, if it can't be encrypted, it should not be copied. This example shows that the consequences of information loss can, in certain circumstances, be life threatening. It also shows that however well trained we may be in keeping secrets, our behaviour can inexplicably lapse and we put thousands of people at risk. Avoid copying data; avoid the problem.

6. **Twelve of Britain's leading banks and financial institutions dump personal details of their customers in outdoor rubbish bins.**

True
In March 2007, twelve of Britain's leading high street banks were rebuked for dumping personal details of their customers in outdoor rubbish bins. Details included cut-up credit and debit cards, money deposit details, bank account information, printouts showing direct debit and bank giro credit information, receipts showing signatures of payees and full details of Switch/Maestro cards, travel insurance application forms, passport details with names and phone numbers, and money transfer forms. Since 2007, there have been no further criticisms by the Information Commissioner's Office of banks for losing information in this way, but financial services firms have been the subject of heavy fines more recently for

losing customer information in other ways. Ordinary refuse bins are not for company confidential or personal information. Always follow the Group Information Security Policies and Dos and Don'ts on Office and Home Working and dispose of confidential material safely in the secure disposal bins that are provided in every office. If you are in any doubt as to whether material contains confidential or personal information, dispose of it in the secure disposal bins as a precaution.

7. **Sensitive personal information about 7 million families lost in the post.**

True
In October 2007, a government department lost 25 million child benefit records, (i.e. 7 million families), complete with sensitive personal information. The information had been despatched on a CD by the post. Sending personal information in the post, whether recorded or not represents a high risk to the people whose information is being transferred, as well as to the business. Sending large volumes of personal information on a CD in the post should be avoided. Any information copied to a CD, whether it is to be transferred or not should be encrypted so that it does not later end up in a disused filing cabinet and become the property of a fraudster.

8. **38,000 patients' details lost or stolen over a one year period.**

True
Patients' records are lost or stolen every time an NHS or similar laptop or PC is lost or stolen. Not all personal information leaves individuals vulnerable to identity theft or fraud. Patients' become vulnerable to serious distress if their medical records are divulged, either inadvertently, (e.g. to family members, when the patient would prefer their family members not to know about their conditions), or if they are lost and stolen for anyone to read. All personal and confidential information should be treated with the utmost respect.

9. **Personal details of thousands of members of a UK professional association are lost.**

True
In February 2010, personal details of thousands of members of a UK professional association were lost when a laptop and memory stick were stolen. The laptop was the property of the professional association and although not encrypted, was password protected. The memory stick, which belonged to a staff member, was neither password protected nor encrypted and contained thousands of the same records as were held on the laptop. Both laptop and memory stick were stolen from the roadside as the member of staff was loading his car. Criminals are constantly on the lookout for people just to take their eyes off their possessions for a moment. Thousands of members of this professional association were put at risk though this staff member's momentary lapse. Never copy data to unencrypted USB memory sticks, drives or CDs. Once copied, the chances of that data falling into unscrupulous hands increases.

Unless you have been given explicit written permission from the customer and senior Capita management to do so, never copy customer data onto removable media such as CDs, DVDs or USB memory sticks. If you are given permission, follow Group Information Security

Policies and Dos and Don'ts on removable media and ensure removable devices, like laptops, are encrypted.

Personal information – why we need to protect it

Millions of people in the UK are put at risk of fraud and identity theft each year, not by a few stupid people, but by millions of ordinary people who have never thought of the consequences of failing to protect their own personal information, their colleagues' or their customers'.

When we hand over our personal information to organisations, whether they are retailers, financial services firms, providers of on-line goods and services, clubs, societies, transport operators, airlines, utilities companies, doctors, hospitals, health trusts, the local council, we trust them to protect our information once they have it.

Legal framework

Aside from the ethical considerations, the Data Protection Act 1998 is there to provide a legal framework within which organisations are legally obliged to protect the privacy of their customers and colleagues and to protect them from financial and personal damage caused if information falls into the wrong hands.

The Data Protection Act 1998 enshrines in law, eight data principles with which we are legally obliged to comply and which are designed to protect individuals' personal information.

Financial penalties

From April 2010 the Information Commissioner's Office (ICO) has new powers to impose financial penalties of up to £500,000 on firms who fail to comply with the eight data principles enshrined in the Data Protection Act. These new powers are in addition to the ICO's existing powers to order organisations to pay compensation to the individuals affected by a breach or to extract public undertakings, which acknowledge breaches and commit organisations to better future compliance. Criminal convictions under the DPA can attract an unlimited fine.

In determining the seriousness of a breach and therefore whether or not to impose a fine, the Information Commissioner has said that a number of circumstances will be considered including:

- the likelihood of substantial damage and distress caused to individuals as a result of the breach
- whether the breach was the result of negligence or a deliberate act
- what reasonable steps had been taken by the organisation to prevent breaches.

All of us, wherever we work in our business, have a personal responsibility to protect the personal information of our clients, their customers and our colleagues.

4. The Value of personal information

So why do people hand over their personal information in the first place?

Buying goods
Because we want to buy goods (and maybe have them delivered), on the high street or on-line.

Applying for finance products
Because we need to open a bank account, a credit card account, or obtain other financial services such as life insurance, health insurance, home insurance, motor insurance, or apply for a mortgage

Networking
Because we want to network with others across the world.

Loyalty cards
Because we want to apply for a loyalty card to collect points or miles.

Offers and prizes
Because we want to take advantage of an offer, enter a prize draw.

Electoral roll
Because we want to be on the electoral roll.

TV license
Because we need a television license.

Paying bills
Because we want to pay for our gas, electricity and telephone bills by direct debit and possibly record our meter readings on-line

Travel cards
Because we need an Oyster Card for travel around London.

Registering with health providers
Because we wish to register with a local GP surgery, arrange a visit to see a medical or surgical specialist, go the dentist or the optician.

Summary
The list is endless. And the more people we give our personal information to, the greater the chance someone will lose it.

But we give our personal information freely to all these and more people and have a right to expect they will protect it as if it was bars of gold! Often, however, we don't check what they are going to do with our personal information before we give it.

Now consider this scenario:

Emma was looking for a great deal when booking a five star weekend away to the Lake District on a website. She narrowed her search down to just two choices.

ABC Travel
Through 'ABC Travel' Emma was able to secure a 5% reduction on the advertised rate, from £295 per person including breakfast and evening meal for two nights, to £285.25 per person, all payable in advance. ABCs terms and conditions of booking stated that they required Emma's name, billing address, contact telephone number, credit card details and dates/times of travel to be entered via their secure website. ABC provided a contact number which Emma could call should she have any queries. They promised to use her personal information purely to:

- manage the processing of her purchase
- conduct statistical analysis within the company
- prevent and detect fraud
- manage debt.

They also promised not to share their information with any 3rd parties, use it for marketing purposes or disclose it to any other body unless they were required to by law. They would only keep Emma informed of products, services or offers if she ticked the box specifically requesting that they do so.

XYZ Travel
Through XYZ Travel, Emma was able to secure a staggering 60% reduction on the advertised rate, from £295 per person including breakfast and evening meal for two nights, to £118. A deposit of £35 per person was payable immediately with the balance due two weeks before the date of arrival at the hotel.

XYZs terms and conditions of booking stated that they required Emma's name, billing address, contact telephone number, credit card details and dates/times of travel to be entered via their secure website. In addition to using her personal information to manage the processing of her purchase, to conduct statistical analysis within the company, to prevent and detect fraud, and to manage debt, they and their group of companies would share and sell her personal information with third parties for marketing purposes, would contact her with details of products, services and offers, unless she specifically requested that they did not do so in writing, and would reserve the right to pass her information to third parties for processing, some of which might be outside the EEA, (that is the European Union plus three other countries).

Furthermore, they might sell Emma's debt to debt recovery agencies and so pass her details to debt recovery agencies who may themselves sell her information to third parties. XYZ also required that Emma answer certain market research questions, providing them, for example, with the number of people in her household, her age (from a range), her marital status, her salary (from a range), her occupation, whether she had any pets and if so, what they were and what were their names. They requested she provide her mother's maiden name which would be used by them as the answer to a secure question in the event she contacted them by phone. Should she not wish to receive any marketing material, all she need do was to contact XYZ Travel and their third parties to let them know.

Based on the information about each company, decide which one you would choose.

ABC Travel
You might be paying more, but you are protecting your personal information from being transferred to third parties. The fewer people have access to your information, the lower your risks are of fraud. ABC will process your booking itself, will not divulge information to third

parties or sell it for marketing purposes. Look what could happen if you had chosen XYZ Travel instead.

XYZ Travel
You have agreed to XYZ transferring your personal information to a third party to process your booking. They can also transfer it to a debt recovery agency, overseas to countries with less robust data protection, and third parties for marketing purposes. XYZ Travel's wording means they can legitimately copy your information countless times – each time another organisation receives it, you are at risk. By choosing XZY, you are valuing your personal information at just £107.

Why do they want personal information?

Most of us fail to read the small print when we sign up to make our purchases, join mailing lists, join social networking sites and subscribe to special interest groups. In fact, most of us find it irritating when we are asked to accept the terms and conditions, (where their policies about data protection and privacy are usually to be found).

We quickly acknowledge we do accept terms and conditions without opening them. These are, after all, reputable sites! Everyone uses them! There's no need to worry! You might remember to tick the box that says *'No marketing materials, please'*, but do you have any idea why they want your information, what they plan to do with it once they have it, or how they will dispose of it once they have used it?

So what do you need to know?

There could be any number of reasons why legitimate organisations want your personal information, including to:

- Process your transaction, e.g. payment / delivery of goods and / or services you are purchasing
- Manage your account, (e.g. your bank account, membership of a group or organisation
- Carry out market research
- Find out more about you.

For most legitimate uses, organisations do not, however, need to know absolutely everything about you!

What will they do with it once they have it?
Again, there could be any number of things legitimate organisations may want to do with your personal information, including to:

- Process your information themselves, (e.g. monthly bank or credit card statements, payment and / or delivery of mail-order items, etc)
- Transfer your information, e.g. by email, hard copy or removable media, or by secure electronic means to third parties in the UK for processing, (e.g. monthly bank or credit card statements, payment and / or delivery of mail-order items, etc)
- Transfer your information, e.g. by email, hard copy or removable media, or by secure electronic means to third parties outside the UK for processing, (e.g. monthly bank or credit card statements, payment and / or delivery of mail-order items, etc)
- Store it with third parties.

All organisations that collect, process, store and dispose of personal information are legally obliged to tell you:

- What information they want you to provide
- Why they want it
- What they will do with it once they have it.

They tell you in what is called a '*privacy notice*' and these are usually tucked away in the terms and conditions or in the privacy policy on the organisation's website. If you accept the terms and conditions, you are authorising them, under the Data Protection Act to use your information in the ways they have described. They breach the Act if they do not follow the privacy policy they have set out.

Just as in our own private lives, we would like our own personal information to be properly protected by the organisations we trust to hold it. At Capita, we must also take our obligations seriously. Our clients and their customers trust us with the personal information they provide us in order for us to manage the business. They have every reason to expect that when they supply us with their personal information, we will treat it with respect and that we will protect it so that they are not put at risk of falling victim to financial crime or identity theft.

The more personal information we collect about our clients' customers, the more valuable it becomes if it falls into unscrupulous hands. If the personal information we hold about our clients' customers is incorrect, out of date, or excessive, the greater are the chances that they will be caused untold distress if their personal information falls into the hands of fraudsters, or if we, as a business, use it inappropriately, for reasons other than those for which it was originally collected. Not only is it the right thing to do to protect personal information, we are duty-bound by law to protect the personal information of our clients, their customers and our employees.

5. Protecting your personal privacy

Now consider in turn each of these scenarios.

1. **Going on holiday**

You have booked and paid for a two week holiday, including flights, from a reputable travel comapny on-line and have provided your full name, address, telephone number and credit card details together with details of your chosen holiday, and the full names as they appear on their passports of the people who will be travelling with you. The travel company says they need this information only to process your booking. You later receive an email from an insurance company explaining that they are aware from the said travel company that you will be taking a holiday and offering you travel insurance.

Is the travel company entitled to pass your details to the insurance company?

No
In this case, the travel company has been clear as to what processing of your personal information will take place - the processing of your travel booking. You are not obliged to take travel insurance from this travel company or any other insurance company it might nominate and passing your information to a third party would be a breach of your rights under the Act. The privacy notice tells you how a company will use the personal information it stores about you. Always read the privacy notice before entering into an agreement.

The first data principle defined in the Data Protection Act compels organisations to process your information fairly and lawfully.

2. **A trip to the optician**

As you grow older, you have noticed a significant deterioration in your sight. You visit the opitcian who you have been seeing for many years and he prescribes stronger lenses. Some time later, you receive a mailing from a national club which specialises in supplying reading material such as books and publications in extra large print. You discover your name, address and contact details have been provided to the club by your optician.

Is the optician entitled to pass your details to the society?

No
The purpose of collecting data would typically include keeping patient notes, diagnostics, prescrbiing, dispensing and communicating with any specialists on your behalf to whom you are specifically referred. If the optician wants to supply details of his patients to any other third party, he must first gain your consent.

The second data principle defined in the Data Protection Act compels organisations to process your personal information only in line with the purposes they have previously disclosed to you.

3. **Mobile phone contract**

You have decided to treat yourself to a new mobile phone on a two year contract. You find a greta deal, submit yourself to a credit check and complete the contract application form. You provide your full name, address and telephone number as well as bank details so that monthly direct debits may be collected. In addition, because you have told the phone supplier that you will insure your new phone with your home insurer, you are asked to provide the name and address of your home contents insurer and the name of your mortgage provider alongside the number of remaining years of the term of the mortgage.

Is the mobile phone supplier entitled to collect all this information.

No
In this case, it is up to you whether you have your phone insured or not, and wiht whom you will insure it. The phone company is entitled to run a credit check since you are paying by direct debit on a long term contract but it can conduct this credit check with any of the credit reference agencies without details of your mortgage or home contents insurance.

The third data principle defined in the Data Protection Act obliges organisations to collect only information that is adequate, relevant and not excessive in relation to the purpose for which it is processed.

4. **That's not me**

Angus has private health insurance. He knows that his insurance is invalid if he does not advise them of any new information about his health from time to time. Recently diagnosed with angina, and having been treated under his health insurance policy, he has written to his insurer explaining the new condition and the medication prescribed. He receives an acknowledgement but later learns that the insurer has recorded his condition as 'anxiety'

Is Angus' health insurance provider entitled to keep 'anxiety' on his medical record?

No
In terms of medical records, where there may have been a misdiagnosis of a patient the details may be left on the patients' record simply because it may be relevant later. But if the misdiagnosis is an error, patients are entitled to expect the error will be corrected.

5. **Time's up!**

You currently have a mini Cash ISA with GreatISARates.co.uk. You have decided to transfer your imni Cash ISA to a new provider, BestISAs.co.uk because they offer you a better interest rate. Your cash is successfully transferred to BestISAs.co.uk but you discover some two years later that GreatISARates.co.uk continue to hold your name, address, telephone number, value of your cash ISA prior to its transfer, your password and mother's maiden name.

Is GreatISARates.co.uk entitled to continue to hold your personal information?

Yes
In fact, it's more 'maybe'. With regard to the ISA, GreatISARates.co.uk will have a legal obligation to provide some information to HM Revenue and Customs for tax purposes and will need to hold on file some of your account details for a period of time after you have closed your account. It is unlikely that they will need to hold your password and mother's maiden name for that length of time.

The fifth data principle of the Data Protection Act obliges organisations not to keep personal information for longer than is necessary for the purposes for which it was collected.

6. I want that job

You recently applied for your dream job. Foreign travel, great pay, long holidays, pension scheem, private health insurance and you felt you were the ideal candidate. You went along to the interview and thought things had gone well. Two of the three interviewers wrote lots of notes and seemed to nod in agreement from time to time with what you were saying. You were very despondent when you later heard that your application had been unsuccessful. You subsequently sent a polite note asking for some feedback and to see the notes that were made about you during the interview. You were given some brief feedback over the phone but were advised that you would not be able to see the notes made at the time.

Is the organisation within its rights to withhold the notes made at interview?

No
These notes must be held on file along with your application until such a time as any claim you might bring about against the company has passed. They should therefore provide those notes. This does mean that managers taking notes during interview should be conscious of the need to be accurate in their note-taking.

The sixth data principle of the Data Protection Act obliges organisations to process personal information in accordance with the rights of data subjects, (that is, the individuals who are the 'subjects' of the personal information held). This includes the rights of those data subject to gain access to the information held about them.

7. Where did that information go?

Graham had to get a schedule of all employees' names, national insurance numbers, monthly salar,y tax and national insurance details out to a contractor to produce the monthly payslips. He usually did this securely by electronic transfer, but the system was down. He copied all the details to a spreadsheet on an un-encrypted CD without any password protection and sent the CD by guaranteed next day delivery, which, he thought, would guarantee not only their arrival, but also provide him with confirmation of receipt. Several days later the contractor advised they had not received the disk. When Graham checked with the post, he learned that the item had not been delivered. It had, after all, been lost in the post. In sending the employee information by guaranteed next day delivery on a CD to his contractor, has Graham kept that information secure?

No
Simply relying on a signature for receipt only guarantees a signature on delivery ,not delivery itself. The fact that the CD was neither password protected nor encrypted meant that anyone who found the CD could gain access to all employee data. Fraudsters could easily use that data to commit financial crime. Moreover, Graham did not check that the CD arrived that day so it was several days before he realised the CD had gone missing.

The seventh data principle of the Data Protection Act obliges organisations to take technical and organisational measures to secure personal information and to minimise risk of unauthorised or unlawful processing of personal information and its accidental loss or destruction.

This is why it is so important that we follow the Group Information Security Policies and Dos and Don'ts setting out how we should work to protect personal information. These policies set out what we must and must not do when we work in the office or from home. They tell us about good password management, and about the use of company internet and email systems. They tell us how we msut manage and dispose of personal and confidential information, and what is permissible when we use mobile devices including laptops and BlackBerries. To minimise the risk of personal information going missing and falling into unscrupulous hands, always follow the Group Information Security Policies and Dos and Don'ts which can be found on Capita Connections.

8. My social networking profile

You have been out for the day with a group of friends and on your return have posted a number o fphotos of you with your friends on your social networking site. Are you in breach of the Data Protection Act?

Yes
That's right! A photograph of someone that can be identified (either because it has a name on it or it is someone well known) is personal data so covered by the Act. If the friends shown in the photos have not given permission for the images to appear, this is likely to be a breach of the Act, (although the Act exempts personal data processed for 'domestic purposes'). The affected person can request that their photographs be removed (or do it themselves if possible). If neither of these options is possible they could report the matter as 'abuse' to the social networking site and ask for the photograph to be removed (assuming it is not the picture of a child and that it is not pornographic / explicit). The social networking site may do this or may refuse or ignore the request. Ultimately, the individuals concerned could make a formal complaint to the Information Commissioner's Office and ask for them to approach the social networking site and instruct them to remove the photo. Before posting photos of others on social networking sites or on web sites, it is wise to seek permission in advance.

9. It's not processed in the UK

You discover that your insurance company, BeInsured, regularly transfers all its customers' perosnal information, including yours, for example their names, addresses, life insurance and medical records to a contractor based in a country outside the European Economic Area, (the European Economic Area is all those countries in the European Union, plus some others including Iceland, Liechtenstein and Norway).

Are BeInsured allowed to transfer personal information outside of the European Economic Area provided they have told customers they will be doing so?

No
The EEA (European Economic Area) recognises several countries outside the EU as porviding adequate protection such as Argentina, Canada, Switzerland, Jersey, Guernsey and the Isle of Man.

The eighth data principle of the Data Protection Act is there to prevent our personal information being processed in countries where standards of protection are not regarded as high which may result in us being put at greater personal and business risk.

The Data Protection Act (1998) serves two fundamental purposes:

1. The eight data principles in the Act provide a legal framework to ensure that our personal information is handled properly by organisations that hold it to reduce our risk of falling prey to identity theft, financial crime and the distress that can be caused when our privacy is breached.
2. It gives individuals the right to know what information is held about them by organisations.

6. Myth or reality?

A number of myths have grown up about the Data Protection Act over the years. See if you can identify which are myths and which is reality out of each of the items below:

Telephone conversations

Insurance companies must not divulge to applicants over the telephone the reason why their applciation may have been rejected unless the applicant applies in writing.

Myth
This may be company policy but it is not required by the Act. As long as insurance companies have robust steps in place to identify and verify that the caller is, indeed, the applicant, there is no reason why information may not be given over the telephone.

Utility companies

Utility companies could not talk to you about your elderly father's energy bill.

Myth
If your father authorises you by telephone or letter to discuss his bill and the utility company accepts that, there is no reason why they cannot discuss his bill with you.

Job applications
If I apply for a job but am unsuccessful in my application, the Data Protection Act does not allow for me to find out why I was unsuccessful.

Myth
Individuals have the right to issue a subject access request to obtain information of this nature. If they do not receive information to which they have a right of access, they may appeal to the Information Commissioner's Office.

Registering with the Information Commissioner
Organisations that are not registered with the Information Commissioner's Office for data protetcion, do not have to comply with the Data protection Act.

Myth
All organisations that use personal information must comply with the Act regardless of whether or not they need to register with the Information Commissioner's Office for data protection. Since all businesses utilise some personal information, for example information relating to employees, agents and directors, it follows that all businesses must comply with the Act.

Disclosing personal information
Organisations must never give your information to anyone else.

Myth
Companies must comply with certain legal requirements. For example, under certain circumstances, they may be required to divulge the personal information of their customers or employees to the police. They must also provide personal information such as salary, tax and national insurance contributions of its employees to HM Revenue and Customs. They may also have third parties carry out their processing; examples might include insurance claims handling, collection of council tax, etc which may be in the UK or abroad. Alternatively, the company might be bought, in which case the customer data may pass to a

new owner. So under certain circumstances, organisations may give your information to others.

The telephone company
When my elderly mother was taken into hospital for a number of weeks, I tried to inform the telpehone company so that they would not chase her payment in the short term but they said they could not discuss her account with me.

Myth
There is a difference between asking for information on behalf of someone and proivding it. As long as you are not attempting to change any of the records of the individual concerned, (e.g. your elderly mother's contact details or bank details), the information that was being offered in this incident was to try to be helpful to the telephone company. Companies have an obligation to take steps to identify and verify the caller who is contacting them.

7. Summary

So Emma may have fallen victim to financial crime and identity theft for any number of reasons:

- She willingly gave away her personal information to organisations that sold it on to third parties whose commitment to protecting it may not have been high. Any number of organisations may have processed or disposed of her information carelessly.
- Her credit card details were left in a waste paper bin and subsequently fell from a refuse vehicle into the street for anyone to see.

The Data Protection Act is there to protect us from these kinds of risks, but it doesn't think for us! We have to think how we guard our own, our colleagues' and our customers' personal information.

What should you do as a result of what you've read in this module?

Disclosing personal information

Think carefully before you disclose your own personal information to callers, post it to social networking sites, or provide it to shops and stores, whether online or on the high street.

Customer and employee information

Be mindful that we are duty-bound by law, only to use the personal information we hold about our customers' and employees, fairly and lawfully and for the purposes for which it has been collected to comply with the first and second data principles of the Data Protection Act.

Accurate record keeping

Ensure that whenever you are asked to add or amend personal information held about a customer or employee, that the changes you make are recorded accurately in line with the third data principle of the Data Protection Act.

Verification

Think before you disclose a customer's or colleague's personal information to anyone without first verifying that they are indeed entitled and authorised to have that information in line with the seventh data principle of the Data Protection Act.

Subject Access Requests (SARs)

If a customer asks to see the personal information we hold about them, you must follow your organisation's process for handling Subject Access Requests.

Data retention

In order to comply with the fifth data principle of the Data Protection Act, avoid holding personal information for excessive lengths of time. What is regarded as excessive may vary from one part of the business to another. Refer to your business's data retention policy.

CAPITA
LEARNING & DEVELOPMENT

Security

To comply with the seventh data principle of the Data Protection Act, always be vigilant about the security, of the personal information of your customers and your colleagues.

Follow the Group Information Security policies set out in the Do's and Don'ts on home working, office working, using mobile devices, using internet and email, using social media, password management, and data management which can be found on Capita Connections.

Indeed, maintaining the security of your own personal information will help protect you from falling prey to identity theft and financial crime.

Information transfer

To comply with the eighth data principle of the Data Protection Act, if personal information is to be transferred abroad for processing, check whether the country in which it is to be processed is in the EEA and seek advice from Group Security.

Email: groupsecurity@capita.co.uk

For further information, see the Group Information Security Policies and Do's and Don'ts, on Capita Connections.

If you have any questions on this topic, please contact groupsecurity@capita.co.uk

If you want more information about data protection, visit the Information Commissioner's website at: http://www.ico.gov.uk/what_we_cover/data_protection.aspx

If you want to find out how healthy your attitude to your personal information is and how much you could be exposing yourself to identity crime, take the "Personal Information Health Check" at: http://www.ico.gov.uk/tools_and_resources/quizzes_or_questionnaires.aspx

Other sites to visit:
www.cifas.org.uk
http://www.aboutidentitytheft.co.uk
https://www.identitytheft.org.uk
http://www.banksafeonline.org.uk