Data Protection Today

How often do you get asked for information about yourself, or fill in a form with your personal details? Maybe you work with other people's data, how do you know if you're handling it correctly?

Data protection is about personal data, what organisations need to do to handle it correctly, and the rights individuals have about what happens to their personal data. We'll look at all these areas, but let's start with what personal data is.

This is Laura. In order for data to be 'personal data' it needs to relate to an identified, or identifiable, living person.

So Laura's name by itself probably wouldn't be enough to identify her, but her name with her address would.

When you're on the phone and the person you're speaking to wants to verify who you are, they'll often ask for your name, address and date of birth. When these three are all together - that's an example of personal data.

But there are many other ways of identifying a living person.

For example, there's biometric data like a picture of a face or a fingerprint, the address a computer or smartphone uses to connect to the internet can sometimes be used, and there's also genetic data such as a person's DNA.

Some of our personal data is sensitive and there are special categories of personal data which must be processed with more care.

Laura's health records, her religious or philosophical beliefs, racial or ethnic origin, political opinions, membership of trade unions, her sex life and sexual orientation, as well as her genetic and biometric data are all classed as special categories of personal data.

And it's fairly clear to see why these need to be treated with greater care and why explicit consent to process them is needed.

What organisations do with personal data is known as data processing. This covers just about everything from obtaining it, storing it, making sure it's secure, transporting or transmitting it, and then erasing and eventually disposing of it.

A data controller is responsible for how data is processed and a data processor carries out the processing. Look at this example.

Recently Laura went online and did some shopping on AmazeMe's website. She gave them a lot of information about herself and her credit card details. In this situation, AmazeMe is the data controller as they decide how that data will be processed - what happens to it.

But AmazeMe outsources its customer support to a third party call centre. Employees in the call centre have access to some of AmazeMe's records, but can only use this data for very specific purposes. AmazeMe is the data controller, and the call centre is known as a data processor.

Because it's Laura's data that's being processed, she's known as the data subject.

So personal data is data which can identify a data subject. The data controller decides how this data will be processed and processing means just about everything that happens to data.

The legislation that's in place to protect our data from being misused is based on a number of principles. Let's have a look at them.

The first is that data must be processed lawfully, fairly and transparently.

And an important part about this, is the privacy notice which explains how an organisation will use the personal data it collects.

AmazeMe's privacy notice states that it needs Laura's details to process her orders, to carry out security checks and that they pass some data to a third party which provides phone and online support for them.

In most cases the data subject must give their consent for their data to be processed.

Laura remembers being asked for her consent when she called about her car insurance and there was a checkbox on the web application for her building society account.

She sometimes gives her consent for her son's data to be processed as he's too young to give it himself.

When Laura asked about health insurance they said they needed some details about her medical history, which is a special category of personal data, so explicit consent was needed before her details could be processed.

Organisations need to be open about why they're obtaining data, and how they'll use it, and they mustn't use it for anything which the data subject wouldn't reasonably expect them to.

Next. Data must be adequate, relevant and limited to what's necessary. This is sometimes called data minimisation.

Like many of us Laura's got a bank account, car insurance and a mortgage.

When she applied for these she gave a lot of information about herself to the different organisations. But the information she gave them had to be relevant to her applications and the organisations could only collect data that they actually needed.

For example, Laura's bank doesn't need to know if she has any points on her driving license or even if she can drive, but the company she used for her car insurance does.

Things can change and our personal data must be correct and, where necessary, up to date.

When Laura renewed her car insurance she was asked to check that all her information was up to date and correct.

And recently, she contacted her mobile phone company and asked them to stop sending her marketing material, so they updated her preferences.

Data must be kept in a form which permits identification of the data subject for no longer than is necessary. Here's an example.

When Laura got a new job, the organisation she used to work for had to keep some of her personal data, so that, for example, they could provide a reference, but they disposed of her personal data they were no longer likely to need. Things like who to contact in an emergency.

Of course, when they disposed of her data, they made sure it was done properly, because data must be processed securely

We've all heard the stories. Hard drives found on rubbish tips, laptops left on trains and hackers getting personal data.

Laura expects, and the regulations require, organisations to look after her personal data securely.

This includes things like how data is stored, backed up and protected from hackers and natural disasters.

And it also means that employers must take steps to ensure employees are reliable, and know what they can and can't do with the personal data they handle.

For instance, when discussing personal data with a customer, they must know how to verify that the person is who they say they are.

Also that they don't do things like leaving personal data lying around where anyone can see it.

Firms often store, or move data to different parts of the world.

And if any of Laura's data is sent abroad the data controller needs to be sure that it will be processed to the same standards as it would be here.

Keeping data secure is particularly important because if the genie ever gets out of the bottle, there's no putting it back.

Laura, as the data subject has certain rights – let's go through them.

The first is the right to be informed and the privacy notice is used to inform us about how our data will be processed and if, for example, it'll be passed on to a third party.

So that Laura can check what data an organisation has about her and that it's being processed fairly, she needs to have access to it. She can do this through what's known as a subject access request which in most cases, can be obtained free of charge.

If there are any mistakes in the data, or if it's incomplete, she can ask for this to be put right.

She could object to her data being processed, if for example, she thought it wasn't being used correctly.

And if there's a dispute about whether an organisation should be processing her data, then the data processing might be restricted to it only being stored.

If Laura posted something on the internet which she now regrets, and there's no real need for it to be kept, she can ask for it to be erased. This is sometimes called the 'right to be forgotten' and is particularly important for posts made by children.

Laura has rights about decisions which are made by automated means. For example, if her application for a loan was refused and the decision had been made purely by automated means, with no human intervention, she could ask for this decision to be reconsidered.

This is also true if an automated form of processing was used to analyse or predict things like Laura's performance at work, her economic situation or her personal preferences. This is sometimes called profiling.

Finally, when Laura has provided personal data to a data controller and it's processed by automated means, she can ask for a copy of her data so that she can transfer it and reuse it. This is called data portability and here's an example.
Laura wants to see if switching her bank account will mean she can get a better deal. All the banks have different offers and it's almost impossible to work out which one is best for her particular needs.

But by taking the transaction history from her current account, and uploading it to a comparison website, her data can be analysed and show the best options based on her previous usage.

We all want our personal data to be handled safely and securely, and for it not to be used in ways which could harm us.

So understanding what the legislation is, how it protects us and those around us, as well as what our rights are as individuals, can all help to make sure our data, and the data we handle, is processed fairly and lawfully.