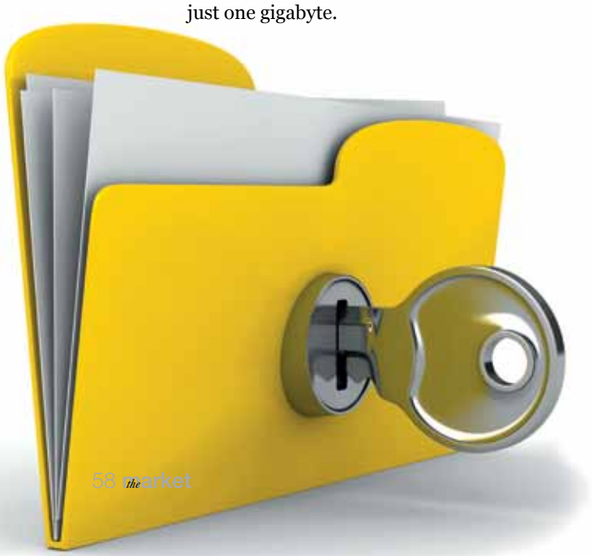
Commercial lawyer, Jo Tall, highlights the law on Data Protection and offers her top tips on how not to break it

Check your pockets or you could face a £500k fine!

We live in extraordinary times where technical advances get better by the day. Barely five years ago, I worked as an in-house lawyer at Sony and was thrilled to become one of the very first owners of a 'Memory Stick', a handy device the size of a lipstick that could replace my cumbersome external floppy disc drive and allow me to store and transport my personal files such as documents, pictures and videos. What's more, it could hold a record breaking 126MB of memory! These days the average memory stick or USB flash drive, as they are also known, holds 5GB of memory and costs a fraction of the price of my old one. You can even get some that hold 256GB. Not being that technically savvy, I thought I would just remind myself what that actually means in real terms: one gigabyte is equivalent to one thousand megabytes! That is the equivalent to 1,664 30-page documents or 512 photos. Yikes -and that's just one gigabyte.



Whilst this is fabulous news for our filing cabinets and trees, the size and portability of these devices means they can also get LOST! Most memory sticks are not encrypted or password protected and hence a lot of information can simply fall into the hands of ANYBODY. And if this happens to be a journalist, they will have a field day with the information, especially if the data is sensitive or belongs to a large corporation, as the countless stories in the press regarding CDs holding vital data lost in the post or left on trains show.

You may be staggered to find out that last year alone, over 4,500 memory sticks were forgotten in peoples' pockets as they took their clothes to be washed at the local dry cleaners! I have washed a couple of my daughters' memory sticks which were stuck in skirt pockets, but I didn't realise this happened on such a large scale. Clearly, this is not good news for our privacy and the Information Commissioner, the officer responsible for enforcement of the Data Protection Act, is now seriously clamping down on breaches of security. He now has the power to impose fines of up to £500,000 on a business and only recently has issued the first monetary penalties. The first penalty, of £100,000, was issued to Hertfordshire County Council for two serious incidents where council employees faxed highly sensitive personal information to the wrong recipients. The first case, involving child sexual abuse, was before the courts, and the second involved details of care proceedings.

The second monetary penalty, of £60,000, was issued to employment services company, A4e, for the loss of an unencrypted laptop which contained personal information relating to 24,000 people who had used community legal advice centres in Hull and Leicester.

So how can you ensure your customers' data is safe and what do you need to do to comply with the Data Protection Act ('DPA')?

The DPA lays down eight data protection principles that must be followed even if you are not obliged to register with the Information Commissioner's Office ('ICO'). The following questions will help you comply and there is a wealth of information on the ICO's website itself (see box below):

1. Do I really need this information about an individual? Do I know what I am going to use it for?

2. Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?

3. If I am asked to pass on personal information, would the people whose information I hold expect me to do this?

4. Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?

5. Is access to personal information limited to those who absolutely need to know? Does your company/do you allow staff to plug in USB flash drives and copy information to take away with them?

6. Am I sure the personal information is accurate and up-to-date?

7. Do I delete or destroy personal information as soon as I have no need for it?

8. Have I trained my staff in their responsibilities under the Data Protection Act? Are they fulfilling them in practice?

9. Do I need to notify the Information Commissioner? If so, is my notification up to date? (See inset box on how to notify)

Remember! If you are going to be processing personal information in an automated form, you will be obliged to notify the Information Commissioner's Office, unless you are exempt. Failure to notify is a criminal offence. Registration is simply a matter of completing a form setting out the types of data you collect and process and for what purpose. The fee is £35 per year if you are a small company or £50 for large companies. See *www.ico.gov.uk* for more details.

The best way to tell your customers what you will be doing with their personal details is by means of a 'Privacy Policy'. Ideally, there should be a link to it on every page of your website or it should be available in print, if a paper form is being completed. Whether personal data is gathered online or from a paper form, there should be a 'tick box' statement which customers have to tick to show that they agree to you processing their data and sending them marketing emails. Do not just assume they do!

Lastly, if you do have to use portable devices, check out the ones that can be encrypted such as the 'Safe Stick'. There are also some clever ones that self destruct, if you find you have lost one or that an employee has used the device to steal vital data. I am glad my daughters' devices were not of that variety; I have this sudden vision of me opening the washing machine and BOOM!!

PLEASE NOTE: this is just an outline of the law. Entire books have been written on the subject, so please seek legal advice if in doubt.

Jo Tall is a commercial and IT lawyer with 20 years' experience
www.offtoseemylawyer.com