Data protection has the protection of individuals at its heart

by Christopher Docksey, Member of the Guernsey Data Protection Authority, Hon.Director-General EDPS.

Most of us would like to respect the data protection rules, in the sense of trying not to break them deliberately. But I have learned, both as a manager and a regulator, that this is not enough. There is a difference between *compliance,* in the narrow sense of not deliberately doing anything wrong, and *anticipation*, taking real care not to cause harm. Good data protection means taking care with people's personal information. It means *thinking in advance* about *what you are doing,* and *why,* and *what risks are involved*

To illustrate this I would like to share three short stories about why data protection is important, and why it needs a change in culture to be effective. The organisations concerned range in size from a US multinational to a major Guernsey company serving the Channel Islands and the Isle of Man, to a local St Peter Port law firm.

My first story is about a major multinational company based in the US but with operations in Europe, including London and Yorkshire in the UK. It analyses the personal data of millions of people in order to provide anonymised customer data to online marketers. Its analytics team developed a model of '10,000 audience propensities', including scores for items such as individuals' shopping behaviour, their favourite brands and their financial assets. Each of these "propensities" carried a "personal score", to allow advertisers to deliver more targeted adverts to consumers when they use social media or the internet. However these propensities also included some very personal scores for a number of sensitive attributes such as 'vaginal itch' and 'erectile dysfunction'.

So the leadership team met to discuss whether the use of such intimate scores might be perceived as too invasive. The analytics team argued that these scores offered a marketing opportunity, but there was one participant at the meeting who was ethically opposed to using them. She devised an effective way of making her point, here's how she described it:

> "I came armed with a piece of paper and I had pulled the scores of all the gentlemen in the room. When I got challenged I said, well, I want to demonstrate the sensitivity and why this is too sensitive for us right now. I don't think this is fair from a marketing perspective. And let me just read your scores out loud to give you a sense of what we're talking about. And they were like, you know what? Point made!"

I have met the individual concerned, she really wanted to remind managers that there are ethics involved in processing intimate personal information. Her story shows very clearly how individuals can have a positive influence inside their organisations.

And being influential means being *practical*. It is important to *anticipate* issues that may arise. We don't know when an accident will happen, but it might, and we should prepare for it. "If you fail to plan, you plan to fail". For example, there could be a *data breach*. Data breaches are very varied. Some of them are committed against us by sophisticated computer hackers, who break into our IT or emails to cause damage or to steal, from us or from our customers. Here, data protection means assessing the risk of hacking attacks and making sure there is adequate security.

But data breaches can also be caused by ordinary people, doing ordinary things. They can be as simple as sending documents containing private information to the wrong person, by email or by post. In 2020 these two types of data breach – emails and letters to the wrong person - were the most common subjects of complaints in Guernsey to the ODPA.

Here, data protection means taking care of others, to stop them suffering harm. I have two more stories, about two ODPA cases last year, that show how thinking in advance about data processing and its possible risks can make a real difference.

My second story is about how *not* to send out documents containing confidential personal information. A law firm was fined £10,000 for accidentally sending 'highly confidential and sensitive personal details relating to the complainant and their family without appropriate security" to unconnected third parties both by email and post. What do we learn from this story? That we could avoid harm to customers by asking three practical questions:

- do we send emails or post letters which contain confidential information?
- if so, could our clients suffer harm if messages like these get sent to the wrong address?
- if so, are there simple precautions we could take to stop that happening?

My third story is about a more complicated data breach. A major Guernsey telecoms company was fined £80,000 for accidentally publishing the private contact details of some customers, which could have caused them real harm. There are many good reasons for obtaining an ex-directory number and expecting it to be kept private. The disclosures happened after the company had combined two electronic databases of subscribers and published the combined information in a paper and online telephone directory. What can we learn from this story? Once again we could ask three practical questions to avoid harm to customers:

- does the directory include ex-directory private information?
- if so, is there a risk that subscribers could suffer data harms from the new systems? For example, publication of their private contact details?
- if so, is the risk serious enough to merit a data protection impact assessment, to assess the risks and the precautions that should be taken?

These three stories show that data protection is *both practical and ethical*. When we "process personal data" we are handling the personal information of real people. Data about us, our friends and family, our colleagues, our customers and the public.

So we have to try to *understand the everyday risks* for individuals when we handle their personal information. Including risks to their dignity and their private and family life. And we should assess *in advance* possible risks from *new* processing operations, *before they start*. Then we can *reduce the risks* by taking sensible precautions. Finally, we should be *transparent* with people about *what* we are doing with their personal data, and *why*.

Most of this is not rocket science, it is common sense. Whether we work for a small company or a big one, a private firm or a government department, we can make a difference. In a nutshell, data protection is about treating people well. According to Emma Martins, the "data protection law has the protection of individuals at its heart."

Project Bijou is about cultural change, led by individuals, for the benefit of individuals. It is absolutely unique, I have never heard about anything quite like this before. I hope you will be interested in joining in and learning more, and I wish you every success. *Bouanne Chànce*!