THE OFFICE OF THE Data Protection Authority

Transcript: Rachel Masterton's presentation

to States Members on 16 November 2020 (held at GFSC)

Guernsey's approach to Data Protection

"Thank you to William and his colleagues for hosting this event and congratulations to you all on your election success – the fruits of democracy in action.

Democracy and data rights are interrelated and interdependent. If you look at a world map of countries that are free and democratic, for the most part you are also looking at countries which give their citizens rights and ensure organisations handle their private data responsibly.

Privacy related issues are as much political and public policy issues as they are legal and technical ones. Those of us in the political and policy field shoulder a responsibility to recognise how much privacy underpins other rights.

And the decisions made need to be made politically to ensure that we as society use technology to deliver on what we want it to deliver and to serve us and our values. If we don't, others will make those choices for us. We owe it to ourselves and also those we are here to serve.

It has often been said that data is the new oil, fuelling the development and diversification of the twenty first century economy in much the same way as oil did in the eighteen century. And there are aspects of that comparison that are true – data, including data about people, is being used in innovative ways to support and enhance the economy, providing products and services we would not have thought possible only a few years ago and to

tackle many of the World's problems. Data is, for many, an asset that when put to work well can drive success, sustaining and growing economies.

However, the oil analogy falls down when it is recognized that data does not dwell in pockets, waiting to tapped and put to work. Neither is data an asset that can be used only once and is then lost. The dot com bubble can be seen as an example of relying on something that cannot last – an approach to business development that looked more at making money quickly rather than seeking ongoing stable growth.

Some thought leaders, including the President of the Centre for Information Policy Leadership, have re-evaluated the oil analogy and, in this world of sustainability, have instead likened data to sunshine – something that is everywhere and when harnessed well can produce results that endure. And if we want to take that analogy and run with it, if the sun were to suddenly go out, it would take eight and a half minutes for us on Earth to know about it and for panic to ensue. How long would it take before chaos reigned if it were the global telecommunications network that was snuffed out?

In 2017, the States of Deliberation agreed their policy objectives in the form of the Future Guernsey Plan. Part of this was the Digital Sector Strategic Framework- summed up by the vision of "driving economic growth by investing in the digital sector to support existing business and strengthen the offer to new business opportunities". The Framework included 4 aims - driving economic growth and competitive advantage in the digital sector (and by extension, the Bailiwick as a whole), delivering next generation digital infrastructure, developing the digitally skilled workforce of the future and fostering a world leading and proportionate compliance and regulatory environment - with the latter aim being evidenced, in part, by the three regulatory offices here today.

Action Plan 8 of the Framework related specifically to data protection and the desire to adopt an innovative approach to create opportunities for digital businesses and provide the optimum balance between privacy protection and economic development. It recognized that data protection legislation and regulation were key facets to retaining the ease of

access to EU markets. And this was further evidenced on the Glorious 25th of May - 2018 when the Data Protection (Bailiwick of Guernsey) Law, 2017 came into force; a piece of legislation essentially equivalent to the EU's GDPR - General Data Protection Regulation and designed to protect the rights of individuals in relation to their personal data and provide for the free movement of personal data, thus underpinning the Bailiwick's economy.

The Bailiwick is currently going through a re-assessment of its adequacy; a process conducted by the European Commission in which the legislative, governmental and regulatory frameworks of the jurisdiction are assessed against the EU's GDPR. The successful completion of this is vital to ensure that Bailiwick organisations still have unfettered access to EU markets, something we have had since our original adequacy assessment in 2003. Without this adequacy, companies based locally would be required to endure increased bureaucracy to trade with the EU, making the Bailiwick a less attractive place to do business. And just as an aside and to pre-empt any wonderings – it is a pass/fail process; adequate or not adequate. It is not like school reports, "C3 – just getting by, more effort needed".

And with an eye on the importance of data transfers, before the end of the year, you as the New House will be asked by the Committee *for* Home Affairs, to approve an extension to the Ordinance that recognises the UK as an authorised jurisdiction to which personal data can be transferred. This is to maintain the status quo locally and enable us to share personal data with the UK while they seek their own adequacy decision. With the Brexit withdrawal period drawing to a close and no adequacy decision for them on the horizon, businesses there are facing those burdensome extra steps to receive personal data from the EU that we avoid by maintaining adequacy.

Data protection is not a sector specific piece of legislation; if an entity is processing personal data the law requires that it meets its obligations. What this means will differ depending on the nature of the processing and the type of data involved but compliant they must be. For us this means we are very much a horizontal regulator, spread out across the many and varied sectors of the economy rather than our efforts being concentrated in key industry

sectors in a more vertical fashion. Companies large and small; SMEs, sole traders and third sector bodies; regulators and government are all processing personal data and come under our regulatory remit. This has required that we look at regulation in a different way –just as the businesses are looking at innovation, so are we.

Our structure was driven, in part, by this diverse make-up of our regulated community and because effective regulation, independent of government, is something that the European Commission is seeking evidence of as part of their adequacy assessment. As a result, the Data Protection Authority was formed in May 2018, to provide governance and oversight to the work of the Commissioner and her team; and to be accountable to the Committee for Home Affairs, as the sponsoring committee for the legislation, whilst being independent from States as a whole.

May 2018 also meant that the Commissioner's team ceased to be civil servants and became employees of the Authority and functions previously provided by Home Affairs and the wider civil service needed to be controlled from within. This separation was vital – how could the Authority be truly independent if its staff were paid directly by Centre? How could it objectively determine compliance by the body that it directly reported to?

Since our inception, we have been funded by a combination of government grants, liability-incurring loans and registration fees. Our last push for independence will be on 1 January 2021 when we move to a self-funded model. This model has been designed to be simple to understand and because the cost of running the Office is spread across the entire regulated community, the fee has been kept low, leaving the Bailiwick as an attractive place to do business.

In developing the model, in conjunction with the States of Guernsey, it was important for any funding model to be straightforward and easy to understand. We do not want organisations spending vast amounts of time wrestling with a burdensome fee regime, distracting them from the 'proper job' of handling data well and meeting their legal obligations. Similarly, it was not appropriate for us to incur additional costs administering a

complex scheme that could end up paying only for itself and not all the good work we knew needed to be done. We believe that the annual levy model now agreed will move us to a self-funding footing, able to concentrate of our statutory functions, supporting the Bailiwick, its economy and its citizens.

To that end, our strategic plan is built around four pillars of effective regulation – Predict, Prevent, Detect, Enforce. Predict – to use horizon scanning and statistics generated from breach reports and complaints to determine areas of greatest risk that need action, Prevent – to do what we can to stop data harms from occurring by educating industry in their legal obligations and the benefits of good data governance, Detect – to identify where things are going wrong and to deal with poor practice and non-compliance and Enforce – to ensure the Law is complied with, wrongs are put right and appropriate sanctions are issued.

One of the biggest challenges we face is the challenge of being a 'horizontal' regulator rather than a 'vertical' one. I just mean that this is a law that affects everyone and every sector. The breadth of that responsibility for us means that we need to think creatively and innovatively about how we regulate well with limited resources. As with so many things in life, education and awareness is crucial and it empowers people to make informed decisions. So we have given a great deal of thought about how to effectively communicate to our community , in turn helping organisations meet their legal obligations before something goes wrong. Make no mistake – there is economic value to the Bailiwick in getting data protection right and maintaining free flows of data but at the heart of data protection is people; people who have a right to expect their personal data to be treated well. People who can suffer harms when things go wrong, whether they be harms to their wellbeing, their assets or their safety.

All too often, data protection is perceived as something that stops businesses operating and places unsurmountable roadblocks in the way of innovation – the 2020 version of 'computer says No!', if you will. We are actively battling against that misconception. As an educator, we push out best practice and timely guidance to help organisations, we run events and

encourage those processing personal data to attend our fortnightly drop-ins to speak to us and seek answers where they are needed.

This week we launch our schools programme, empowering children to understand how to look after their own data, to keep them safe and to help them develop as responsible citizens, in line with the Big Picture Curriculum. And this lunchtime, we are again supporting Global Entrepreneurship Week, delivering a session to SMEs, some of those very businesses the Bailiwick is encouraging through the Digital Sector Strategic Framework. We have even ventured into the world of sandboxing (bring your own bucket and spade) – seeking to provide a safe environment in which innovation can be blended with timely regulation to promote privacy by design that builds trust and confidence in the final product or service.

The Law provides us with a broader range of powers and sanctions than we have had previously. We are a complaint handling body for individuals that feel their personal data has been misused. When received, complaints be investigated and determinations will be made as to whether the Law has been complied with. Sanctions can follow – based on nature of the data involved, the harm caused and how things can be put right. Organisations are now obligated to report breaches of security relating to their handling of data and these are assessed, followed up and dealt with appropriately. Where we feel there are areas for concern we can initiate inquiries, with the full range of sanctions available, if needed. And as we have done recently with one business sector, we undertake thematic reviews – to address perceived poor practice across an industry sector. Information gleaned from these activities will be used to drive our communications plan as well as our compliance activities – where trends seem to be emerging, timely awareness may prevent harms happening to others.

Just as the depth and breadth of data use and its implications means we as the regulator have many roles to fulfil, the same can be said for government. Government sets the overall strategy in order to support our economy and our citizens. Government directs the drafting of legislation in order to achieve that strategy and Government seeks to support both through an independent regulatory framework. It must not be forgotten however,

that Government itself revolves around personal data and relies upon its processing to achieve many of its own aims and provide its diverse range of services. As such, it is vital that due regard is paid to the responsibilities this brings, by government and those that serve within it.

If I don't like the way my insurer is processing my data, I can move to another insurance company and ultimately good practice becomes its own business differentiator. Citizens often do not have such choice when it comes to the workings of government – laws compel the provision of personal data and inform how it is to be used. The data collected by government and public bodies can often be the most sensitive in nature and its use, whether good or bad, can have wide-reaching consequences. It is crucial that public sector engages as much, if not more, with the obligations within the Law as the private sector, and truly understands the power of the data in its control, both for the delivery of excellent public services and for the protection of the rights and freedoms of those people it serves.

And to bring this section of proceedings to a close, I find myself drawn to an opening used by orators far greater than myself (specifically Martin Luther King and Abba) – for 'I have a dream'… of a day when data protection ceases to be a 'thing' that is 'done'. Driven by a recognition that we need to shift how we all look at data and a move from a tick box approach to seeing data protection as a fundamental human value. We are uniquely positioned to do that as a small jurisdiction that has committed to ensuring our economy is built on ethical and legal data handling practices, and our citizens have autonomy and rights around their data.

'I have a dream'… of a day when data protection becomes simply part of what it is for good people to do great things in a prosperous jurisdiction."

- **Rachel Masterton**
  Deputy Data Protection Commissioner
  Office of the Data Protection Authority

  Bailiwick of Guernsey