Presentation by Privacy Commissioner John Edwards to the Institute of Directors (IoD)

on 7 June 2018 in Wellington

Introduction – What is the GDPR?

- The European Union's General Data Protection Regulation (GDPR) is a data protection framework that requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states:
    - Adopted by the European Parliament in April 2016
    - Took effect on 25 May 2018
    - Provisions are consistent across all 28 EU member states
    - It means all companies doing business in the EU have just one standard to meet
    - A harmonisation of disparate data protection and privacy laws and regulations across the region
- GDPR defines several roles that are responsible for ensuring compliance
    - data controller
    - data processor
    - data protection officer

Which types of agencies are covered?

- Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU
- Specific criteria for companies required to comply are:
    - A presence in an EU country
    - No presence in the EU, but it processes personal data of European residents
    - More than 250 employees
    - Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data

What are the penalties for non-compliance?

- Up to €20 million or 4 percent of global annual turnover - whichever is higher

- Management consulting firm Oliver Wyman predicts the EU could collect as much as $US6 billion in fines and penalties in its first year
- The fines are big news to US businesses – estimates vary but the consensus is that half of the American companies that should be compliant will not be by 25 May
- Commentators are predicting EU regulators will act quickly on a few non-compliant companies to send a message to everyone

So how does the GDPR affect New Zealand?

- We've seen a lot of confusion about how New Zealand businesses will be affected as the build-up to the GDPR comes in
- I think partly the issue is that anxiety is being promoted by people who are talking up the extra territorial elements of the GDPR
- Laws have extra territorial effect only in quite limited circumstances.
- The GDPR says you may be subject to this law if you are effectively operating in Europe
- If you are selling Manuka honey from a website in Northland and somebody in The Netherlands has ordered it and shipped it, and you have their data in your data base, that does not make you subject to the GDPR
- Do you have a base in Europe?
- Are you advertising on your website in European languages?
- These are some of the tests that will be used to indicate whether you also have to comply with that legal framework
- Compliance with the New Zealand Privacy Act takes you quite a long way in terms of the GDPR and keeps you pretty safe
- It doesn't get you all the way - which we can talk about - but I think some elements of that concern about companies around the world having to comply are a bit overstated.

GDPR and the Privacy Bill

- Some of the features of the GDPR are in New Zealand's Privacy Bill

- The Privacy Bill is a reboot of the 25-year-old Privacy Act 1993
- The Bill had its first reading last month, and is currently before Select Committee
- The Bill's genesis is the Law Commission's report and recommendation in 2011, predating the GDPR
- There's been a long period of review and analysis with the Ministry of Justice
- Fundamental aspects of the Privacy Act remain the same
- The Bill introduces a number of key changes and some new enforcement powers for my office

Current Privacy Bill

What are the key changes in the Privacy Bill?

- Mandatory data breach notification – an agency must notify my office of privacy breaches (defined as unauthorised or accidental access to, or disclosure of, personal information) that pose a risk of harm to people, and to affected individuals.

- Compliance notices – I will be able to issue compliance notices that require an agency to do something, or stop doing something, in order to comply with the law.

- New criminal offences – it will be an offence to mislead an agency in a way that affects someone else's information and to knowingly destroy documents containing personal information where a request has been made for it. The penalty is a fine up to $10,000.

- Binding decisions on access requests – and I will be able to make decisions on complaints relating to access to information, rather than the Human Rights Review Tribunal.

Our submission

I recently made my submission on the Privacy Bill to the Justice and Electoral Select Committee. It recommended:

- Penalty Power - empowering the Commissioner to apply to the High Court for a civil fines to be imposed in cases of serious breaches (up to $100,000 for an individual and up to $1 million for a body corporate)

- Accountability - a power to require an agency to demonstrate its ongoing compliance with the Act

- Letting the Commissioner decide which cases are to proceed to the Human Rights Review Tribunal and act as the plaintiff in those cases, instead of the Director of Human Rights Proceedings.

- In addition, I also recommended the introduction of these provisions, which have an equivalent in the GDPR:

- Protection against the risk that individuals can be unexpectedly identified from data that had been purportedly anonymised
- Portability - data portability as a consumer right.
- Erasure, or the 'right to be forgotten' – a right to for individuals to erasure of personal information. This right is also included in legislation currently before the UK Parliament.
- Algorithmic transparency and automated decision-making – addressing risks to personal privacy from the use of algorithms to make decisions about individuals.

What you can do

- As I mentioned, the best path towards compliance with GDPR is compliance with privacy law right here in New Zealand
- Become familiar with privacy and privacy law
- Lead by example
- Put measures in place to mitigate privacy issues
- Take responsibility when issues arise
- Ask OPC for help

Privacy principles

- Principle 1 – when an agency can collect personal information
- Principle 2 – where an agency can collect information from
- Principle 3 – what agencies should tell individuals when collecting their information
- Principle 4 – how agencies should collect information
- Principle 5 – storage and security of personal information
- Principle 6 – an individual's right to access information
- Principle 7 – an individual's right to seek correction
- Principle 8 – an agency's obligation to ensure information is accurate and up-to-date
- Principle 9 – how long an agency can retain information for

- Principle 10 – what an agency can use personal information for
- Principle 11 – disclosure – when to disclose e.g. when a child is at risk
- Principle 12 – using unique identifiers

OPC functions

- Investigate complaints about an interference with privacy
- Policy advice – both public and private sector
- Examine new legislation for privacy impact
- Public awareness and education
- “Making privacy easy”

OPC resources

- We provide free privacy training modules on our website
- The courses cover a variety of privacy topics and suit different skill levels
- Encouraging your employees to take these courses will make sure they’re up to speed and foster a culture of privacy compliance
- If you want to try something new with personal information, do a privacy impact assessment to find out the potential risks
- Recent example from the news; facial recognition technology
- Search “privacy impact assessment” on our website to find our PIA toolkit
- Recently I launched the Privacy Trust Mark.
- The Trust Mark identifies products and services that I consider to be outstanding in the way they manage personal information.
- If you put in the work and take account of privacy values in the design of your product or service, the Trust Mark gives people more confidence to engage with it
- You can find out more about the Trust Mark and how to apply for one on our website.