Jersey to stay in the European mainstream for data protection

Jersey is not satisfied with merely being adequate with EU DP law. **Dr Jay Fedorak**, Jersey Information Commissioner explains.

Jersey is staying in the European mainstream in the field of data protection. This is part of a shift to diversify its foreign policy, which traditionally has over-relied on the United Kingdom. Jersey aspires to retain its European adequacy designation to ensure the continuing flow of personal data from Europe. By implementing a GDPR data protection regime, the Jersey government demonstrates that it is not satisfied with merely being adequate. Instead, it endeavours to meet the highest European standards in the text of its laws, the effectiveness of its supervisory authority and the level of compliance among the community. In my opinion, Jersey values data protection and understands its benefits as well as anywhere in the world and strives in good faith to provide a level that is effective and appropriate to the size and nature of the community. Jersey's close alignment with GDPR forms part of a general economic strategy to demonstrate that it is a well-regulated jurisdiction.

Background

Jersey has never been part of the UK or the EU. It is a Crown Dependency, like Guernsey and the Isle of Man, which have unique ties to the British Crown. It has its own national assembly, *les Etats de Jersey* (the States of Jersey), with records dating back to the 14th century, that has sole constitutional authority for passing laws relating to Jersey internal affairs. The Jersey legal system, which incorporates elements of Norman law, is independent of the English legal system.

As an Anglo-Norman island only 23 kilometres from the coast of France, Jersey has always maintained stronger ties to Europe than the UK has.

While by treaty, the UK provides us with foreign policy and defence services, Jersey has been asserting itself internationally by signing its own treaties. It has offices in London, Brussels, Caen and Paris. As a demonstration of its independence, Jersey participates in international associations and bilateral relationships that exclude the UK. *Les Etats de Jersey* are part of the *Assemblée parlementaire de la Francophonie*. Jersey and Guernsey government officials hold regular summits with government officials from the department of *ille-et-Villaine* (the administrative title for the Normandy region) and Brittany. My office is also a voting member of the *Association francophone des autorités de protection des données personnelles*.

Question of adequacy

As the Jersey economy is overly dependent on the UK, it is seeking to diversify in new financial markets in Africa, the Gulf, the Far East and North America. It is also expanding existing markets in Europe. As a small island economy aspiring to a greater role on the international stage, it is crucial for Jersey to preserve its reputation as a well-regulated jurisdiction that upholds international standards. It must be a safe place to invest, do business and store data. It has implemented world-class standards of financial regulation and takes great pains to dispel the misperception that it is a tax haven.

Striving to maintain the free flow of personal data from Europe and the UK is one of Jersey's economic goals. The European Commission recognised Jersey as an adequate jurisdiction under the previous data protection regime in 2008. Jersey hopes the Commission will confirm its new regime as adequate under GDPR. The Jersey government has demonstrated a commitment to comply with all of the requirements of the European Commission to achieve this end. For my part, I take every opportunity to demonstrate to European Commissioners on the European Data Protection Board our commitment to protecting all personal data in accordance with European standards.

Jersey demonstrated its eagerness to comply with GDPR when, along with Guernsey, they became the first non-EU countries to pass new legislation to meet the GDPR standard. Their laws came into force on 25 May 2018, which preceded the implementation dates of several EU member states. Jersey's laws include the Data Protection Law and the Data Protection Authority Law. The first implements new requirements for public agencies and private sector organisations governing the management of personal data in compliance with GDPR. The second establishes a new independent authority to regulate the implementation of the first.

The Jersey laws have a unique statutory structure but their terms replicate the GDPR in every meaningful sense. Many passages are verbatim from text of the GDPR. To provide just two of many examples, the principles relating to the processing of personal information and the criteria for determining the application and extent of fines are virtually identical to the GDPR articles 5 and 83.

Differences from the GDPR

There are a few differences between the Jersey laws and the GDPR. There are no provisions regarding a lead supervisory authority equivalent to those in articles 56 and 60, because, as a third country, they are inapplicable to Jersey. The Jersey law also restricts the application of transparency and access rights where they conflict with provisions of current Jersey legislation relating to trusts, which has its own rules governing access to information. With respect to adequacy derogations, the Jersey law permits the Jersey Financial Services Commission to disclose information to law enforcement officials in other countries where it would be in the public interest and subject to an information sharing agreement.

There are also some minor modifications. Jersey has set its upper limit on

fines at £5,000,000 for some offences and £10,000,000 for others, which is lower than some other jurisdictions. The requirements in the Jersey law for offshore companies to designate representatives in Jersey are limited to cases where a processor not established in Jersey uses equipment in Jersey for processing data. The GDPR requires representatives in additional circumstances. The age of consent to data processing in the Jersey law is 13. A data controller may employ automated decision making or profiling, over the objections of data subjects, where this processing is necessary for the performance of a contract or is authorised by a law that includes safeguards to protect individual rights and freedoms. Finally, whereas decisions under the GDPR are reviewable by the Court of Justice of the European Union, decisions under the Jersey law are subject to the Jersey Royal Court.

Independence of DPA

The Government of Jersey has also ensured that the supervisory authority meets the GDPR standard for independence and effectiveness. Whereas previously the Office of the Information Commissioner had been an arm of the government, it now reports directly to an independent board. The government has supported a plan of staff expansion with the budget to fund it. Our complement has grown from four employees to ten, with a projected target of sixteen. The new laws also give us GDPR standards of enforcement powers, including investigatory tools, powers to compel changes of practice and the authority to issue GDPR levels of financial penalties. In summary, I believe Jersey's laws align more directly to the GDPR than do the laws of any other third countries.

In conclusion, our office is regulating to the GDPR standard, in harmony with Europe. This requires a joint effort with the Government of Jersey and Jersey businesses to ensure that the administration of our laws consistently meet the highest standards. We need to complement our new laws with a balanced regulatory approach and robust compliance from businesses and public agencies. Fortunately, there is clear, cross-sector support for data protection in Jersey. I have met with many stakeholders who have demonstrated a spirit of collaboration and respect, as well as commitment and support for data protection. There is a determination throughout our community to be at the forefront of international standards of regulation. We aspire to a leadership role in demonstrating how third countries can achieve European Commission levels of data protection. We will continue to follow closely developments in European data protection law, as well as the work of the European Data Protection Board, to ensure that Jersey stays in the European mainstream. While the UK government may be attempting to disengage from Europe, Jersey is gravitating back towards its natural connection with the Continent.

INFORMATION

See jerseyoic.org

CJEU rules on Google and Right to be Forgotten

In a landmark case about privacy versus freedom of speech, the Court of Justice of the European Union (CJEU) has ruled that Google does not have to remove links worldwide when responding to Right to be Forgotten (RTBF) requests.

The court has now ruled that the RTBF applies only in the EU Member States; the operator is not required to carry out de-referencing on all versions of its search engine. It is, however, required to carry out that de-referencing on the versions corresponding to all the Member States. It is also required to put in place measures discouraging Internet users from gaining access from one of the Member States to the links in question, which appear on versions of that search engine outside the EU. It also points out that numerous third States do not recognise RTBF or have a different approach to that right. However it also says that EU Member States' authorities remain competent to assess the situation regarding de-listing to achieve balance between privacy and freedom of information.

The case goes back to 2015 when France's Data Protection Authority, the CNIL, ruled that when responding to RFBF requests, US-based Google had to delist information from Internet search results globally.

Peter Fleischer, Senior Privacy Counsel at Google, said: "It's good to see that the Court agreed with our arguments, and we're grateful to the independent human rights organisations, media associations and many others around the world who also presented their views to the Court."

A second decision also issued on 24 September concerns a prohibition on processing certain categories of sensitive personal data. The court says that this applies also to operators of search engines – a balance must be struck between the fundamental rights of the person requesting the de-referencing and those of Internet users potentially interested in that information (such as political opinions, religious or philosophical beliefs and sex life).

With regard to criminal proceedings, the court says that "the operator of the search engine must take into consideration all the circumstances of the case, such as, in particular, the nature and seriousness of the offence in question, the progress and the outcome of the proceedings, the time elapsed, the part played by that person in public life and his or her past conduct, the public's interest at the time of the request, the content and form of the publication and the consequences of publication for that person."

The decisions concern the interpretation of Directive 95/46/EC (EU Data Protection Directive) and Article 17 of the GDPR which replaced the Directive and includes the 'Right to erasure'.

• *See /bit.ly/2OwVyd5 regmedia.co.uk/2019/09/24/cp190112en.pdf and curia.europa.eu/jcms/upload/docs/application/pdf/2019-09/cp190113en.pdf*

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Thailand – Asia's strong new data protection law

The law which will enter into force in May 2020 includes many GDPR-informed principles, but also some omissions.
By **Graham Greenleaf** and **Arthit Suriyawongkul**.

A military coup in 2014 imposed a junta government in Thailand. In February 2019, three weeks before the first general elections since the coup, this government enacted a data privacy law to override an old and ineffective law applying only to the public sector. A military-backed party now leads a coalition government with a Prime Minister and Cabinet members from the previous military

Continued on p.3

CNIL's guidance on cookies sets stricter consent requirements

Web publishers need to adapt their websites to France's new rules. **Ariane Mole** and **Juliette Terrioux** of Bird & Bird explain.

On 4 July 2019, France's Data Protection Authority (the "CNIL") adopted new guidelines on cookies and similar technologies[1], which replaced the previous guidance published by the CNIL in 2013[2].

The major change concerns the means to obtain a valid consent from users. The consent of users can no longer result from their browsing on the website. Web publishers will now have to comply with stricter requirements for users' consent.

Continued on p.7

Future PL&B Events

- *Asian data privacy laws*, 30 October, Linklaters, London
- *New Era for US privacy laws: California and more*, 14 November, Latham & Watkins, London.
- *Balancing privacy with biometric techniques used in a commercial context*, 29 January 2020, Macquarie Group, London.
- *PL&B's 33rd Annual International Conference*, St. John's College, Cambridge 29 June to 1 July 2020.

privacylaws.com

Issue 161 OCTOBER 2019

INTERNATIONAL report

ISSUE NO 161 OCTOBER 2019

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Ariane Mole and Juliette Terrioux
Bird & Bird, France
Guoda Šileikytė
WALLESS, Lithuania
Jay Fedorak
Office of Jersey's Information Commissioner
David Barnard-Wills
Trilateral Research, UK
Arthit Suriyawongkul
Foundation for Internet and Civic Culture, Thailand
Inês Antas de Barros and Isabel Ornelas
Vieira de Almeida, Portugal
Wenlong Li
University of Edinburgh, UK
Alvin Cheung
University of Oxford, UK

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

From Thailand to Jersey – GDPR's global effect is evident

Our Asia-Pacific Editor, Graham Greenleaf writes in this issue that the Thai data protection law is the first explicitly "GDPR-based" law yet be enacted in Asia (p.1), and Jersey's Information Commissioner, Jay Fedorak says that Jersey's close alignment with the GDPR forms part of a general economic strategy (p.12). It is therefore clear that the GDPR is having a global effect – also in Australia where there are pressures to modernise the law (p.17).

In our series of GDPR implementation across EU Member States, we now turn to Portugal. Its law, adopted in June this year has been in force since August. Read an interview about the law with Portuguese DP lawyers on p.14. In Lithuania, a new data protection law was adopted in June 2018, and the regulator has now issued the first significant fine. There are some national specifics that are different from the GDPR such as the provisions regarding the processing of national identity numbers (p.9).

Meanwhile, organisations need to get on with training. The STAR project's ready-made, easy-to-customise training materials, developed for the busy DPO, are now available (p.20). The STAR training materials are based upon research into existing GDPR training practices and should therefore be relevant and very useful.

We also return to the issue of recent cookie guidance from France's regulator (p.1). Things are moving fast in this area – the Internet Advertising Bureau Europe has released the second version of its consent and transparency framework, and Google has said it expects to join by the end of next March.[1]

We are also pleased to bring you the winning competition essays from PL&B's Student Essay Competition this summer. These two winning entries discuss consent, legitimate interest and joint controllership in AdTech (p.24), and the market and legal challenges in convincing companies that GDPR-compliance is a competitive advantage (p.28).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

1 digiday.com/media/google-to-join-iabs-revamped-gdpr-framework-by-next-march/

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 165+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"*PL&B's International Report* is obligatory reading for our team members worldwide to keep them up to date on relevant developments in other jurisdictions. Concise but always precise!"

Professor Dr. Patrick Van Eecke, DLA Piper

UK Report

Privacy Laws & Business also publishes *PL&B UK Report*, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.