GDPR: Unintended consequences

What are some of the practical issues that the legislator did not foresee? Will complying with the GDPR have unintended consequences in some areas? Laura Linkomies reports.

Paul Lavery, Partner, Head of Technology & Innovation Group, McCann FitzGerald, Dublin, tackled this intriguing topic at PL&B’s 31st Annual International Conference in July. He said that certain issues have been raised by clients – perhaps there are potential consequences of the GDPR which EU Member States did not fully appreciate.

One of these areas is anti-bribery and anti-corruption due diligence. Would the solution be EU-wide rules? This could take a long time, Lavery said.

ANTI-BRIE OLY AND ANTI-CORRUPTION DUE DILIGENCE

Holding companies responsible for the corrupt acts of their agents and intermediaries necessitates that companies undertake adequate and relevant due diligence on current and prospective intermediaries in supply chains, and the people associated with such intermediaries, Lavery said. The EU has a Convention against Corruption Involving Officials, and there is also an OECD Convention.

“Companies operating globally are investing more in due diligence and are requiring current and prospective partners to complete complex compliance paperwork. Even if a company contractually prohibits agents and intermediaries from paying bribes on its behalf, actions of such third parties may still lead to criminal liability for the company, its officers and employees.”

There is clearly public interest involved but also interaction with data protection law. It comes by necessity as anti-bribery due diligence involves the processing of personal data. The nature of bribery risks often requires the processing of personal data in relation to prior criminal activities and convictions.

The issue at hand, Lavery said, is the GDPR’s Article 10 and its prohibition of processing of data relating to criminal convictions or criminal offences unless authorised by EU or Member State law.

Lavery said that there will be potential divergence of approaches between Member States. The solution could be EU or Member state law, but legislation at EU level takes a long time. A quicker solution is legislation at Member State level, and there are some solutions already. In the UK, the DP Act 2018 does facilitate this type of processing as long you have appropriate safeguards. In Ireland, a late amendment to the Data Protection Act 2018 allows regulations to be made permitting processing of Article 10 data where the processing is relevant and proportionate to assess the risk of bribery or corruption, or both, or to prevent bribery or corruption or both.

CONSENT TO MARKETING

“There is ambiguity regarding interaction with the current e-Privacy regime. Many organisations have been confused about whether they need re-consent for marketing, and as a consequence many emails were sent to consumers prior to 25 May addressing this issue. This is clearly an unintended consequence. I do wonder why people who opt-in under e-Privacy have to consent under the GDPR as well. I find this difficult to understand. But in Ireland it is a criminal offence if you get this wrong under e-Privacy, and there have been many prosecutions. Pre-ticked boxes are not sufficient. I do hope that people will recognise that soft opt-in for existing customers was never a proper consent in the first place.”

BIOMETRIC DATA

Using biometric data for identification purposes is regarded as processing a special category of data – probably the legislator did not mean that as a result there would be less use of biometric data, Lavery said. He was advising a company that wanted to use biometric data for identifying staff when they were entering the building – his data protection advice on GDPR was not well received. “This will have a chilling effect. Many countries will not bring on additional legislation to facilitate this type of processing, and explicit consent is an unlikely option.”

PROVISIONS REQUIRING OR ALLOWING LOCAL LAWS

Recital 10 states that the aim of the GDPR is “consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons should be ensured throughout the Union”.

But it is difficult to fully achieve this objective when Member State laws differ from each other. The sheer size of national implementing measures and exemptions indicate that there will be slightly different approaches and the GDPR’s goal may not be met. In Ireland, the Act is 182 pages long, so longer than the GDPR text. However, it also implements the Law Enforcement Directive – again a route that only some Member States have taken.

There is also the question of conflict of laws between the GDPR and law outside the EU. GDPR Article 28(3)(g) refers to retention of personal data by a processor where EU law or the law of a Member State makes it a requirement. A valid and not easily reconciled conflict of law issues arises where an EU controller engages a non-EU processor, particularly in a regulated industry (e.g. in financial services). US service providers typically have record-retention obligations under US law.

Amending existing contracts has caused much more work in many organisations than was envisaged. Lavery said that they have tried to come up with two potential solutions, but they are not perfect and he was seeking views from the audience.

1. Firstly, an organisation could envisage that retaining the data would be part of the processing and that would mirror the requirements in the local law.
2. Secondly, an organisation could be converted from a processor to a controller at the time when they are obliged to retain the data – but this can also be problematic as effectively the data has been left outside the EU, and could infringe the rights of the data subjects.
CONSENT AS A LEGAL BASIS
Organisations experience difficulties with consent as the GDPR sets a high bar. Is that driving a move towards reliance on legitimate interests instead?

Lavery said some have argued that this will result in data subjects being less actively involved in managing the processing of their data, as relying on legitimate interests moves the decision-making back to the controller. As a consequence, does the legal basis become less obvious to data subjects – included in long transparency notices – and maybe unlikely to be read? Lavery did not agree with this hypothesis – as long as controllers provide enough information about their processing and conduct a proper balancing test, there is no problem.

OTHER ISSUES
Lavery also touched on competition concerns – do increased compliance requirements make it more difficult for start-ups to compete with bigger players? Will EU countries be disadvantaged in the fields of AI and Big Data due to our strict rules compared with other regions, Lavery asked.

SOME RESPONSES FROM THE EUROPEAN COMMISSION
The answer came from Karolina Mojzesowicz, Deputy Head of the unit responsible for data protection at the European Commission (DG Justice and Consumers). She said that, in fact, there will be more competition due to the level playing field. Accountability and portability will open up the market, she said. When consumers trust companies with their data, and choose the companies that have privacy friendly services, privacy will bring competitive advantages. Other regions will follow GDPR standards.

Data protection developments in the Nordic countries

In May, the Data Protection Authorities of Denmark, Norway, Sweden, Iceland, Finland and the Aland islands decided on enhanced cooperation. Their Copenhagen Declaration says that they will together develop guidance materials to share the work across the offices, and facilitate organisations’ Data Protection Impact Assessments (DPIAs) by developing a list that defines common situations where a DPIA is required. In addition, the authorities promise to work together on data breach notifications to assess which are the most severe cases that require further attention.

The authorities agreed to conduct investigations to ensure that public authorities have appointed a Data Protection Officer, with a follow-up in case of non-compliance. In June, Sweden’s Data Protection Authority announced that it is investigating whether companies and authorities obliged to designate a so-called Data Protection Officer have really done so.

In the first instance, private healthcare providers, public transport providers, insurance companies, telecoms operators, trade unions and banks will be inspected. The results will be ready by the end of August.

SWEDEN
Swedew has updated its law according to the GDPR – the new law was adopted on 18 May and it entered into force on 25 May 2018. The general Swedish derogations are found in the act with supplementary provisions to the GDPR (Sw. Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning), a spokesman for Sweden’s Data Protection Authority said.

“The act regulates the minimum age for children’s consent to processing of personal data when using information society services. The minimum age is 13 years. The act and the GDPR will not apply to the extent it would be in conflict with the Swedish Freedom of the Press Act or the Swedish Fundamental Law on Freedom of Expression. Administrative fines apply to both the private and public sectors, but the maximum limits are 5 million and 10 million Swedish kronor. Among other things, the act contains limitations regarding the processing of Swedish personal identity numbers and coordination numbers and personal data relating to criminal convictions and offences.”

There are numerous other acts include derogations applicable to processing of personal data within a certain sector, body or database, e.g. acts regulating camera surveillance, processing of personal data within the healthcare sector and the Swedish Tax Agency’s processing of population and taxation data.

FINLAND
In Finland, the draft law is still at the Committee stage, and will be debated in a plenary session in Parliament.
California passes strictest data privacy law in the US

Businesses covered by the new Act must work towards meeting the requirements before 1 January 2020. Michelle Hon Donovan and Sandra A. Jeskie of Duane Morris LLP report from California.

On 28 June 2018, California passed the California Consumer Privacy Act of 2018 (CCPA), establishing the strictest data privacy law in the United States. It includes the consumers’ right to know what personal information is collected and the purposes for which this information will be used, to whom this information is sold or disclosed, the right to opt out of the sale of personal information, and the right to access their personal information and (with some exceptions)

Japan’s proposed EU adequacy assessment: Substantive issues

What are the underlying issues behind the EU and Japan’s mutual adequacy decision? Graham Greenleaf assesses what has been achieved and what is still to be resolved.

On 17 July 2018, the European Commission announced that: “The EU and Japan successfully concluded today their talks on reciprocal adequacy. They agreed to recognise each other’s data protection systems as ‘equivalent’, which will allow data to flow safely between the EU and Japan. Each side will now launch its relevant internal procedures for the adoption of its
Japan and EU strike trade deal and agree on adequacy

Japan and the EU have agreed to recognise each other’s data protection systems as “equivalent”, which will allow data to flow safely between the EU and Japan. But the agreement has not been finalised and there may be hurdles along the way, as Graham Greenleaf points out (p.1). Although starting further ahead, could a reciprocal adequacy agreement also be a way forward for the UK?

In California, a new data protection law includes many elements of the GDPR (p.1) and the same may be the case for Brazil’s data protection regulation which is now in the pipeline (p.18).

Within the EU, Member States are making progress in adopting their GDPR adaptation laws. Romania’s new law entered into force on 31 July (p.22). On 17 July, Hungary’s Parliament adopted the national law supplementing the GDPR. The majority of the companies there are micro-enterprises, which may regard the GDPR’s administrative requirements as a burden. PL&B understands that the DPA will not in the first place impose administrative fines on SMEs in Hungary, but will issue warnings.

At the Facebook/Cambridge Analytica hearing on 25 June at the European Parliament, Andrea Jelinek, Chair of the European Data Protection Board (EDPB), said that it is already investigating more than 20 cross-border complaints. Ireland’s DP Commissioner would have been the lead authority if this case had started after the GDPR applied in May. But the UK’s ICO is the investigating authority; its work started last year. Elizabeth Denham, the UK’s Information Commissioner, announced on 28 July that “we’re committed to completing the majority of our enforcement work and further findings by the end of October.”

What will be the extent of regulators’ fines under the GDPR, and what kind of infringement is likely to result in a maximum fine (p.13). Will there be any differences of fining practice in countries, such as Denmark, with no previous experience of the DPA directly imposing this sanction?

Now that stakeholders are looking into the details of the GDPR, it emerges that there may be some unintended consequences of the law (p.9). National fragmentation is inevitable to some degree, even if the EU monitors national legislation to ensure that Member States stay within the GDPR’s framework.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

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
Six issues published annually

PL&B’s International Report will help you to:
Stay informed of data protection legislative developments in 100+ 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 tribunal 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.

Included in your subscription:

1. Online search functionality
   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.

2. Electronic Access
   We will email you the PDF edition which you can also access via the PL&B website. You may also choose to receive one printed copy.

3. E-Mail Updates
   E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
   Access all the PL&B International Report back issues since 1987.

5. Special Reports
   Access PL&B special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
   Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and PL&B Annual International Conferences, in July, in Cambridge, UK.

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

To Subscribe: [www.privacylaws.com/subscribe](http://www.privacylaws.com/subscribe)

"PL&B’s International Report is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network"

Subscription Fees

Single User Access
International Edition £550 + VAT*
UK Edition £440 + VAT*
UK & International Combined Edition £880 + VAT*

* VAT only applies to UK based subscribers

Multi User Access
Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts
Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):
Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30
Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

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

Privacy Laws & Business also publishes the United Kingdom Report.
[www.privacylaws.com/UK](http://www.privacylaws.com/UK)