Who will get the first big GDPR fine – and how to avoid it

Eduardo Ustaran of Hogan Lovells UK ponders the sort of activities likely to prompt regulators into exercising their increased fining powers under the EU GDPR. Reported by **Tom Cooper**.

The potential of data protection fines of up to 4 per cent of global turnover under the EU General Data Protection Regulation (GDPR) has generated something close to "panic". Eduardo Ustaran, a partner at Hogan Lovells in London, says now is the time for some "objectivity" when it comes to fines. "In 20 years of practising in this area I have never seen this degree of panic, anxiety and stress," he told *PL&B's* 31st Annual International Conference on 2 July. While there is a lot of talk about fines, there is not enough discussion of what you have to do to incur a large fine, he said.

A fine can be triggered by:

- Breaching any of the basic principles of processing, including the conditions for consent
- Not respecting data subjects' rights
- Not getting international transfers right
- Breaching national laws
- Being dismissive towards the regulator.

Principles of processing

The principles of data protection have not fundamentally changed under the GDPR, Ustaran told the audience at St John's College Cambridge. "They are at the core of what European data protection law is about, and always has been about," he said.

These principles are:

1. How to be transparent.
2. What are lawful grounds for processing?
3. What amounts to valid consent?
4. How to rely on legitimate interests.
5. How to respect data minimisation.
6. How long to keep the data.

Data minimisation, for example, has "always been there with a different name," he said. "But now, we have to understand what it means, or we are in serious trouble. Similarly, "you should have all had data retention policies for 25 years!"

Despite the essentials remaining the same, the consequences for transgressing are higher, and the GDPR has injected a degree of uncertainty. "Now these issues – despite being basic, despite being essential, suddenly become more difficult," Ustaran said. "We are going to see real legal battles over things like 'I got your consent; no, you didn't'. That dispute will go all the way to the Court of Justice of the EU (CJEU) – "something as simple as that".

Regulators are going to be paying attention to the "difficult essentials," he said. "It is really important that we nail these basic issues."

Data subjects' rights

One of the objectives of the legislation is to "change the emphasis" and make individuals more aware of their rights as data subjects, Ustaran said, "the rights, which have always been there, that have always been underused. There are signs this is working. "I am surprised that there has been the uptake that I have seen, in just a few weeks, of subject access requests (SARs) and data deletion requests. We will see if that carries on," he said.

"This is an area that businesses are not well prepared for because this had not been a massive deal." In the past there was the odd SAR. Now organisations are not prepared to deal with "industrial scale" SARs or data deletion requests. "We need to pay attention to what processes are in place to deal with them because the consequences can be severe."

International transfers

The consequences of "failing" at international transfers are now serious. This area has received "less attention in the last year, at a time when there is more uncertainty than ever before," Ustaran said. The EU-US Privacy Shield could end with the next Presidential Tweet. Model Clauses could fall with a CJEU ruling due next year. Maybe Binding Corporate Rules (BCRs) offer some refuge? "What is going to happen? If anything is going to survive the argument that we are protecting data anywhere in the world it goes, it will be having gone through the scrutiny of having your BCR approved," Ustaran said.

National variations

National variations in implementing the GDPR affect areas such as freedom

of expression, processing employment data, and research data. Organisations should be wary of inconsistencies. "Everyone is a data controller of employee data," he said. And mistakes could have "possibly dire consequences."

Regulators

Ignoring or even irritating a regulator is not a wise choice. "If you annoy a regulator by your attitude – by becoming too arrogant, defensive or [with a] 'you got it wrong we got it right' attitude – what do you think a regulator is going to do?" Ustaran said.

"I'm not saying do everything a regulator is saying." Regulators can be right and can also make mistakes, but "if you don't listen to what they are saying, you don't know what their position is."

In terms of what regulators have said already, the UK Information Commissioner's Office (ICO) has mentioned cyber security, Artificial Intelligence and device tracking as priority areas. The approach to security is going to change, Ustaran said. "Not because the law changes its approach – appropriate technical and organisational measures is not a new expression – what is new is that as of 25 May we are required to notify if not all at least the risky breaches, to the regulator. That means visibility," he said.

Ireland's Data Protection Commissioner had highlighted priorities including large scale processing and high-risk data, online tracking and profiling, special categories of data, emerging technologies and Artificial Intelligence, as well as automated decision making and profiling.

Who will get the first big fine?

Putting all that together, what is the answer to the potentially multi-million-euro question? Ustaran said it isn't possible to name names, but a "risk profile" was clear. The first big fine was likely to involve:

1. A sophisticated technological development. "This is the kind of thing that develops so quickly you don't think – you just want to make things happen at a speed the regulators can't operate at."
2. Big Data.
3. Tracking and/or 'high risk' profiling. "Knowing who you are, what you are likely to like, how you are likely to react. How can I manipulate what you do next? That is going to get the attention of regulators," he said. There is no definition of 'high risk' as such. But reading GDPR article 22, on automated individual decision-making, including profiling, and considering the way regulators are interpreting that article, reveals "very clearly" their fears. "That technology is going to be used in a way that the collection of information about people is going to be used to deprive us of opportunities, information" or the right to do things others can, he said.
4. A surreptitious element.
5. Hostility to regulatory scrutiny. An arrogant attitude of "this shouldn't happen to me, I am disrupting and you are interfering" may play well with the shareholders. "It will not play well with the regulator."
6. A whistleblower or data security breach. One, or both, of these will trigger the investigation, he said.

How to avoid a fine

"Try to comply with the law," Ustaran said. "Because in reality I have observed corporate cultures where the intention is not to comply with the law." Effort is for example spent on "escaping" the territorial scope of the GDPR (Article 3), rather than accepting where it applies. A better approach is to "make a plan, make a list, decide what is important. You are going to have to do something – so nail the basics."

"We don't know what 'compliant' is going to look like – it is going to develop over time," he said. "We are going to be deciding what the scope of legitimate interest is for the next 20 years." So apply your "strategic thinking" to the basic issues. "The GDPR even has a tool for making you think about those basic issues – it is called the Data Protection Impact Assessment (DPIA)."

DPIAs have two benefits. "You may find the right answer for how to comply with the law," he said. "Not only that, complying with the law is difficult in practice. But if you have tried, and you have evidence you have tried, that is at least going to allow you to make the argument you are trying – and that is very important."

On top of listening to regulators, doing DPIAs and nailing the basics, if you are still struggling, Ustaran said, try "thinking like a data subject." Legitimate Interest, for example is one of the most "complicated terms" in the law. At the end of the day it is about what the data subject thinks. That is it," he said.

"If you do all of that, maybe just maybe you will stay out of trouble," Ustaran concluded.

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

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)

Continued on p.3

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[1] 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

Continued on p.4

Issue 154 **August 2018**

INTERNATIONAL report

ISSUE NO 154 **AUGUST 2018**

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
Sandra A. Jeskie and Michelle Hon Donovan
Duane Morris LLP, California, US

Robert Waixel
Anglia Ruskin University, UK

Helen Moores
Information Commissioner's Office, UK

Matteo Colombo
Labor Project, Italy

Stefania Tonutti
PL&B Correspondent, Italy

Nicola Fulford
is to join Hogan Lovells, 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
Fax: +44 (0)20 8868 5215
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"

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

"*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