Think tank says DPAs should fine only seriously negligent conduct

With an increasing array of duties, DPAs have to prioritise to be able to function effectively. This could mean not investigating all complaints. **Laura Linkomies** reports from Hong Kong.

A discussion paper by the Centre for Information Policy Leadership (CIPL) evaluates how Data Protection Authorities (DPAs) can maximise their effectiveness in the modern information age. The think tank suggests that DPAs globally should produce cost-effective outcomes, which effectively protect individuals in practice, promote responsible data use and facilitate prosperity and innovation.

In Europe, the GDPR imposes many more tasks on DPAs, yet their budgets are often meagre. However, the authors of the discussion paper say that "nothing in the GDPR, or in laws elsewhere in the world, prevents the development of a more strategic, results-based approach." Part of this thinking is that DPAs should not investigate every single complaint but "be selective to be effective". This approach suggests that DPAs would identify the most pressing problems and sectors to concentrate on and therefore be able to concentrate their investigative and enforcement efforts on the worst offenders. This idea and the other proposals in the paper were discussed at the DPAs' international conference in Hong Kong on 25 September.

Risk-based approach

CPIL says that effective regulators adopt a risk-based approach – this is particularly relevant in the GDPR context. There should be constructive engagement between accountable regulated organisations, effective DPAs, media, and market forces.

"Only seriously negligent conduct should be fined", said *Richard Thomas*, CIPL's Global Strategy Advisor and previous UK Information Commissioner. "We recommend prevention rather than cure. Accountable organisations should be given incentives for good compliance – authorities should pay less attention towards them, and enforce against the wrong-doers."

Most organisations follow leaders, Thomas said. DPAs need to identify the leaders that are doing their very best to comply and others in the sector will follow them. Singapore is already experimenting with the idea of a regulatory sandbox – allowing companies regulatory space to experiment with new ideas – and this is also happening in the UK with the Financial Conduct Authority.

"We are not telling DPAs what to do, just giving them ideas. They must decide for themselves what works and is right. This paper might provide a framework – and we encourage feedback."

New approach to complaints handling?

"Though the need to deal with individual complaints can be an important component of protecting individuals, handling high volumes is very resource intensive and can impede wider strategic goals. Complaints should be tightly managed with clear criteria to determine the extent of the investigation, also taking into account that complaints are a valuable source of intelligence," the paper says.

Helen Dixon, Ireland's Data Protection Commissioner, said that she welcomes the discussion paper as it starts an important conversation. However, she said that she does not fully agree with the observation that there is currently no prioritisation: the EU DPAs' Article 29 group has talked about a risk based approach.

"There is a very small danger of some contradiction in outcomes focused regulation – and to reward good compliance. A firm that has top-class compliance may still have a serious breach as a result of individual action."

She said that complaint handling should not swamp the DPA's work, but also said that this is a little bit more difficult in the European context. It is often very difficult to dismiss vexatious and frivolous complaints, and sometimes they are difficult to identify, she said, referring to the *Schrems* case where the court said that Irish DPA had a responsibility to fully investigate.

"But we need to take a more strategic approach and investigate the more serious breaches. I have had bad reaction to this idea when I have spoken about it. Now the GDPR gives individuals the right to go to the courts. Lawyers will first seek DPAs to issue a decision before going to courts, so a whole new industry is opening up here. CIPL's ideas are interesting but moving in this direction is more difficult than you suggest."

The GDPR prescribes that DPAs shall handle complaints lodged by a data subject, or by a body, organisation or association, and investigate, to the extent appropriate, the subject matter of the complaint. *PL&B* asked Richard Thomas whether the approach that the CIPL is proposing is in contrast with the GDPR or other national privacy laws in this respect. "We recognise that the approach we put forward is perhaps an idealised approach – it is not driven specifically by any piece of legislation. We have had regard to the GDPR – it poses a duty to handle complaints but there is a degree of discretion to the DPAs. On the face of it, there is a duty as Helen Dixon said but sometimes a more pragmatic approach is required. I do not think there is a direct conflict in what we are saying, certainly publishing guidance and supporting organisations to get it right is what is encouraged by the GDPR."

"The wider point is that the GDPR imposes 21 separate duties on the DPAs. I do not think that any DPA can fulfil all of those tasks – there has to be some latitude in their approach."

Thomas said that during his time at the ICO, the office adopted a risk-based strategy and set out the various factors to take into account. "We identified

different harms to individuals and society, the seriousness of the harm, the likelihood of the risk materialising. As to how to evaluate where to intervene - complaints is one of the sources of information but not the only one – you have to be close to the marketplace. And engage and talk to people, as at the end of the day it is a judgement call."

Hugh Stevenson from the US Federal Trade Commission said that much of what is in the paper resonates with what is done at the FTC. Regulators need a risk based approach – but what are the issues that people see as most pressing? And where can we really make a difference to consumer welfare, he asked?

He said that it does not encourage complaints if not everything is investigated. "But I appreciate the aspect of investigating the ones that pose most risk."

There was a discussion about the possibility of making organisations the first point of call for individuals who have a complaint. *Christopher Hodges*, Professor of Justice Systems, Centre for Socio-Legal Studies, University of Oxford, said that a consumer ombudsman serves this role. But Richard Thomas observed that during his term of office at the UK ICO, it received 25,000 complaints a year, and the majority of individuals had already been in contact with the organisation in question. However, not all cases were about data protection issues, but individuals were pursuing a labour dispute, for example.

Benefits for companies

The paper suggests that organisations trying to behave responsibly and to "get it right" should be encouraged to identify themselves, for example by transparently demonstrating their accountability, their privacy and risk management programmes, the influence of their DPOs and their use of seal/certification programmes, Binding Corporate Rules, Cross Border Privacy Rules and other accountability frameworks.

"I think that at the very general level, if an organisation can demonstrate accountability – it may have certifications or trust marks, and a privacy management programme – then the regulator should give them less attention," Thomas said.

He said that the track record of a particular organisation could have an effect on whether the DPA would fine at all, and also on the amount of the fine.

The CPIL recommends that DPAs should treat organisations in a consistent manner adopting similar approaches across and within sectors, irrespective of the type or geographical reach of the organisation.

Models of regulation

Professor Hodges spoke about models of regulation and compliance. He said that there are two broad approaches to enforcement:

1. **Authority, breach, enforcement**: classic commander enforcer. No deterrence there, however.
2. **Social framework**: parties agree what is acceptable – an inclusive club. Trust drives this model. Everyone deals differently with the ones they trust.

He cited the example of civil aviation which has an open, no blame culture, where actors learn from their mistakes. He concluded that "it is not the question about the law but how you enforce and apply it."

Giovanni Buttarelli, European Data Protection Supervisor, said: "I appreciate the paper but I disagree with some points. It is nevertheless a stimulating contribution on how we may improve. DPAs are increasingly under time pressure, there are growing expectations because of the GDPR and also many are under-staffed with limited budgets. Accountability should be the motto also for DPAs. We need to be more authoritative and more efficient. And extremely severe where needed."

He said that regarding GDPR implementation, guidance from the European Data Protection Board (EDPB) will play an important role. He said that DPAs should use more technology and be more predictable to organisations. He also commented that we are underestimating the increased fragmentation of rulings by national courts. DPAs should do more to insist on exchange of expertise.

Stephen Wong, Hong Kong's Privacy Commissioner said his office used to be in favour of enforcement. But the maximum fine, even after the amendment to the Ordinance is only about US$4,000. No administrative fines are available, only court orders after lengthy administrative proceedings.

"More carrots are therefore needed. We recently issued a privacy management programme. The other area of work where we are dedicating more resources is public consultations. And we respond proactively to consultations as well. I took over the post of Commissioner two years ago and now have managed to engage industry in formal or informal meetings. I want to understand their concerns and explain what our expectations are, and help them to comply."

What is next

Thomas recognised that there may be some scepticism amongst international DPAs on CIPL's ideas, but he stressed that these issues have been addressed in almost every other field. "There is almost a universal consensus that the priority should be to help organisations get it right. You use the stick in those cases where you need it but not as a first point of call."

The CIPL anticipates that, in due course, it will put the questions it has identified in open letters to the leaders of the International Conference, the EU Article 29 Data Protection Working Party, the European Data Protection Board, the Asia Pacific Privacy Authorities (APPA) forum, GPEN and the APEC Cross-border Privacy Enforcement Arrangement (CPEA).

INFORMATION

CIPL was founded in 2001 by Hunton & Williams LLP and leading companies. The discussion paper can be found at www.informationpolicycentre.com/

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

East meets West: Converging regimes, different approaches

Data Protection Authorities discussed legislative frameworks, data transfers and new technologies at their 39th International Conference. **Laura Linkomies** reports from Hong Kong.

The conference was attended by more than 750 representatives from Data Protection Authorities, policymakers, government and business leaders. The DPAs, in their closed session, accepted as new members the Data Protection Authorities of Japan, Montenegro, South Africa and Turkey, and Belgium's Supervisory Authority for Police Information Management.

The DPAs adopted resolutions on automated vehicles (p.30),

Continued on p.3

Poland takes further steps to adjust to the GDPR

DPA to conduct inspections without prior notification. Specific rules for processing of employee data. By **Joanna Tomaszewska** and **Filip Drgas** of Spaczyński, Szczepaniak & Wspólnicy, Warsaw.

After a few months of silence (following the announcement of the partial draft of the new data protection law in March 2017 – the "March Proposal"), Poland's Ministry of Digital Affairs has finally published the draft of the new act on data protection and the draft of a separate act seeking to implement the GDPR into Polish law in sectoral provisions (both proposals are referred to as the "Draft").

Continued on p.5

Issue 149 **October 2017**

INTERNATIONAL report

ISSUE NO 149 OCTOBER 2017

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.thomas@privacylaws.com

CONTRIBUTORS
Robert Belair
Arnall Golden Gregory LLP, US

Sarah Cadiot
Wilson Sonsini Goodrich & Rosati, Belgium

Rainer Knyrim
Knyrim Trieb Attorneys at Law, Austria

Whon-il Park
Kyung Hee University, South Korea

John Selby
Macquarie University, Australia

Joanna Tomaszewska and Filip Drgas
Spaczyński, Szczepaniak & Wspólnicy, Poland

Patricia Gelabert
PL&B Correspondent

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

Can the GDPR create a new global standard?

European privacy principles and the GDPR have a huge impact outside of Europe (p.21). In the US, companies are signing up to the EU-US Privacy Shield to ensure continued data flows, but the arrangement's future is still not certain, although the first year looks promising (p.12). The first annual review started 18 September, and the EU Commission should release its assessment any day now, to be followed by a separate report by the EU Data Protection Authorities (p.9).

At the Data Protection Authorities' 39th International Conference in Hong Kong in September which I attended with *PL&B* publisher Stewart Dresner and Asia-Pacific Editor, Professor Graham Greenleaf, many speakers from Asian countries told the participants how they are preparing for the GDPR. The Hong Kong Privacy Commissioner's Office has developed a Privacy Management Programme to mark a strategic shift from compliance to accountability. This is one of the examples of how the thinking in the East meets West (p.1), even if there is not a common regulatory framework.

South Korea has applied for an EU adequacy decision but our correspondent says that it may have to be satisfied with a partial adequacy assessment in the area of information and communications networks (p.23). Read an overview of privacy developments in South Asian countries on p.18, and a short summary of the Asian Privacy Scholars Network conference which discussed a wide range of topical privacy issues (p.29).

Country-specific reports in this issue discuss GDPR implementation in Poland (p.1) and Austria (p.10), and how it also affects data protection in a European Economic Area country, Iceland (p.16). In addition, we report on the Belgian DPA's recommendation on the role of Data Protection Officers (p.7). Progress is being made with GDPR implementation in Spain and Ireland, and we will report on them in a future issue. We are also following closely in our UK Report (to be published next month) progress on the UK's draft DP law which will implement both the GDPR and the so-called Police Directive (p.17). If you would like to inform us of GDPR implementation in your country, please contact me.

In this issue, we also report for the first time on the work of the United Nations Special Rapporteur on the Right to Privacy (p.27), and data privacy and intellectual property challenges with the Industrial Internet of Things (p.25).

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