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.

East, West... from p.1

collaboration between DPAs and consumer organisations, and further options for enforcement cooperation, and elected France's DPA Authority's (CNIL) President Isabelle Falque-Pierrotin as the new President of the conference. It has been decided that the 2018 conference will be jointly organised by the European Data Protection Supervisor (EDPS in Belgium) and Bulgaria's DPA. In 2019, it will be Albania's turn.

Stephen Wong, Hong Kong's Privacy Commissioner, welcoming the delegates, noted that there were 80 DPAs present. He said that his office would organise information sessions about how the EU GDPR affects companies outside of the EU, including Hong Kong. "In my office, the number of data breach notifications we receive has rapidly increased. We will publish guidelines in a few months' time. We must pay attention to the GDPR, and help businesses to understand the implications including data transfers. If their processing is targeting EU data subjects, they are caught. Interoperability and DPA cooperation are now crucial," he said.

The global regulatory landscape

Julie Brill, Corporate Vice President at Microsoft (former US Federal Trade Commissioner) spoke in the session on the global regulatory landscape. She said that Japan's and Korea's governments are creating regulatory frameworks that align with the GDPR. Both are seeking adequacy decisions. Also the Hong Kong Ordinance is being reviewed to see what changes are needed in light of the GDPR.

"The Privacy Shield could be a model for other jurisdictions. It is a reference point for Japan in its discussions with the European authorities, and also for China. The APEC developments are also encouraging," Brill said.

She said that law enforcement access to data is critical. Microsoft has played a leading role in ensuring appropriate access whilst protecting privacy. "We sued the US government to stop them accessing an email that was on a server in Ireland. The US Court of Appeal ruled in our favour. In July this year the case went to the US Supreme Court. We chose to go to court as this issue poses key questions for us and around the world. The US congress is now considering legislation in this field which would modernise the ageing framework. We strongly support the passage of this bill. But we will not hesitate to go to courts in the future if needed."

Jane Horvath, Senior Director of Global Privacy at Apple said that data localisation laws are causing some concern as they have now become distorted from their original aim. She said that in terms of international transfers, we should build on APEC's Cross Border Privacy Rules (CBPRs). "There is some room for improvement, but we should have mutual recognition between EU Binding Corporate Rules (BCRs) and CBPRs."

Nigel Cory, Trade Policy Analyst, the Information Technology and Innovation Foundation said that he agreed there was a risk to data innovation and free flow of data as a result of data localisation laws. He has identified 34 countries with some form of data localisation, with China, Russia, Indonesia, and Vietnam at the forefront.

"Many policymakers believe that data is more secure if kept within borders. However, a cyber security breach can happen regardless of where the data is stored. Data security depends on the service provider's security measures. This is where we should concentrate."

He said that sometimes countries want to facilitate government access to data, and compel everyone in the country to use the local service providers. This discriminates against foreign firms. There is a clear need to update legal treaties to come into the digital age. New rules at the international level are also needed.

Dr Hiroshi Miyashita, Associate Professor of Chuo University, Japan, said that in Asian jurisdictions there are many different data transfer provisions. The reasons for restricting data exports vary from human rights aspects to trade. He said that in Japan the trust mark is now used by some 15,000 companies. He believes that the system, JIPDEC, will spread in the APEC region. There are many similarities between CBPRs and BCRs, but also differences. Personal data is not a commodity, he said.

Bruno Gencarelli, Head of the EU Commission's Data Protection Unit spoke about increasing convergence between privacy laws. "This is not a European obsession. In India, an important ruling just recognised privacy as a fundamental right. Also, we have a growing membership of Council of Europe Convention 108. Asia Pacific is missing in that arena, however. The EU communication on our international strategy in January confirmed that we are committed to developing tools for convergence."

Significant progress has been made with Japan's adequacy application and a result is expected next year. He indicated that the Commission would ensure the continuity of existing adequacy decisions. The EU-US Privacy Shield could be used as a model in other countries.

With regard to possible synergies between the GDPR and APEC, he said that both partners need to do more work.

Jennifer Stoddard, former Privacy Commissioner of Canada and now Regulatory Advisor with Nymity, said that the recent EU position on adequacy is a milestone in international DP attitudes. "I am encouraged that the EU is working on adequacy, and to see a totally new approach under Gencarelli's leadership," she said.

In the law enforcement area, we have to recognise that citizens' data is exported and set limits, she said. Adequacy is not a one-way street. Sectoral adequacy is possible under the GDPR. Stoddard suggested that the EU should issue a checklist for countries so that they can estimate how long it might take to reach adequacy. Cities might like to become adequate for trade purposes, she said.

Gencarelli responded that the EU Article 29 Data Protection Working Party is now reviewing adequacy requirements in light of the GDPR. "In the past years, the process has become much more transparent. Discussions are very technical. Now political sensitivity is such that there is more transparency. The Canadian adequacy decision and the EU-US Privacy Shield are partial adequacy decisions. In partial decisions, we always also have a look at public access to data just like in a full adequacy decision, but it is true that they can be geographically specific or industry specific."

Privacy and ethics in Artificial Intelligence

Marty Abrams, Chief Strategist at the Information Accountability Foundation spoke about their research paper.[1] "AI, when applied, can make decisions for people rather than suggesting the decisions that should be made. Collision avoidance braking was once an AI experiment. It is now the way new cars work. Increasingly we will want more technology to simply take care of things. Unlike previous disruptive technologies, with these technologies there is less opportunity for human intervention at the point of decision. This is a good thing; but how do we provide an assurance of fairness when how things work will be less obvious?"

"We begin with how do we build values into AI design objectives and which values might they be? Accountability requires data stewardship. To make accountability work, we believe stewardship needs an upgrade. It needs to be enhanced for this world where machines make decisions for people. We call the new level of stewardship stakeholder-focused stewardship. It requires organizations to be open about their values and how those values will be applied. It also requires companies to understand the stakeholders impacted by AI and how they will balance the interests of the various stakeholders."

Wojciech Wiewiorowski, Assistant European Data Protection Supervisor said that with AI, a practical approach with engineers is important as AI also includes human design. "We promote ethics but need to also create awareness in stakeholders. At EDPS, we have created a group of engineers dealing with Privacy by Design."

Simon Longstaff, Executive Director at the Ethics Centre said that many companies have wonderful descriptions in their policies but sometimes their actions are very different.

JoAnn Stonier, Executive Vice President at Mastercard explained that we are at the beginning of a mind-shift and cultural shift that has to start in our organisations. We are all struggling with AI, she said. "Data stewardship, as described in the paper is more complex than currently practised in my organisation. Our programme has been legal and regulation based. Now the paper is talking about value-based programmes. How should cultural differences impact how values are set? Is there a tension between values in law and ethical values?"

Worapat Patram, Director of Public Policy, Intel Microelectronics, Thailand, explained that at his organisation, his team sit together with engineers and policy managers and lawyers and try to figure out the technical requirements, as well as the regulatory requirements. Then the more difficult area, ethics.

"One example is autonomous cars. The car learns from its changing environment. If taught in Europe, it is different from Asia. Many South East Asian countries are still considering privacy laws."

Cybersecurity versus data protection

Speaking at the session about the rise of cyber security, UK Information Commissioner, *Elizabeth Denham*, said that under the new EU Cyber Security Directive which the UK is also implementing, the ICO receives breach notifications in the digital sector. She is worried that her office may be swamped by cyber notifications and this will take resources away from privacy work. "Our regulatory remit is changing, and more coordination is needed. We have the national cyber security centre – they are responsible for issuing guidance but they are not a regulator. So we need to work with the Government Communications Headquarters (GCHQ)."

Denham said that 85% of fines related to general data breaches are in fact security incidents. "In terms of resources, we now have an opportunity to partner with other agencies. We need to purchase appropriate software, and set up strategy groups. But will there be overinvestment on cyber attacks? I wonder if cyber is swamping operations at other organisations?"

She said that the ICO is working on a joined-up approach between the regulators. Does the GDPR help? "We will have to wait and see. My hope is that GDPR will enable more robust protection for all data. Boards think that security is the same as privacy. That worries me."

Denham said we need to avoid a situation where several agencies would fine for one breach.

Timothy Pilgrim, Australia's Privacy Commissioner spoke about the Australian national census last year which was organised completely online. Whilst it was not the intention to retain data for longer than necessary, this was not communicated as well as it should have been. There was a cyber attack, and the government quite rightly turned the system off. The Office of the Privacy Commissioner investigated and luckily there was no loss of personal data.

"Organisations need to be careful of cyber threats. There is now a cultural change within our government structure. We contracted in cyber experts for the investigation as this work is resource intensive. Now, the Data Breach Law on mandatory notification will come into effect in Australia in February 2018."

Privacy in Asia

Standing Privacy Commissioner of South Korea, *Chaeho Rheem*, explained that privacy culture in Korea has been firmly established since 2000. The law provides sanctions of imprisonment of up to ten years or fines up to 100 million Korean Won (£66,665). It is now under discussion how to strengthen the DPA's powers. A Bill proposed by National Assembly members would make the authority completely independent and increase its enforcement powers.

Singapore DPA's Deputy Commissioner, *Zee-kin Yeong*, said that they are encouraging organisations to move from pure compliance to accountability. The Commission is producing an online tool – a data protection management programme that will help organisations to conduct PIAs, and the office will issue a trust mark by the end of 2018.

Isabelle Falque-Pierrotin, President of France's CNIL said that there are cultural differences, but the regions share many common initiatives, for example Singapore's regulatory sandbox initiative. The CNIL already has this kind of regulatory experiment. In the end we are all trying to reach the same goals

although we have different approaches, she said.

Xiaodong Zuo, Vice President from the China Information Security Research Institute said that culture has a big impact. Individual rights have been historically suppressed in China, as traditionally individual rights have been less important than duties to the family and/or clan but the situation is changing with exponential financial growth. Legal barriers are already in the way of economic development. There is now a cyber security law.

Do differences between East and West result in different enforcement? *Maureen Ohlhausen*, Acting Chairman of the US Federal Trade Commission said that the FTC is now taking the unusual step of publicly saying that it is investigating the recent Equifax breach. Under the FTC Act, a great number of cases have been brought – 500 on data security alone, she said. "We undertake privacy audits and work with foreign enforcers."

Stephen Wong, Hong Kong's Privacy Commissioner said that Hong Kong law does not include class actions, but individuals can get compensation. The office offers legal assistance for individuals to pursue their claims.

INFORMATION

See www.privacyconference2017.org/eng/index.html

REFERENCE

1 informationaccountability.org/wp-content/uploads/Artificial-Intelligence-Ethics-and-Enhanced-Data-Stewardship.pdf

Poland... from p.1

The latter is particularly interesting since it proposes several important changes to data processing in different legal acts, such as in the employment context as well as specific provisions on automated individual decision-making, including profiling in several regulated sectors.

New Data Protection Act

The Draft does not deviate significantly from the March Proposal and aims primarily to adapt the national legal framework to the GDPR regime. The new act will replace the currently binding Data Protection Act of 29 August 1997 (Act). The draft new act covers primarily the following issues:

Data Protection Officer: A data protection officer (DPO) will replace the current counterpart, known in Poland as an information security officer – *administrator bezpieczestwa informacji* (ABI). According to the Draft, a data controller or data processor who appoints a DPO is obliged to inform the Polish Data Protection Authority (DPA) about such an appointment within 14 days of the appointment date. The Polish draft law includes interim provisions regarding the continued functioning of ABIs. These provisions state that pre-appointed ABIs will automatically perform the functions of a DPO as outlined in the GDPR, but only until 1 September 2018. By that date, controllers or processors are obliged to notify the DPA about the appointment of a DPO or to provide information that the current ABI will not perform the DPO's functions. If no such contact details of the up-to-date ABI are provided to the DPA, as of 1 September 2018 any pre-appointed ABIs will automatically cease to perform the functions of a DPO.

Recommendations on data security: The DPA will publish and update from time to time recommendations on the technical and organizational measures aimed at ensuring data security. Such recommendations are eagerly awaited, since they will repeal the currently applicable, detailed secondary legislation on technical data protection documentation, and technical and organizational conditions.

Data breach proceedings: One of the DPA's responsibilities will be to conduct administrative proceedings regarding personal data breaches. The DPA will be entitled not only to impose fines, but also to issue warnings. A warning will be sufficient if the breach is insignificant and the data processing entity has ceased to infringe the law. There will only be one single instance of administrative proceedings with regard to the infringement of the data protection provisions, but the parties will have the right to appeal to the competent administrative courts. Lodging an appeal will suspend the execution of the DPA's decision with respect to any financial fines imposed. It is worth noting that, according to the Draft, the DPA will maintain an online system that will allow controllers to notify it of a personal data breach.

Interim decisions: The draft provisions entitle the DPA to issue interim decisions in the event that it is proven during the administrative proceedings that a given entity has infringed data protection provisions and its further processing may cause serious risks to the privacy of the individuals. By virtue of such a decision, the DPA may restrict the processing of the controller in question.

Inspections: In addition to scheduled and *ad hoc* audits, the DPA will also be entitled to conduct an inspection during the course of administrative proceedings initiated in connection with the breach of data protection provisions. Moreover, the Polish government intends to entitle the DPA to conduct inspections without any prior notification. As a result, it may be crucial for entrepreneurs to draw-up relevant internal codes of conduct to be fully prepared for any unannounced DPA inspections.

Certification and accreditation: The Draft regulates the issue of certifying as well as accrediting entities that are entitled to monitor compliance with approved codes of conduct. The DPA will be responsible for certification awarded for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors. The certification criteria will be published at a later stage. The DPA will maintain a publicly-available register of certified controllers and processors. The DPA will also be allowed to conduct inspections to verify whether the certification criteria are met. Furthermore, the DPA will also be responsible for accrediting the bodies entitled to monitor compliance with approved codes of conduct.

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