ABLI’s intra-Asian focus: A new privacy forum

Graham Greenleaf reports from a meeting in Singapore that gathered together almost all of the data protection authorities in the region.

Towards a shared legal ecosystem for international data flows in Asia was the theme of the first Privacy Forum of the Asian Business Law Institute (ABLI, see PL&B International October 2017 p.35) held in Singapore on 7 February 2018. In an opening address, Singapore Chief Justice Sundaresh Menon, Chair of ABLI’s Board, mentioned factors increasing the need for greater consistency between the approaches taken to privacy issues in Asian countries. These include concerns about data localisation heightened by China’s Cybersecurity Law, India’s imminent entry as a significant participant in data privacy debates following the Puttaswamy decision and the White Paper proposals for a new law, and region-wide needs to adjust to the potential of extra-territorial enforcement of the EU’s GDPR.

Who is at the table?
The 90 invited attendees at the Forum came from 18 Asian countries (including New Zealand and Australia) extending from Japan to India. All data protection authorities of the region were represented except Macau and Australia, and various countries without specialised data protection authorities sent senior government or other representatives (Indonesia, Cambodia, Vietnam, China). Representatives of regional business groups, and local lawyers with deep experience in data privacy work made up a significant part of the attendees. There was little direct representation of data subjects by consumer or employee organisations, though they were indirectly represented by civil liberties NGOs and academic experts.

Various Asian-based US business representatives were involved, but the meeting was far less dominated by US speakers than is often the case in the Asia-Pacific. Anti-privacy rhetoric was almost completely absent. The European Commission was represented, due to current regional interest in the GDPR and ongoing adequacy assessments. In the days before and after the Forum, there were numerous side-meetings, including a first-ever closed meeting of Asian DPAs. It is possible that these ABLI Forums and associated meetings could become the principal Asian-focused meetings on privacy. Their coverage of Asian jurisdictions is much broader than the Asia-Pacific Privacy Authorities (APPA) in including government representatives from countries with no DPA, or of APEC data privacy meetings (not India), but at the same time, it is Asia-focused in not including any countries from the Americas. ABLI can provide the only opportunity for Asian (and Australasian) jurisdictions to “talk among themselves”.

Appetiser
For the past six months, ABLI’s main work has been its “descriptive” phase, in which honorary “reporters”, experts from each of the 14 jurisdictions covered, have prepared reports setting out the law and practice of cross-border data transfers in their particular jurisdiction. A draft compilation of these reports of around 200 pages has been distributed to ABLI reporters and chairs, and a final version will be edited and published by ABLI (and available free from its website) in April/May. It will form the basis for the second “prescriptive phase” of the project (in Menon CJ’s words), where the expert group will attempt to recommend paths toward more consistent/interoperable/harmonious laws (there are still many opinions on the best term to describe the objective!).

Five main courses
The Forum was structured around discussion of five topics, with chairs of each session drawing out comments from four or five panellists from numerous countries, and general discussion following each session. Dozens of people contributed to the overall discussion. In the first session on Asian regulatory developments, notable points were:

1. the preparation of a new comprehensive (not sectoral) regulation in Indonesia which would take into account new developments such as the GDPR in a “balanced” way;
2. Japan’s representative did not include the “carve-out” for Anonymous Processed Information (API) as one of the five notable features of its 2015 Act, but did highlight that there was no longer a “small business”/SME exemption;
3. China may introduce into its legislative agenda a separate Personal Information Protection Law, but before that the new Consumer Law will be finalised, as will many regulations now underway, including cross-border transfer regulations;
4. development of a data privacy law is likely to be long process in Cambodia, though it has started; and
5. New Zealand lawyers await with impatience updating of its law in light of Law Reform Commission and Privacy Commissioner recommendations, particularly with respect to ongoing GDPR reviews of existing adequacy determinations. Problems caused by inconsistencies and gaps in Asian data protection laws were addressed in the second session. This involved the identification of twelve areas of substantial differences in the coverage of Asian data privacy laws, and a further ten types of gaps in how various forms of processing are regulated by these laws.2 Panellists identified major practical problems as including more flexible enforcement of some obligations on SMEs. There was general agreement that, significant though these gaps are, they are less significant than the high degree of similarity between Asian data privacy laws, which on average include more than...
Ireland advises on DPO qualifications

Ireland’s Data Protection Commissioner states that the qualifications which a Data Protection Officer (DPO) needs depend on the complexity and sensitivity of data processing in organisations.

The relevant skills and expertise for a DPO include: expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR; understanding of the processing operations carried out; understanding of information technologies and data security; knowledge of the business sector and the organisation; and ability to promote a data protection culture within the organisation. For example, a DPO may need an expert level of knowledge in certain specific IT functions, international data transfers, or familiarity with sector-specific data protection practices such as public sector data processing and data sharing, to adequately perform their duties.

The Data Protection Commissioner recommends that when selecting a DPO training programme, organisations pay attention to:

- the content and means of the training and assessment;
- whether training leading to certification - the standing of the accrediting body; and
- whether the training and certification is recognised internationally.

Spain adopts DPO certification

Spain’s new certification scheme establishes the requirements for Data Protection Officers, as required by the GDPR. DPO’s have to be able to demonstrate at least one of the following criteria:

1. Professional experience of at least five years on projects and/or activities and tasks related to DPO functions regarding data protection.
2. Same as one except three years, plus at least 60 hours of recognised training on subjects related to the programme.
3. Same as two except two years, plus at least 100 hours.
4. At least 180 hours of recognised training on subjects related to the programme.

Spain’s DPA (AEPD) will maintain an updated registry of authorised certification bodies.

REFERENCES

1 Asian Business Law Institute (ABLI) ABLI’s Data Privacy Project [abli.asia/PROJECTS/Data-Privacy-Project] for the programme, opening address etc, see ‘Towards A Shared Legal Ecosystem for International Data Flows in Asia’ [abli.asia/NEWS-EVENTS/Whats-New/ID/52]
Ireland issues Data Protection Bill to implement the GDPR

The long awaited Irish Data Protection Bill was published on 1 February 2018. Paul Lavery of McCann FitzGerald reports on the potentially controversial issues in the Bill.

The Irish Data Protection Bill will now be subject to debate and potential amendment in both of the Irish Houses of Parliament (the Seanad and the Dáil) prior to its expected enactment in advance of 25 May 2018 (when the EU General Data Protection Regulation replaces existing data protection law).

The Bill is to be welcomed as it provides a degree of clarity in respect of certain matters such as exemptions from processing obligations and access requests. But there are regulatory environment. One of the problematic questions is the future of standard contractual clauses.1

In 2016, Ireland’s DPC made an application to Ireland’s High Court to stop the transfer of personal data to the US under the Privacy Shield framework, a framework for facilitating the transfer of personal data from the EU to the US. The DPC argued that the EU-US Privacy Shield does not provide adequate protection for personal data transferred to the US.

Between two Commissions: Views from Dublin and Brussels

At the CPDP conference in Brussels, the use of standard contractual clauses for data transfers stimulated debate between the EU Commission and Ireland’s DPA. By Laura Linkomies.

Bruno Gencarelli, head of Data Protection at the EU Commission’s DG Justice, and Helen Dixon, Ireland’s Data Protection Commissioner (DPC), were on the podium to discuss the changing regulatory environment. One of the problematic questions is the future of standard contractual clauses.1

In 2016, Ireland’s DPC made an application to Ireland’s High Court to stop the transfer of personal data to the US under the Privacy Shield framework, a framework for facilitating the transfer of personal data from the EU to the US. The DPC argued that the EU-US Privacy Shield does not provide adequate protection for personal data transferred to the US.

Continued on p.3
Consistent implementation of GDPR is critical for the EU

As we go to print, only Germany and Austria have adopted new data protection laws that are in line with the EU GDPR (p.8). Some GDPR adaptation laws are in the pipeline but it seems likely that many countries will miss the deadline. In the UK, the Bill has advanced from the House of Lords to the House of Commons, and is expected to be adopted in time for 25 May when the GDPR takes effect. In Ireland, a Bill has now been issued – read an analysis of it on p.1 and Hungary waits for Parliamentary debate on its Bill (p.10). Bills in France and Spain are also making progress. By now, it is evident that there will be many differences and the idea of almost complete harmonisation of the laws is unachievable.

Elsewhere, the impact of the GDPR is felt in different ways. South Korea has applied for an adequacy decision (p.14) and is hoping for a positive finding. Meanwhile, the EU has taken a decision that it will insist on high level data protection standards when it signs future trade deals. According to the Financial Times, a letter, signed by six commissioners has now been sent to MEPs and EU governments. In the US, the EU-US Privacy Shield agreement is being implemented but is also being constantly reviewed (p.17). Several issues may have an impact on the EU Commission’s view on how the pact is working.

My colleague Stewart Dresner and I were in Brussels at the CPDP conference in January and report back on many of the debates we heard there; see p.12 on GDPR data breach notification, and p.7 on GDPR fines, and the practical issues that have already been encountered when preparing for the new law. National DPAs are making preparations for issuing guidance on the GDPR to varying degrees. An interesting development is guidance from Spain’s DPA on Data Protection Officer qualifications (p.21).

All these issues will feature at PL&B’s 31st Annual International Conference, Navigating GDPR: The art of the possible, where we will bring you the latest news on GDPR implementation, Brexit and the UK data protection regime and much more. We have invited a UK government representative to give her views, and, of course, several national DPAs will be there either as speakers or participants. Register now with an early bird discount at www.privacylaws.com (until 28 February).

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