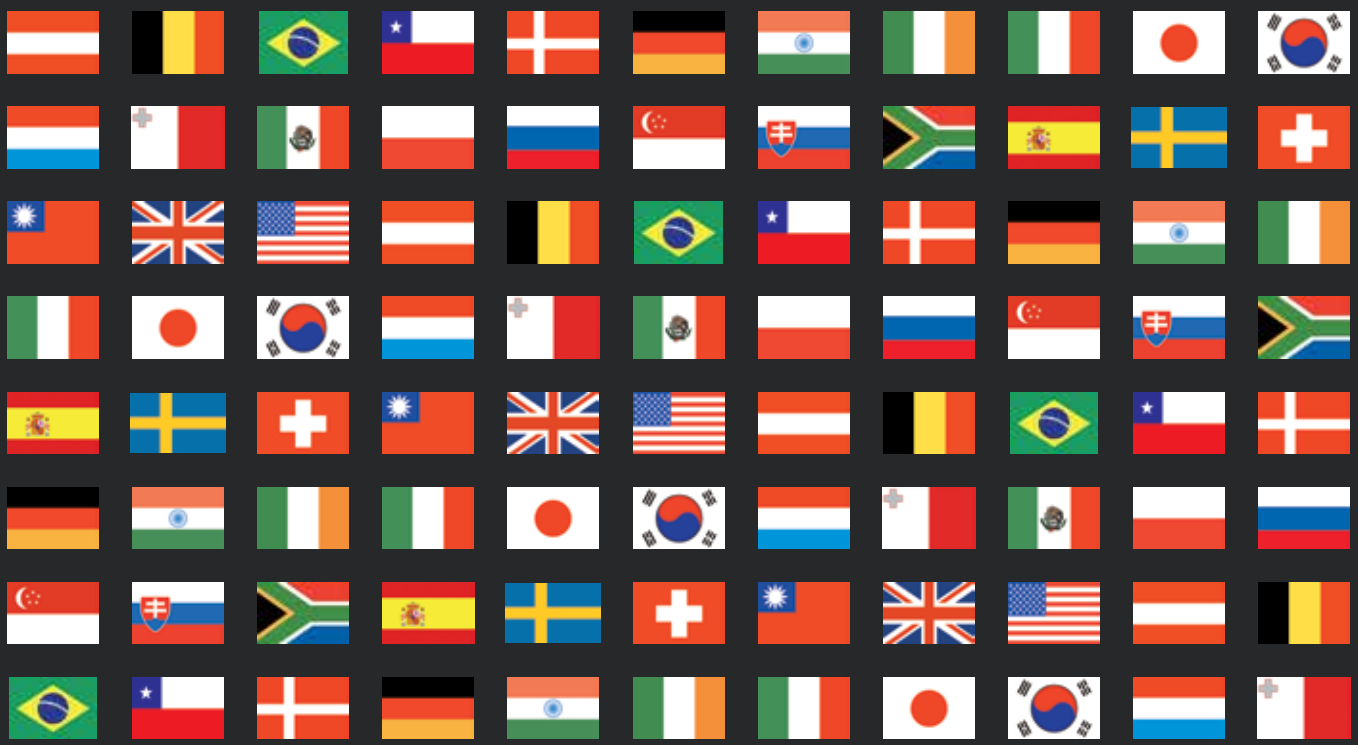
Data Protection & Privacy

Contributing editor
Rosemary P Jay



2016

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2016

Contributing Editor

Rosemary P Jay

Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
Alan Lee
alan.lee@lbresearch.com

Adam Sargent
adam.sargent@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Fourth edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Introduction

Rosemary P Jay
Hunton & Williams

Introduction

The first introduction to this series in 2013 noted the extensive development of data protection or privacy laws[1] and reflected on the commercial and social pressures giving rise to this global development. Those economic and social pressures have not diminished since that edition and nor has the apparently insatiable appetite for law in the field.

This piece aims to highlight the main international developments. However, as data protection laws and initiatives are developing at a dizzying speed, it is likely to be out of date within a few months. Anyone looking at a new project will need to check whether yet more have appeared on the scene since the date of writing.

The continuing growth of legislation further emphasises that the law affecting personal information has become a field in its own right. As information has become ever more necessary to commercial and public life, the laws governing its use have become ever more significant.

The global convergence

In previous editions the variation in the types and content of data privacy laws across jurisdictions has been noted. It has also been noted that, although privacy and data protection laws are far from identical, they do follow the same themes and many have elements in common. There was a point in the development of the data protection field when the more optimistic among the lawyers and policymakers started to make noises about the possibility of 'convergence' between the different families of laws and international standards. The thought was that, gradually, the different approaches would begin to coalesce. Actors would work out common standards enabling a gradual move towards a global standard on data privacy.

While there can be little doubt that a convergence in global approaches to privacy protection would be good for business and arguably for consumers, as it would reduce the need to deal separately with local laws and help consumers benefit from a common set of standards, it is now clear that it will be a long time before standards do converge.

Privacy laws reflect national and cultural attitudes and outlooks as well as different legal traditions and different levels of technological and social development. We are looking at widely different standards for some time yet. A global business looking to introduce or change a business process which involves the use of data about consumers or staff will need to appreciate the areas of broad similarity, the 'families' of law in force and where these 'families' strongly diverge.

International instruments

The various laws have been influenced by a number of international instruments which continue to have a significant influence on the development of law in this domain.

The main international instruments are the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Treaty 108) of the Council of Europe, the OECD Privacy Recommendations and Guidelines (the Guidelines), The European Union Directive 95/46/EC (the Directive) and the APEC Privacy Guidelines. To these must now be added the African Union Convention on CyberSecurity and Personal Data Protection. Treaty 108 has been ratified by 47 countries and those countries have passed laws which implement its standards. The Treaty has been reviewed with the aim of bringing it into closer convergence with Directive 95/46/EC.[2] The OECD Guidelines are not subject to a formal process of adoption but were adopted by the Council of the OECD in 1980. Like Treaty 108, the OECD Guidelines have been reviewed and revisions were agreed in July 2013. Treaty 108 covers the states that belong to the Council of Europe.[3] The OECD covers a wider range of countries including the US, which accepted the Guidelines.

Both Treaty 108 and the OECD Guidelines date from the 1980s. By the 1990s the EU was becoming increasingly concerned about wide variations across the EU in data protection laws and the possibility that trade could be impacted by these variations. The EU passed the Directive which was implemented in EU member states by 1998 and remains the governing instrument for all EU member states.

In 2004 these instruments were joined by a newer international instrument in the form of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. Although it was subject to criticism as being without real force and described as 'OECD lite' when it was launched in fact the Framework has been influential in advancing the privacy debate in the Asia-Pacific region. In November 2011 APEC endorsed its Cross-Border Privacy Rules; a clear indication that the Framework is operating as a focus for the development of privacy protection in the region.

A further international instrument has been proposed, an international Standard on Privacy and Personal Data. The proposal to develop such a Standard was endorsed in 2008 by the 30th International Conference of Privacy and Data Protection Commissioners, a conference which brings together privacy regulators from around the world.

Most recently the African Union adopted a Convention on the establishment of a legal framework for cybersecurity and personal data protection in June 2014. It has been reported that a number of African countries are planning legislation based on the Convention although no country has yet ratified it.[4]

European approach

Data protection laws are a standard feature of European legal systems. Every country in the European Union has legislation based on Directive 95/46/EC. The Directive made it mandatory for all member states of the EU to implement such laws to the EU standard. In the same way the regulation of electronic communications, marketing and the use of cookies follow the requirements of the EU E-Privacy Directive (as amended).[5]

The laws of the member states of the EU and the three associated states in the European Economic Area (that is, Iceland, Lichtenstein and Norway) and Switzerland follow the same pattern. Because the laws are based on a Directive, there remains scope for some local variation. Anyone reviewing the laws needs to be aware that there is scope for national difference in some areas but the variations are limited and the basis and structure of the law is the same in each state. There are wider variations in the broader European area. As an example Russia has a data protection law which is based on the EU standard but has more recently amplified that by an amendment to the law with a purely national aspect.[6] Under these new provisions a localisation requirement is imposed on personal data operators who process personal data on Russian citizens to use databases physically located in Russia.

One of the distinguishing characteristics of the data protection laws of EU member states is the prohibition on the transfer of personal data to any country which is not regarded as offering equivalent protection,[7] unless a derogation applies. This banning provision has operated as an incentive to some non-EU countries to follow the same model as the EU because, where a country adopts a law that is regarded as equivalent to the EU model, the European Commission may make a formal finding that the country offers

equivalent protection. Once such a finding is in operation personal data may flow freely between that country or territory and any EU member state without any further transfer mechanism being implemented by the data transferer. Reviewing the list of those countries which have followed this model, it must be remarked that it has not proved a very strong incentive to date. Those jurisdictions which have applied the EU standards to the required level and had a formal finding of adequacy have, in the main, been dependencies of EU states or those with close historical links to EU states such as the UK Crown Dependencies,[8] the Faroe Islands,[9] Andorra and Switzerland. A number of others have joined the ranks of those which have passed EU style laws, that is Israel, Canada, Uruguay and Argentina. The EU approach has been particularly influential in South America where a number of countries have passed EU style laws and are seeking findings of adequacy from the EU.[10]

Moving outside Europe the picture is far more varied. There can be a tendency (particularly among Europeans) to regard European Union style laws as the 'gold standard'. However, others characterise the EU approach as doctrinaire and inflexible. The US has traditionally been considered (at least among some Europeans) to have less regard for the importance of personal privacy than Europe, however, the US has had a Privacy Act regulating government departments and agencies since 1974 and many US states have their own privacy laws. The US has traditionally adopted a sectoral approach to privacy, for instance it has implemented specific privacy legislation such as the Children's Online Privacy Protection Act 1998 (COPPA). There are current proposals for further developments in the law in the US, although whether they will make it through the legislature remains to be seen. In January 2015 President Obama announced further developments in laws impacting on privacy in three areas. Following that the Personal Data Notification Act has been introduced and went to Congressional Committee in March 2015. The Act would replace the patchwork of data breach notification requirements imposed by State law with one uniform standard. In April 2015 the Student Digital Privacy and Parental Rights Act was proposed to Congress. This Act would restrict the use of data by those who provide apps, websites and other online services for children and give parents the right to see the data collected on children. Finally, a Consumer Privacy Bill of Rights is proposed to strengthen the rights of consumers. A proposal for legislation was published in February 2015 but so far appears to have made little headway. The US also (uniquely) has in place the Safe Harbor scheme, which has been found by the European Commission to be sufficiently stringent to be regarded as offering adequate protection for the transfer of personal data from the EU.[11] This formal finding of adequacy for companies which join and comply with the US Safe Harbor Scheme has been the subject of criticism from the EU following the Snowden revelations, but remains fully in force. The US is the only country in which the European Commission has been prepared to recognise a self-regulatory scheme as offering adequate protection. Canada has had a data privacy law in its Personal Information Protection and Electronic Documents Act 2000 for over a decade as well as several provincial laws.[12] On 18 June 2015 Canada introduced further requirements in the form of mandatory breach notification under the Digital Privacy Act. This has introduced an explicit obligation to notify individuals in cases of breaches, and report to the Office of the Privacy Commissioner.

In Asia-Pacific the early adopters of privacy and data protection laws, Australia, New Zealand and Hong Kong have been joined by Malaysia in 2014,[13] Singapore[14] and South Korea.[15] Australia has also strengthened its regime with the Privacy Amendment (Enhancing Privacy Protection) Act 2012[16] and the APEC Privacy Framework is now supported by the APEC Cross Border Privacy Rules.

South America has seen the passage of laws in Argentina, Uruguay, Columbia, Chile and Peru with Argentina and Uruguay following the EU model. Other South Amercian countries, although they have not enacted EU-style privacy laws, have some degree of constitutional protection for privacy, including a right to habeas data, for example Brazil and Paraguay.

The global gaps in coverage lie in Africa and, to some extent, the Middle East. There are, however, some laws in both regions. As noted earlier the African Union adopted a Convention on the establishment of a legal framework for cybersecurity and personal data protection in June 2014. The Convention has, however, been criticised as both vague and insufficiently focused on privacy rights. It has been reported that a number of African countries are planning legislation based on the Convention although no country has yet ratified it.[17] South Africa has passed law based on EU standards but it is not yet fully in force.[18]

In the Middle East there are several laws that cover specific centres but, apart from Israel, no country yet has comprehensive data protection law.

We are therefore facing a patchwork of different laws and regulations throughout the globe which can make it difficult for global businesses to roll out policies with a common approach. In some countries, consents may be required; in some countries, regulators must be consulted or permissions sought; in some countries, technical requirements must be met. Some laws include public registers, some have special provisions for employees. In this environment the support provided by this publication will be invaluable to those doing business globally.

Current proposals in the European Union

It is to be hoped that eventually a global consensus will triumph over regional differences, but at the moment development continues at uneven pace. Major changes are afoot in the EU since the European Commission in January 2012 delivered its long awaited draft legislative instruments for the reform of the data protection regime in the EU. The two legislative instruments proposed are:

- a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (the draft Regulation);[19] and
- a proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (Police and Criminal Justice Data Protection Directive) (the draft Directive).[20]

The proposed instruments are considered further in the second part of this Introduction. If they are passed, and in particular if the draft Regulation becomes law, it will be the most radical shake-up of data privacy regulation we have seen to date.

The impact of the Regulation will not be confined to businesses based in the EU. The new rules will apply to any processing conducted from outside the EU which involves the offering of goods or services to individuals in the EU or the monitoring of individuals resident in the EU.[21] This ambitious approach to jurisdiction, coupled with the potentially high level of fines, determined by worldwide turnover [22] has raised concern outside as well as within the EU.

The draft Regulation represents a radical proposal in terms of convergence. There will be greater convergence within the 28 member states of the EU once it is implemented but at the price of an even greater gap between the EU and the rest of the globe.

Whether this is the best way to achieve the right balance between privacy protection and the needs of the digital economy will remain a topic of live and intense political debate. What can be said is that the proposal as it stands will effectively end the hope of a move towards greater compatibility of laws in the foreseeable future and dealing with privacy on a global basis will continue to pose a real challenge.

Notes

1 Privacy Laws and Business International Report Issue 115 Special Supplement February 2012. Graham Greenleaf, Professor of Law and Information Systems UNSW, noted that 89 data protection or data privacy laws were in force or in preparation.
2 Modernisation proposals November 2011 and further reports of January and March 2012, July 2013, meeting December 2014.
3 Uruguay, a non-Council of Europe state, has also acceded to, but not ratified, the treaty.
4 Ephraim Percy Kenyanito writing in an Access blog in February 2015 reported that laws to implement the Convention are proposed in Kenya, Madagascar, Mauritania, Morocco, Tanzania, Tunisia and Uganda.
5 Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
6 July 2014 due to come into effect in September 2015.
7 Directive 95/46/EC, article 24.
8 The States of Jersey, the Isle of Man and the Bailiwick of Guernsey.
9 The Faroe Islands are part of the Kingdom of Denmark.
10 Uruguay, Mexico and Colombia.

11 Council Decision 2000/520/EC.
12 Quebec, Alberta and British Columbia have privacy laws.
13 Malaysia Personal Data Protection Act 2010, in force from 15 November 2013 and effective from 15 February 2014.
14 Singapore Personal Data Protection Act 2012 in force from 2 July 2014.
15 South Korea amended its Personal Information Privacy Act to cover all sectors handling personal data. The Act has been in force since August 2014.
16 In effect from March 2014.
17 Ephraim Percy Kenyanito writing in an Access blog in February 2015 reported that laws to implement the Convention are proposed in Kenya, Madagascar, Mauritania, Morocco, Tanzania, Tunisia and Uganda.
18 The Protection of Personal Information Act 2013 (the Act) was signed in November 2013 and certain sections of the Act came into force in April 2014. These sections enable the establishment of the information regulator as well as the power for regulations to be made under the Act. There is no commencement date yet set. There will be a 12-month implementation period after commencement.
19 COM(2012) 11/4 draft.
20 Version 34 2011-11-29.
21 COM (2012) 11/4 draft, article 3.
22 Ibid, article 79.

HUNTON& WILLIAMS

Rosemary P Jay **rjay@hunton.com**

30 St Mary Axe
London EC3A 8EP
United Kingdom

Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
www.hunton.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Executive Compensation & Employee Benefits
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law