INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Russian DP law amendments impose stringent requirements

Changes clarify some of the concepts in the 2006 law, but also place new obligations on organisations. **Natalia Oleynikova** and **Leonid Zubarev** report from Moscow.

On 26 July 2011, the Russian President signed a new law clarifying the rules on the processing and transferring of personal data as well as the rights and obligations of data controllers and subjects.

The law "On Personal Data" was adopted five years ago and, has since then been amended repeatedly. However, it is clear that these amendments are the most significant since the law first came into force. Their adoption will force legal entities to again revise their internal policies related to personal data processing.

The initial aim of adopting the new law was to clarify certain provisions of the existing law "On Personal Data" and to simplify the

Continued on p.3

The Netherlands: Consent for tracking cookies still a hot topic

The Netherlands chooses the opt-in approach for cookies in its implementation of the amendments to the e-Privacy Directive. **Frank Simons**, **Gerrit-Jan Zwenne** and **Feyo Sickinghe** report.

On 14 June 2011, the Lower House of the Dutch Parliament adopted a Bill implementing the European Citizen Rights Directive (which amended the e-Privacy Directive), but only after introducing its own amendment on the subject of cookies. The amended Bill is now before the Senate and is expected to come into force in January 2012. The Bill has generated much debate, with the new rules on cookies attracting most attention.

Current cookie regime

Currently, the rules on cookies in the Netherlands require that subscribers or end-users be informed about

Continued on p.4

Issue 112 **September 2011**

public has unrestricted access, such as the internet;
- when the data is collected for a reason relating to the state's duties; or
- when the data is limited to the data subject's name, national ID card number, tax or social security identification, occupation, date of birth or domicile.

The Act prohibits the transfer of any type of personal information to countries or any international or supranational entities which do not provide adequate levels of protection, except when individuals have given their consent, or where such a transfer is required by international transfer agreements. The DP Authority sets out which countries meet Argentina's adequacy standards.

The Act also specifies that data subjects have the right to access their personal information, correct and update it, and to object to automated personal assessments. Data subjects also have the right to opt out of marketing campaigns, to sue for damages or illegal treatment (a right which opened up class action cases, most notably *Union de Usuarios y Consumidores (UDES) v Citibank*), and the right to lodge administrative claims.

Argentina's Data Protection Authority itself is independent, but located within the Ministry of Justice. Its official functions include the registration of databases, the enactment of rules and regulations, ensuring compliance with data integrity and security norms, the enforcement of administrative sanctions, and the approval of marketing codes of conduct. It also acts as the complainant in criminal actions bought for violations of the Act. There are also provincial data protection agencies, with which the federal agency must maintain a relationship.

Chile

In Chile, following the drafting of a data protection bill with the help of the OECD in 2008 (which was compatible with EU standards), a new data protection bill was introduced into the legislature in June 2011 which also met EU standards, although it has yet to pass into law.

Peru

Following on from its 2001 credit reporting law and its 2008 spam law, Peru is expected to introduce a data protection law this year, based on a bill introduced by the previous government of President Alan Garcia. The bill sets out full EU-style data protection provisions, but also leaves much of the interpretation to the regulatory body, the Autoridad Nacional de Protección de Datos Personales, which sits within the Ministry of Justice. (See *Privacy Laws & Business International* July 2011, p.21).

INFORMATION

Mexico is hosting the 33rd International Conference of Data Protection and Privacy Commissioners' Conference in Mexico City, 1-3 November this year – see www.privacyconference2011.org

Pablo A. Palazzi is a lawyer at Allende & Brea, Buenos Aires, Argentina.
E-mail: pap@allendebrea.com.ar
web: www.allendebrea.com.

AUTHOR

Asher Dresner is a *PL&B* correspondent.

Koreans' ID numbers fall prey to hacking business

Breach notification duty imposed to reduce identity fraud. By **Whon-Il Park**.

This summer, South Koreans suffered most not only from heavy rains, which caused unexpected landslides with casualties in wealthy neighbourhood in Seoul, but also from massive data leakage. In the final week of July, Korean citizens were surprised to hear that Nate and Cyworld, the biggest portal services run by SK Communications, were assaulted by unidentified hackers, and personal information of up to 35 million Korean citizens were leaked to a third country. As soon as they found out that customers' personal data, including ID, name, mobile phone number, email address, encrypted password and resident registration number, was snatched away by hackers, SK Communications notified the authorities concerned of the incident. The number of customers whose data was leaked was so enormous that they could not initially find any judge, not affected by the incident, for the purpose of fair court proceedings.

The resident registration number, a universal identifier in South Korea, has been a unique and efficient tool to identify a Korean resident for administrative and anti-crime purposes since the 1960s. It was originally used to establish where such number holders live and what they do. Later on, with the advent of the Information Age, this unique ID number was regarded as indispensable to identify users of Internet services.

There are those willing to pay to obtain the resident registration numbers of living Koreans. For example, minors wishing to be admitted to an adult site, gamblers intending to play illegal casino in the cyberspace, merchants sending spam or conducting

direct marketing, or criminals committing e-commerce fraud. As a result, those with a high level of hacking knowledge desire to tap and attack the security-fragile servers of Korean Internet service providers which contain a large volume of personal data. In particular, a third country beyond the capabilities of Korean anti-cyber crime police has been a host country to such hackers.

Flourishing hacking business against Koreans

Recently, the Korean government admitted that more than 15,000 ID numbers have been exposed and traded in cyberspace during the past three years, and half of this took place in China. But an expert in the industry guessed the actual number could be far more.

In fact, it is alleged that a few clicks in the Chinese communications networks will yield hundreds and thousands of real names and ID numbers of South Koreans. They are probably used as a means of voice phishing, spam mailing and fraudulent commerce. According to the statistics published by the Korea Internet Security Agency, in June 2011 only, more than five million hacking attacks from foreign countries took place, and around 60 percent of such attacks originated from China.

Hacking operations from China are sometimes carried out by profit-chasing South Korean culprits or dollar-thirsty North Korean agents. North Korean hackers have been trained by the military to attack the servers of both the public institutions and private companies, sometimes for money and other times to show-off of their capability. The shut-down of computer systems of Nonghyup Bank (Agricultural Cooperatives Association) was allegedly caused by North Korean hackers stationed in China. At this juncture, a question is raised, who is benefiting from this?

Government counter-measures

In view of the importance of such incidents, at-risk companies as well as the government are taking efforts to prevent hacking and similar incidents. From September this year, SK Communications will make it a rule to delete the customer's ID number immediately after the sign-up process, unless such customer is engaged in the Internet sale and purchase of items like avatar characters or BGM files and other financial transactions. And the collection of resident registration numbers for the authentication of a real person will be replaced by the checking services provided by credit bureaus.

In addition, as from 30 September this year, the new Personal Information Protection Act will require mandatory data breach notification and collective dispute mediation procedures. Prior to its implementation, the government is introducing actively an alternative ID number, such as i-PIN (Internet Personal Identification Number), which is used with a personal ID and password in order to replace the resident registration number, and reduce the controversial real name system on the Internet. So far, the real name system on the Internet has been enforced to prevent vicious replies or illegal election campaigns on Internet bulletin boards. From now on, the resident registration numbers should only be collected to a minimum extent or in a separate grouping other than the birth date. Whether these measures will be effective in reducing ID fraud remains to be seen.

Netizens' angry responses escalate

Right after the SK incident, a lawyer, who argued that his privacy has been violated, filed a lawsuit against SK Communications for compensation for mental distress. However, the court has not yet made a ruling. He will have to overcome the effect of similar lawsuits in the massive data breach case of Auction, the largest Internet shopping mall in Korea, which resulted in the court denial of such claims for compensation in January 2010. The court ruled, "There's no evidence that Auction was lenient about its security measures against hacking." The court added, that it was not legally mandatory for companies to set up firewalls for their websites, considering that Internet firewalls had little credibility among businesses at that time.

Apple fined for collection of iPhone location data

At present, what makes Korean users angry – besides the ID numbers – is the fact that their location information, indispensable for social networking services, is often collected without data subjects' consent, and misused by the mobile phone service providers. In July 2011, after an investigation that lasted several months, the Broadcasting and Communications Commission fined Apple Korea three million won (equivalent to $2,800) for the illegal collection of iPhone user location information, in breach of the location information law.

The amount is insignificant for Apple, but the Korean authority's decision to impose the fine might influence regulators elsewhere, and this is a second series of damages Apple has faced in South Korea. A few months ago, a district court ordered Apple Korea to pay one million won in compensation to an iPhone user. In that case, Apple Korea did not argue the plaintiff's complaint at the court. Certainly the court did not decide the case on its merits. However, more than 27,000 iPhone users have joined the collective suit (class action) to demand compensation for their mental distress from violation of privacy.

As with various complaints and criticisms that Apple has faced in other countries, iPhones is reported to have stored the locations of nearby cell phone towers and Wi-Fi hot spots for up to a year. Such data can be used to create a rough map of the device owner's movements unless tracking is turned off. Anyhow, it was Apple's bug or fault that caused iPhone to keep location data even when tracking was disabled by the user. The Korean communications authority also demanded that both Apple and Google ensure that user location information on their mobile phones is saved in an encrypted form.

AUTHOR

Whon-Il Park is Professor of Law, Kyung Hee University, South Korea.

GLOBAL DATA PRIVACY LAWS

SPECIAL REPORT: Forty years of acceleration

In this exclusive report for *Privacy Laws and Business* **Professor Graham Greenleaf** has identified privacy legislation in 76 jurisdictions across the world.

How many countries now have data protection laws? The usual answer is somewhat vague: "about 60" or perhaps "more than sixty", a well-informed respondent might say at present, because the precise answer cannot conveniently be found. In fact, the answer is that there are now 76 countries (or otherwise independent legal jurisdictions) which, as of mid-2011, have enacted data privacy laws. The following table lists all countries which have enacted data privacy laws, when they did so, and the international commitments of each country, or the international recognition their laws have received.

It is almost forty years since Sweden's Data Act 1973 was the first comprehensive national data privacy law, and the first to implement what we can now recognise as a basic set of data protection principles. This article surveys the forty years since then of global development of data privacy laws to mid-2011. The picture that emerges is that data privacy laws are spreading globally, and their number and geographical diversity accelerating since 2000. There are some surprising inclusions, and some illuminating trends in the expansion of these laws.

Criteria: Largely comprehensive private sector coverage

In this article, and the accompanying table a country is only considered to have a "data privacy law" if it has a national law which provides, in relation to most aspects of the operation of the private sector, a set of basic data privacy principles, to a standard at least approximating the OECD Guidelines, plus some methods of legislation-based enforcement (i.e. not only self-regulation). "Largely comprehensive private sector coverage" is therefore the basis for inclusion. This excludes countries which only have scattered sectoral privacy laws (e.g. the US sectoral laws, Qatar's regulations concerning the financial sector, countries which only have credit reporting laws). Many countries have some exceptions in their private sector coverage, such as various forms of "small business" exceptions (e.g. Japan and Australia), or exceptions for non-automated records, but this is not a basis for exclusion.

"Countries" is a slight exaggeration, and a more accurate term would be "separate legal jurisdictions". The table includes the two Special Administrative Regions (SARs) which have constitutionally different legal systems from the rest of China (Hong Kong and Macao, under the principle of "One Country, Two Systems") and five British dependent territories which have their own legal systems (the Isle of Man, Jersey, Guernsey, Gibraltar and the Bahamas). However, sub-national jurisdictions which do not have their own separate legal systems, or are subject to the laws of a federation, are not included. So jurisdictions such as Quebec, New South Wales and Hesse are excluded even if they do provide some coverage of the private sector, as are certain provinces of the People's Republic of China which have enacted local laws.

The year stated in the table under "From" is the year from which the legislation was enacted which provided coverage of most of the private sector. So, for example, the year shown for Australia is 2001, even though the Privacy Act 1988 had then been operation for 13 years in relation to the public sector, and for a lesser period in relation to the credit industry. In one case where the coming into force of a law was so long-delayed after enactment (i.e. Russia, from 2007 to 2011) the date stated is the latter enforcement date. In other cases the year stated is that of enactment, ignoring the year or so that it often takes for regulations to be made and preparations made for the law to be administered. The year of the most recent known amendment to the current law is given in the "Latest" column. The purpose of these columns is to indicate trends in enactment and updating, not to give precise "in force" dates.

> A country is only considered to have a "data privacy law" if it has a national law.

Almost all jurisdictions listed have laws which also cover their national public sectors, possibly by different legislation to that covering the private sector, and very often with principles

and enforcement mechanisms which differ significantly from those applying to the private sector. Exceptions where there is no protection provided in relation to the public sector are Malaysia and India. Some jurisdictions also provide basic data privacy protection in relation to their public sector, but do not do so for most of their private sector and so are not included in this Table. Examples include the United States (Privacy Act 1974) and Thailand. Quite a few jurisdictions which now have private sector coverage initially only covered their public sectors, including Australia, Japan, Canada and South Korea (but those earlier dates are ignored). Privacy protection in the public sector is obviously important, and a table showing the dates of introduction of such laws would tell a somewhat different story involving two more countries. But both stories cannot be told at once.

Almost all jurisdictions provide in their legislation for a Data Protection Authority (DPA), a separate institution which has responsibility for the data privacy legislation. DPAs vary greatly in name (often called "Privacy Commissioners"), functions and degree of independence from other government authorities. From 76 jurisdictions, Chile, Colombia, the Kyrgyz Republic, India, Japan and Taiwan are among the few remaining exceptions with no DPA.

Growth by decade

The total number of new data privacy laws globally, viewed by decade, shows that their growth is accelerating, not merely expanding linearly: 7 (1970s), 10 (1980s), 19 (1990s), 32 (2000s) and 8 (1.5 years of 2010s), giving the total of 76. In the 1970s data privacy laws were a western European phenomenon (Sweden, Germany, Austria, Denmark, France, Norway and Luxembourg), and similarly in the 1980s (UK, Ireland, Iceland, Finland, San Marino and the Netherlands, and three UK territories), with Israel as the first non-European state in 1981 (Australia's 1988 legislation was public sector only). Acceleration commenced in the 1990s, as most remaining western European countries (European Union and European Economic area) enacted laws (Portugal, Belgium, Spain, Switzerland, Monaco, Italy and Greece). More significantly, with the collapse of the Soviet Union many former eastern bloc countries enacted data privacy laws as part of their protection of civil liberties (Slovenia, Czech Republic, Hungary, Slovakia, Poland and Albania), and the first ex-Soviet-republics (Lithuania and Azerbaijan) did likewise. The spread outside Europe also started, with the first laws in Latin America (Chile) and the Asia-Pacific (New Zealand, Hong Kong and Taiwan).

In the 2000s the acceleration continued, with the expansion in the former eastern bloc and Soviet republic countries the most striking (Latvia, Bosnia and Herzegovina, Romania, Bulgaria, Croatia, Estonia, FYROM (Macedonia), Moldova, Serbia and Montenegro), plus the addition of the remaining European states (Cyprus, Malta, Andorra, Liechtenstein, Gibraltar). Outside Europe, expansion accelerated in the Asia-Pacific (Australia, South Korea, Japan, Macao SAR) and Latin America (Argentina, Colombia, Uruguay). In the Americas, Canada and the Bahamas added further new laws. Rapid development took place in Africa with new laws in Tunisia and Morocco (North Africa) and Mauritius, Cape Verde, Benin Senegal and Burkina Faso (Sub-Saharan Africa). The Kyrgyz Republic became the first country in Central Asia to legislate in 2008. In the first 18 months of this decade eight new laws have been enacted (Faroe Islands, Malaysia, Mexico, India, Peru, Russia – more accurately, brought into force – Ukraine and Angola), making this the most intensive period of data protection developments in the last 40 years.

> Almost all jurisdictions provide in their legislation for a Data Protection Authority.

Geographical expansion

Geographically, almost two thirds of data privacy laws are in European states (48/76), EU member states are little more than one third (27/76), even with the expansion of the EU into eastern Europe. There are data privacy laws in all 27 member states of the European Union, and a further 21 laws in other European countries or jurisdictions. Only a few European states remain without such laws, such as Georgia and Belarus. There are six laws in Latin America, with Brazil set to become the seventh. In the Americas are also the laws in Canada and the Bahamas (the only law in the Caribbean). In Asia there are now eight data privacy laws, with Singapore promising a ninth, and the other eight ASEAN states committed to improved privacy protection by 2015. Both Australia and New Zealand have data privacy laws, but none of the Pacific Islands do so (the only region with no such laws). In North Africa and the Middle East, there are three such laws, and six in Sub-Saharan Africa. Further Acts are likely soon, with Bills progressing in South Africa and Ghana. The French-Speaking Association of Personal Data Protection Authorities (AFAPDP), and France's CNIL have both played key roles in developing expansion of data privacy in Africa. The Kyrgyz Republic law is the first in Central Asia, though Mongolia's laws also come close to qualifying. So there are 27 data privacy laws outside Europe.

Measuring growth

For over two decades the rate of adoption of new data privacy laws per year has been steadily increasing, and the regions of the globe that have such laws has been steadily expanding. If the current rate of expansion is continued, 50 new laws would result in this decade. Even on the conservative (and probably unrealistic) assumption that the 2010s will see no more data privacy laws than the 2000s, the number of countries with data protection laws will exceed 100 by the decade's end, with the majority of data privacy laws by then coming from outside Europe. In addition, many existing laws are being strengthened to keep up with rising expectations of privacy protection, international agreements, and the

examples set by other countries (see the "Latest" column in the table).

There are other ways that expansion could be measured, say by the populations of the countries concerned, or by their GNP. These could show different trends, but reflection on the size and economic significance of the countries so far included makes it obvious that data privacy laws are more common in the world's larger and more economically significant countries. The recent inclusion of India accelerates this trend, as will the likely inclusion of Brazil in the near future. By any measure, data privacy laws are of increasing and accelerating global significance.

The most economically significant countries currently missing from the list are the USA, China and Brazil, now that India has adopted a data privacy law in 2011. The omission of Brazil is also expected to be remedied this year. China is currently in what can be called the "warring states period" of data protection, where the states concerned are the numerous parts of the Chinese bureaucracy disputing the best way to deal with data protection issues, and no-one knows what the outcome will be. The US has many privacy laws and some effective enforcement, but no comprehensive privacy law in the private sector, nor it seems much prospect of one. Most other countries that do not yet have data privacy laws are of relatively low significance in international trade, though some countries with large populations are among them, particularly in sub-Saharan Africa (e.g. Nigeria), and in Asia (e.g. Indonesia).

Finally, for the purposes of this brief overview, it is important to note that "growth" or "expansion" of data privacy laws cannot be simply equated with improvement in privacy protection. Surveillance activities in both the private and public sectors can grow at the same time, and quite often do when data privacy laws are a trade-off for, or a belated response to, more intensive surveillance.

International commitments and recognition

International agreements concerning data protection have had a considerable influence on national and sub-national adoption of data privacy laws for thirty years since the drafting of both the OECD's privacy Guidelines and the Council of Europe data protection Convention at the outset of the 1980s. Since then, the European Union's data protection Directive of 1995 has been the most influential international instrument, and APEC's Privacy Framework has created regular opportunities for discussion of privacy issues among some Asia-Pacific jurisdictions.

All 27 Member States of the European Union are required to have data privacy laws which implement the EU privacy Directives, and all do so (see the table). Five additional countries have applied to join the EU[1], and two of these (Montenegro and Turkey) do not yet have data privacy laws. The European Economic Area (EEA) includes the European Union member states plus Iceland, Norway and Liechtenstein, all of which have data privacy laws.

> "Growth" or "expansion" of data privacy laws cannot be simply equated with improvement in privacy protection.

Countries or jurisdictions outside the EEA can obtain from the EU a decision that their laws provide an "adequate" level of protection of privacy, to enable free flow of personal data from EU member states to organisations in those countries. As yet, the EU has only made such decisions in relation to nine jurisdictions as a whole, a minority of which are of economic or political significance.[2] Uruguay and New Zealand will soon be added to this list, after receiving favourable Opinions from the Article 29 Working Party.

Forty-one Council of Europe Member States (most of the members) have ratified the Council of Europe Data Protection Convention of 1981 (41 in total) (Convention 108), and have data privacy laws. Armenia, Turkey and the Russian Federation have signed but not ratified the Convention. San Marino has done neither. However, Russia does now have a data privacy law (in force 2011). Armenia, Georgia and Turkey are the only Council of Europe Member States not to have enacted a data privacy law. Belarus is not a Council of Europe member because of human rights concerns, and the Vatican is not a member because it is not a democracy. The Additional Protocol (ETS 181) to the Convention also requires a commitment to data export restrictions and to an independent data protection authority, and brings the standards of the Convention up to approximately the same level as the Directive. Thirty European countries have also ratified the Optional Protocol. Twelve countries that have ratified the Convention (plus three territories on whose behalf the UK acceded to the Convention) have not ratified the Optional Protocol. Where a Council of Europe member has ratified both Convention 108 and the Additional Protocol, it is extremely unlikely as a matter of practice that data exports to that country would be prevented, so obtaining an adequacy finding under the Directive becomes irrelevant in practice. This is noted in the table.

Since 2008 the Council of Europe has made it clear that it wishes the Convention and Optional Protocol to become global agreements, and that it welcomes requests by states outside Europe with suitable data privacy laws to apply to accede to both. It is not confirmed, but Uruguay appears to be the first non-European state to be invited to do so (see Council of Europe website) but does not appear to have acceded. An adequacy finding from the EU does not impose any reciprocal obligations on the recipient to allow free flow of personal data from it to EU countries. This obligation will arise when countries outside the EU become members of the Council of Europe Convention 108.

Turkey is the only OECD (Organisation for Economic Cooperation and Development) member country, other

Continued on p.17

GLOBAL TABLE OF DATA PRIVACY LAWS (as at 30 July 2011)

Jurisdiction	Key Act	From[i]	Latest	Region	EU[ii]	CoE[iii]	Other Int.[iv]
Albania	Act on the Protection of Personal Data	1999	1999	Europe	[I]	M; P	
Andorra	Law on the protection of personal data	2003	2003	Europe	A	M; P	
Angola	Data Protection Act	2011		Africa			
Argentina	Personal Data Protection Act	2000	2000	Latin Am	A		
Australia	Privacy Act 1988	2001	2001	Australasia			APEC; OECD
Austria	Datenschutzgesetz	1978	2009	Europe	M	M; P	OECD
Azerbaijan	Law on data, data processing and data protection	1998	1998	Europe		M	
Bahamas	Data Protection Act	2003	2003	Caribbean			
Belgium	Law on Privacy Protection in relation to the Processing of Personal Data	1992	1998	Europe	M	M	OECD
Benin	Loi sur la Protection des données personnelles	2009	2009	Africa			ECOWAS
Bosnia & Herzegovina	Law on the protection of personal data	2001	2001	Europe	[I]	M; P	
Bulgaria	Law for Protection of Personal Data	2002	2007	Europe	M	M; P	
Burkina Faso	Law on Protection of Personal Information	2004	2004	Africa			ECOWAS
Canada	Personal Information Protection and Electronic Documents Act	2002	2002	North Am	A		APEC; OECD
Cape Verde	Data Protection Act (Law N° 133/V/2001)	2001	2001	Africa			ECOWAS
Chile	Privacy Law	1999	1999	Latin Am			APEC; OECD
Colombia	Data Protection Law	2008	2008	Latin Am			
Croatia	Act on Personal Data Protection	2003	2003	Europe	[I]	M; P	
Cyprus	The Processing of Personal Data (Protection of the Individual) Law	2001	2003	Europe	M	M; P	
Czech Republic	Personal Data Protection Act	1992	2000	Europe	M	M; P	OECD
Denmark	Act on Processing of Personal Data	1978	2000	Europe	M	M	OECD
Estonia	Data Protection Act	2003	2003	Europe	M	M; P	OECD
Faroe Islands	Act on processing of personal data	2010	2010	Europe	A		
Finland	Personal Data Act	1987	1999	Europe	M	M	OECD
France	Law relating to the protection of individuals against the processing of personal data	1978	2004	Europe	M	M; P	OECD
FYROM (Macedonia)	Law on Personal Data Protection	2005	2005	Europe	[I]	M; P	
Germany	Federal Data Protection Act	1977	2001	Europe	M	M; P	OECD

GLOBAL TABLE OF DATA PRIVACY LAWS (continued)

Jurisdiction	Key Act	From[i]	Latest	Region	EU[ii]	CoE[iii]	Other Int.[iv]
Gibraltar	Data Protection Act	2004	2004	Europe			
Greece	Law on the Protection of individuals with regard to the processing of personal data	1997	1997	Europe	M	M	OECD
Guernsey	Data Protection (Bailiwick of Guernsey) Law	1986	2001	Europe	A	M*	
Hong Kong SAR	Personal Data (Privacy) Ordinance	1995	1995	Asia			APEC
Hungary	Law on the protection of personal data and the disclosure of public information	1992	1992	Europe	M	M; P	OECD
Iceland	Law on the Protection and Processing of Personal Data	1989	2000	Europe	EEA	M	OECD
India	Rules under s43A (2008 Amendt), Information Technology Act 2000	2011	2011	Asia			
Ireland	Data Protection Act	1988	2003	Europe	M	M; P	OECD
Isle of Man	Data Protection Act	1986	2002	Europe	A	M*	
Israel	Privacy Protection Act 1981	1981	1981	M.East/N. Af	A		OECD
Italy	Consolidation Act regarding the Protection of Personal Data	1996	2003	Europe	M	M	OECD
Japan	Act on the Protection of Personal Information	2003	2003	Asia			APEC; OECD
Jersey	Data Protection (Jersey) Law	1987	2005	Europe	A	M*	
Kyrgyz Republic	Law on Personal Data	2008	2008	Central Asia			
Latvia	Law on Protection of Personal Data of Natural Persons	2000	2002	Europe	M	M; P	
Liechtenstein	Gesetz über die Abänderung des Datenschutzgesetzes (2002)	2002	2008	Europe	EEA	M; P	
Lithuania	Law on Legal Protection of Personal Data	1996	2003	Europe	M	M; P	
Luxembourg	Data Protection Law	1979	2002	Europe	M	M; P	OECD
Macao SAR	Personal Data Protection Act (Law 8/2005)	2005	2005	Asia			
Malaysia	Personal Data Protection Act	2010	2010	Asia			APEC
Malta	Data Protection Act	2001	2001	Europe	M	M	
Mauritius	Data Protection Act	2004	2004	Africa			
Mexico	Federal Law on the Protection of Personal Data Held by Private Parties	2010	2010	Latin Am			APEC; OECD
Moldova	Law on Personal Data Protection	2007	2007	Europe	[I]	M; P	
Monaco	Act controlling personal data processing (2001)	1993	1993	Europe	[I]	M; P	
Montenegro	Law on Personal Data Protection	2008	2008	Europe			
Morocco	Data Protection Act	2009	2009	M.East/N. Af			

GLOBAL TABLE OF DATA PRIVACY LAWS (continued)

Jurisdiction	Key Act	From[i]	Latest	Region	EU[ii]	CoE[iii]	Other Int.[iv]
Netherlands	Personal Data Protection Act	1988	2000	Europe	M	M; P	OECD
New Zealand	Privacy Act 1993	1993	2010	Australasia	[A]		APEC; OECD
Norway	Personal Data Act	1978	2000	Europe	EEA	M	OECD
Peru	Law on Protection of Personal Data	2011	2011	Latin Am			APEC; US FTA
Poland	Act on the Protection of Personal Data	1997	2004	Europe	M	M; P	OECD
Portugal	Lei 67/ 98 – Lei da Protecção de Dados Pessoais	1991	1998	Europe	M	M; P	OECD
Romania	Law on the protection of individuals with regard to the processing of personal data and the free movement of such data	2001	2005	Europe	M	M; P	
Russia	Federal Law Regarding Personal Data	2011	2011	Europe	S	M	APEC
San Marino	Law regulating the Computerized Collection of Personal Data	1983	1995	Europe			
Senegal	Act on the Protection of Personal Data	2007	2007	Africa			ECOWAS
Serbia	Law on Personal Data Protection	2008	2008	Europe	[I]	M; P	
Slovakia	Act on the Protection of Personal Data	1992	2005	Europe	M	M; P	OECD
Slovenia	Personal Data Protection Act	1999	2004	Europe	M	M	OECD
South Korea	Data Protection Act	2001	2011	Asia			APEC; OECD
Spain	Ley Orgánica de Protección de Datos de Carácter Personal	1992	1999	Europe	M	M; P	OECD
Sweden	Personal Data Act	1973	1998	Europe	M	M; P	OECD
Switzerland	Data Protection Act	1992	1992	Europe	A	M; P	OECD
Taiwan	Personal Data Protection Act	1995	2010	Asia			APEC
Tunisia	Law on the protection of personal data	2004	2004	N.Af/M.East			
Ukraine	Law on Personal Data Protection	2011	2011	Europe	[I]	M; P	
United Kingdom	Data Protection Act 1998	1984	1998	Europe	M	M	OECD
Uruguay	Law on the Protection of Personal Data	2008	2008	Latin Am	[A]		

TABLE: EXPLANATORY NOTES

i. **Date columns:** 'From' = date original law enacted; 'Latest' = year of last significant amendment known

ii. **European Union column:** M = country is an EU member state; A = country's protection of personal data has been held 'adequate' by the EU; [A] = Favourable Article 29 Working Party opinion on adequacy, but no final decision announced; EEA = country is a member of the European Economic Area; [I] = Adequacy finding is in practice irrelevant due to country acceding to both Council of Europe Convention 108 and Additional Protocol

iii. **Council of Europe column:** M = country is a member state of the Council of Europe and has ratified the Convention; M* = United Kingdom has ratified Convention on behalf of sub-jurisdiction; P = country has also ratified the optional protocol; S = country has signed but not ratified Convention

iv. **Other international commitments column:** APEC = 'economy' is a member of APEC; OECD = country is a member of OECD; ECOWAS = country is a member of Economic Community of West African States

than the US, which does not have a data privacy law, in compliance with the OECD's privacy Guidelines of 1981. The OECD's plans for enlargement[3] mean that more countries in future will be likely to be influenced by the OECD privacy Guidelines to adopt data privacy laws.

A slight majority (12) of the 21 APEC (Asia-Pacific Economic Cooperation) member "economies" do have data privacy laws (see the Table), but nine do not: Brunei; Indonesia; Philippines; Singapore; Thailand; USA; China; Papua New Guinea; and Vietnam. Singapore says it will introduce legislation in 2011; the Philippines and Thailand have bills before their legislatures. Whether APEC will expand beyond 21 members is still an open question. Numerous countries have been trying to join for some time[4]. In refusing India's application for membership, APEC decided not to admit more members until 2010. India has been invited to be an observer for the first time at the APEC meeting in November 2011. India is the only Asian country which is not an APEC member but does have a data privacy law (Macao SAR has such a law but is not a country). If APEC's membership is expanded, this will at least mean that more countries are involved in the six monthly discussions of APEC's privacy group.

The Economic Community of West African States (ECOWAS), a grouping of 15 states under the Revised Treaty of the ECOWAS, agreed to adopt data privacy laws in 2008. A Supplementary Act on Personal Data Protection within ECOWAS (ECOWAS, 2010) to the ECOWAS Treaty, adopted by the ECOWAS member states, has established what the content of such data privacy laws should be, influenced very strongly by the EU Directive, and that each state is to establish a data protection authority. Four ECOWAS states have so enacted laws (Benin, Burkina Faso, Cape Verde, and Senegal), and a Bill is before Parliament in Ghana, leaving 10 yet to take action.

Bills in progress

Bills to enact new data privacy laws in countries that do not have them are currently known to be before the Parliaments of Brazil, the Philippines, Thailand, Ghana and South Africa.

RESOURCES AND ACKNOWLEDGEMENTS

Thanks to the Stewart Dresner and Laura Linkomies (*Privacy Laws & Business*), Marie Georges (Planete Informatique et Libertés, Paris) and Magda Cocco and Joana Saldanha Santos (Vieira de Almeida & Associados, Lisbon www.vda.pt) for their assistance in locating legislation.

Some of the resources which have been valuable in the research for this article are as follows:
Council of Europe website, for ratifications of the Convention and the Protocol; EU website for legislation of Member States http://ec.europa.eu/justice/policies/privacy/law/implementation_en.htm
EU website for adequacy decisions http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm
Privacy Laws & Business website www.privacylaws.com
Christopher Millard 'Privacy Laws & Business European Data Protection Laws Chart' *Privacy Laws & Business Newsletter*, May 1997.
dataprotection.eu website. http://www.dataprotection.eu/
Morrison & Foerster 'Privacy Library' http://www.mofo.com/privacylibrary/
Linklaters 'Data Protected' website.
Bureau of National Affairs website.

All errors and omissions remain my own. Please email graham@austlii.edu.au and laura.linkomies@privacylaws.com with any updates.

AUTHOR

Professor Graham Greenleaf is *PL&B's* Asia-Pacific editor.

UPDATES

Details of new data privacy laws from countries which do not have them will be included in subsequent issues of *Privacy Laws & Business International Report*, plus a note of Bills for new laws. A periodically updated version of the table will be available from the author's webpages at www2.austlii.edu.au/~graham.

REFERENCES

1. Croatia; Former Yugoslav Republic of Macedonia (FYRIM); Iceland; Montenegro; Turkey.
2. Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, and Jersey.
3. "In May 2007, OECD countries agreed to invite Chile, Estonia, Israel, Russia and Slovenia to open discussions for membership of the Organisation and offered enhanced engagement to Brazil, China, India, Indonesia and South Africa" (OECD website). Chile, Slovenia, Israel and Estonia have since become members.
4. "In addition to India, Mongolia, Pakistan, Laos, Bangladesh, Costa Rica, Colombia, Panama and Ecuador, are among a dozen countries seeking membership in APEC by 2008." – see http://en.wikipedia.org/wiki/Asia-Pacific_Economic_Cooperation#Member_Economies.