PRIVACY LAWS AROUND THE WORLD:

Europe/Eurasia • Asia-Pacfic
Western Hemisphere • Africa-Near East

Bloomberg Law®

Privacy Laws Around the World

Development of international privacy laws and regulations with critical impact on the global economy been extremely active over the last several years.

This *Privacy Laws Around the World* compilation of reports by Cynthia Rich of Morrison & Foerster LLP compares common and disparate elements of the privacy laws from 61 countries. Rich provides expert analysis on privacy laws in Europe and Eurasia (non-EEA), East, Central and South Asia and the Pacific, the Western Hemisphere (Latin America, Caribbean and Canada), as well as Africa and the Near East.

This report gives you at-a-glance access to:

- Side-by-side charts comparing four key compliance areas including registration requirements, cross-border data transfer limitations, data breach notification requirements and data protection officer requirements;
- a country-by-country review of the special characteristics of framework privacy laws and
- discussion of privacy legislation in development around the world.

Rich shares her practical insights into how privacy practices differ from region-to-region. For example, that compared to their European and Asian counterparts, most countries in the in the Western Hemispheres (Latin America, the Caribbean, and Canada) require organizations to respond to access and correction requests in a much shorter period of time.

Table of Contents:

Privacy Law Watch™

June 07, 2016

Legislation

Privacy Laws in Europe and Eurasia (non-EEA)

Framework Privacy Laws

In the first of a series of articles on the status of data protection laws around the world, the author explores developments in non-European Economic Area parts of Europe and Eurasia, where 17 jurisdictions have comprehensive privacy laws.

By Cynthia Rich

Cynthia Rich is a senior advisor at Morrison & Foerster LLP in Washington. As a member of the firm's international Privacy and Data Security Practice since 2001, Ms. Rich works with clients on legal issues relating to privacy around the world.

Introduction/Region at-a-Glance

With the recent adoption of the European *General Data Protection Directive* (GDPR), attention of the business community has been focused on changes to the privacy rules in the 28 members states of the European Union (and as well as Switzerland and the other members of the European Economic Area or EEA). However, these changes are likely to have a ripple effect on existing privacy laws in the 17 jurisdictions in Europe and Eurasia that are not part of the EU or EEA: Albania, Andorra, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Georgia, Kosovo, Macedonia, Moldova, Monaco, Montenegro, Russia, San Marino, Serbia, Turkey and Ukraine.

These laws contain the basic elements found under EU member state laws, but some also have unique elements not found in other laws in the region or within the EEA. Almost half of the laws were enacted in the past five years, so it is unclear if or how soon these countries will amend these relatively new laws to follow the changes under the GDPR.

This article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments.

Common Elements Found in European/Eurasian Laws

Notice:

All of the laws in region include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, why it is collected and with whom it is shared.

Choice/Legal Basis for Collection and Use (Processing):

Every privacy law contains some kind of choice element and requires organizations to have a legal basis on which to process personal information. Similar to those found in the EU, these legal bases include the following: the individual has consented to the processing (consent); the processing is necessary to fulfill a contract (contractual necessity); the processing is necessary to pursue a legitimate interest of the controller (legitimate interests); and the processing is necessary to protect the vital

interests of the individual (vital interests) or the processing is necessary to comply with a legal requirement (legal requirement). However, depending on the jurisdiction, not all of these legal bases are available. For example, one third of the countries in the region do not permit organizations to rely on legitimate interests as a legal basis for their processing. Three of the countries in this group also do not provide for contractual necessity as a legal basis. One country permits processing on the basis of consent only.

Security:

Furthermore, all of the laws require organizations that collect, use and disclose personal information to take reasonable precautions to protect that information from loss, misuse, unauthorized access, disclosure, alternation and destruction. Two-thirds of the countries have specified in greater detail how these obligations are to be met.

Access and Correction:

One of the core elements of every privacy law is the right of all individuals to access the information that organizations have collected about them and, where possible and appropriate, correct, update or suppress that information. Interestingly, compared to their EU and Asian counterparts, many countries in this region require organizations to respond to access and correction requests in a much shorter period of time. Slightly more than half of the countries (nine) require organizations to respond to access and/or correction requests within 15 days or fewer (two require as little as five days); more than one-third (seven) require responses within 30 days and two others do not specify any time periods.

Data Integrity:

Organizations that collect personal information must also ensure that their records are accurate, complete and kept up-to-date for the purposes for which the information will be used.

Data Retention:

Generally these laws require organizations to retain the personal information only for the period of time required to achieve the purpose of the processing. Specific retention periods of time are not prescribed in many of laws in this region, with Russia being the most notable exception. Russia requires that when the purposes have been achieved or if the individual withdraws his or her consent to the processing, the operator must discontinue the processing, destroy the data within 30 days and notify the individual that his or her data has been destroyed.

Differences in Approaches

While the core data protection principles and requirements are embodied in all of these laws, specific requirements, particularly with respect to cross-border transfers, registration, data security, data breach notification and the appointment of a data protection officer (DPO), vary widely from each other and from laws in other regions of the world.

For example, all but two of the countries in the region require registration of processing, and all but one restrict cross-border transfers; however, the reality is that there are 15 different registration and 16 different cross-border rules and procedures. Generally a contract, consent or a contract and consent are required to transfer outside the country. In some cases, the EU Standard Contractual Clauses (SCCs) may be used; in others, the data protection authorities (DPAs) have not specified what must be contained in these contracts or rules. Two-thirds of the DPAs in the region recognize the EEA countries and/or signatories to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) as providing adequate protection. One-third have not issued lists of countries that they believe provide adequate protection, and thus companies are left to assume that all countries are deemed to be inadequate and must put in place mechanisms (such as consent or contracts) to satisfy the rules.

There are 15 different registration and 16 different cross-border rules and procedures.

The differences widen when comparing their respective rules on data breach notification, security and DPO obligations: one-quarter require notification in the event of a data breach; one-third require the appointment of a DPO; and two-thirds have specified in greater detail how their security obligations are to be met.

A careful read of these laws is imperative. These differences pose challenges to organizations, with respect to the adjustments that may be required to global and/or local privacy compliance practices, as well as privacy staffing requirements. Compliance programs that comply with only EEA obligations will run afoul of many of the country obligations of this region.

A country-by-country summary of the obligations in these key areas is provided below. Other noteworthy characteristics are also highlighted and, where applicable, the responsible enforcement authority is identified. In addition, a chart is provided at the end to show at a glance the countries with mandatory cross-border, DPO, data security breach notification and registration obligations.

Trends

Enforcement:

There are wide variations within this region with respect to enforcement activities, depending on the maturity of the regulatory regime. In some countries, there is no real DPA (Belarus), the DPA has yet to be established (Armenia) or the DPA was recently established (Azerbaijan and Georgia). For example, in Georgia, the DPA's enforcement powers vis-a-vis the private sector only began in late 2014 but the DPA has already imposed fines for law violations, such as for failing to obtain consent, violating direct marketing rules by not providing the ability to opt out, and failing to demonstrate that consent had been obtained to disclose personal information.

One of the most significant, recent developments in this region was the entry into force of Russia's data localization requirements in September 2015.

Countries such as Kosovo, Macedonia and Moldova are more focused on building awareness of individuals' privacy rights and private and public sector obligations under the law; although all three conduct routine inspections and issue enforcement actions when violations are found. In Bosnia, the DPA has been largely focused on public sector processing of personal information.

In contrast, in Albania, which has had a privacy law in place since 2008, the DPA conducts regular inspections, issues corrective orders when violations are found and then conducts follow up inspections to confirm the changes have been implemented. It issues administrative fines if the organization fails to implement its orders. In 2015, in response to complaints received, the Albania DPA conducted a joint investigation of call center companies with the Italy DPA. Fines were issued to call center companies for law violations.

In Serbia, the DPA is advocating for the adoption of a new data protection law: one that will, among others, provide the DPA with authority to issue binding decisions. Last year, the DPA reported that most of the data controllers have failed to comply with Serbia's data protection requirements, citing as an example that less than half of one percent of data controllers have filed the mandatory DPA notifications/registrations.

Data Localization:

One of the most significant, recent developments in this region was the entry into force of Russia's data localization requirements in September 2015 (174 PRA, 9/9/15). Enacted in July 2014, the Data Localization Law amends three existing laws, including the Federal Law No. 152-FZ On Personal Data, and requires that personal information of Russian citizens be stored in Russia (134 PRA, 7/14/14;130 PRA, 7/8/14). All operators who are subject to DPA notification requirements under the Federal Law No. 152-FZ On Personal Data must notify the DPA of their personal data processing servers, and operators found by a court to have violated Russian laws on processing personal data will have their websites blocked by the DPA and be listed on a public register of companies that have been found to be in violation of the law. Non-compliance with the data localization requirement can result in administrative penalties, civil penalties and damages and criminal sanctions. Individuals whose personal information is not processed in compliance with the law also have a private right of action for damages and compensation of moral harm.

While the current maximum fines are very low, the Russian Parliament may amend the Russian Code of Administrative Offences to increase the maximum fine to 300,000 rubles ($4,537). The Russian state magistrate courts responsible for deciding administrative fines also may issue an order to rectify noncompliance with the law. Failure to comply with the magistrate court's order may result in criminal liability for company executives.

Since the data localization requirements went into effect, the DPA has been actively auditing large multinationals to determine whether their local businesses meet the Russian data localization requirements. In 2015, the DPA audited 317 companies and found only two local businesses violating the data localization requirements. In mid-January 2016, the DPA announced a detailed plan for 1000 scheduled data localization compliance audits during the course of the year.

Right to Be Forgotten:

Russia has enacted a law on the right to be forgotten and Ukraine is poised to do the same. In addition, a Turkish court has recently recognized for the first time, a very broad right to be forgotten that applies to digital and analog information carriers (e.g., books).

Russia passed its right to be forgotten law in July 2015 (135 PRA, 7/15/15). The law, which entered into effect on Jan. 1, 2016, requires that a search engine remove links to information that is unreliable or false, outdated or irrelevant, or posted in violation of the law (01 PRA, 1/4/16). Search engines have 10 days to either remove the links or provide a reasoned explanation for refusal. Search engines that violate the law on the right to be forgotten are subject to fines of 80,000 to 100,000 rubles ($1,210-$1,512) if they refuse to remove links at an individual's request and fines of 800,000 to 1 million rubles ($12,098-15,123) if they violate a court order to remove links. However, Russian search engines have been hesitant to approve many of the right to be forgotten requests. Since the law took effect in January, 73 percent of requests have been denied by Yandex LLC—Russia's leading search engine.

Russia has enacted a law on the right to be forgotten and Ukraine is poised to do the same. In addition, a Turkish court has recently recognized for the first time a very broad right to be forgotten.

In April 2016, legislation was introduced into the Ukrainian Parliament that if approved would amend the country's Civil Code to allow Ukrainian citizens to demand removal and retraction of online information if it discredits “honor, dignity or business reputation of an individual” (74 PRA, 4/18/16). The legislation would also make the retraction available online.

Lastly, in a recently published judgment, the Turkish Court of Appeals has recognized a very broad right to be forgotten that applies not only to digital but also to analog information carriers (e.g., books) . At the time of the Court of Appeals ruling, Turkey had not yet enacted data privacy legislation; however, the court used the EU data protection laws and the European Court of Justices' Google v. Spain decision to develop and apply the right to be forgotten. The Turkish Court of Appeals defined the right to be forgotten as a broad right to request erasure and prevention of further dissemination of information pertaining to an individual's past, when such personal information could have negative effects on the individual's future.

New Data Protection Law:

Turkey became the most recent country in this region to enact data protection legislation in March 2016. The Law on the Protection of Personal Data is intended to bring Turkey, which is seeking to gain admittance into the EU, into compliance with the EU data protection law. Some provisions of the Turkish Law took effect in April while others, such as cross-border transfers, access and correction, registration, and penalties, do not take effect until October 2016.

ALBANIA

The Protection of Personal Data Law (Albanian Law) which became effective in 2008 and amended mostly recently in 2014, regulates the processing of all personal information of natural persons by both the public and private sectors.

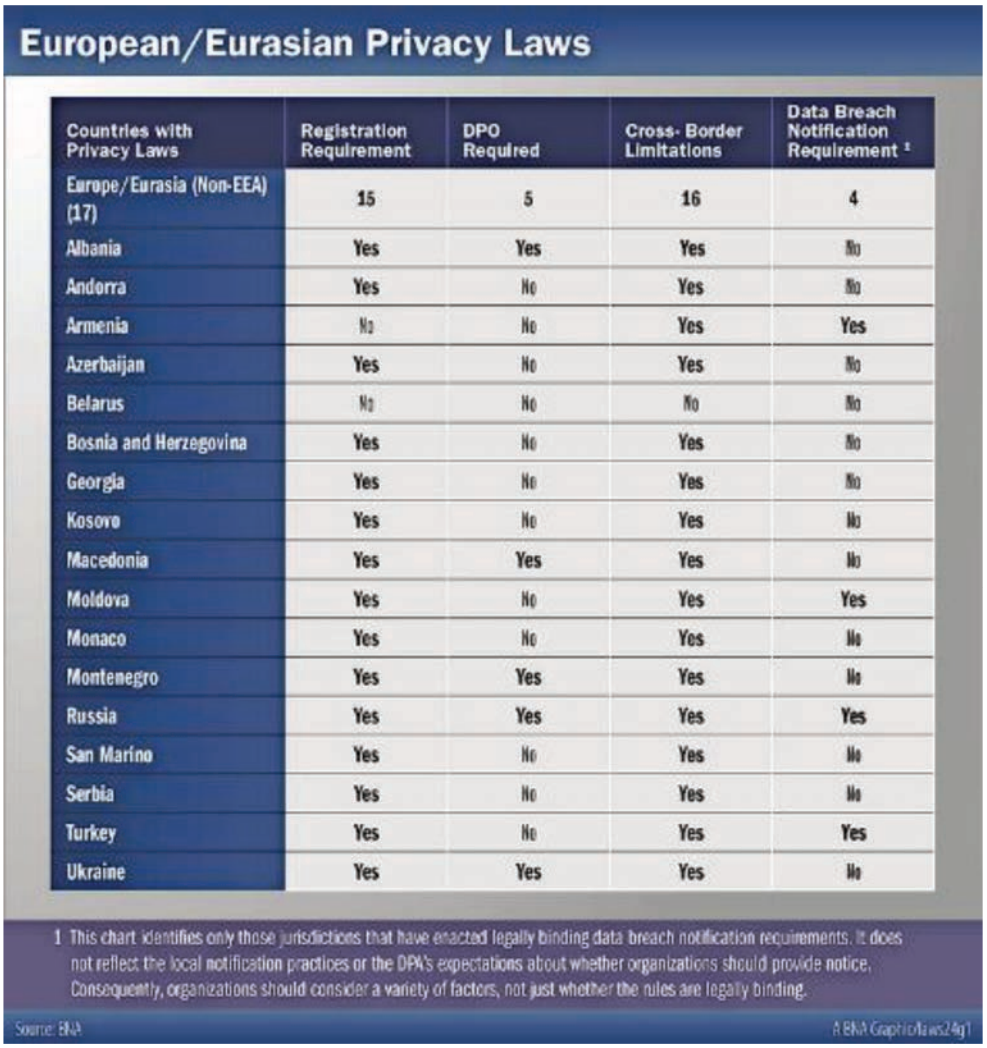
In Brief

The Albanian Law requires database registration, imposes DPO and special data security obligations, and restricts cross-border transfers to countries that do not provide adequate protection.However, there are no data breach notification requirements.

Special Characteristics

Data Protection Authority

The Commissioner for Information Rights and Protection of Personal Data (DPA), an independent administrative authority, is charged with overseeing compliance with the Albanian Law. It carries out online and onsite inspections on its own initiative and in response to complaints and issues fines, most commonly in cases where organizations fail to implement its recommendations or orders. In 2015, in response to complaints received, it conducted a joint investigation of call center companies with the Italy DPA which resulted in administrative fines.



European/Eurasian Privacy Laws

Countries with Privacy Laws	Registration Requirement	DPO Required	Cross- Border Limitations	Data Breach Notification Requirement [1]
Europe/Eurasia (Non-EEA) (17)	15	5	16	4
Albania	Yes	Yes	Yes	No
Andorra	Yes	No	Yes	No
Armenia	No	No	Yes	Yes
Azerbaijan	Yes	No	Yes	No
Belarus	No	No	No	No
Bosnia and Herzegovina	Yes	No	Yes	No
Georgia	Yes	No	Yes	No
Kosovo	Yes	No	Yes	No
Macedonia	Yes	Yes	Yes	No
Moldova	Yes	No	Yes	Yes
Monaco	Yes	No	Yes	No
Montenegro	Yes	Yes	Yes	No
Russia	Yes	Yes	Yes	Yes
San Marino	Yes	No	Yes	No
Serbia	Yes	No	Yes	No
Turkey	Yes	No	Yes	Yes
Ukraine	Yes	Yes	Yes	No

1 This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

Source: BNA

BNA Graphics/laws24q1

Country-by-Country Review of Differences

Access and Correction

Access and correction requests must be responded to within 30 days.

Cross-Border Transfers

There are no restrictions on cross-border transfer of personal information to recipients in countries that provide an adequate level of protection. Albania has recognized all EU/EEA countries, signatories to the 1981 Council of Europe Convention for "Protection of Individuals with regard to Automatic Processing of Personal Data," and countries recognized by the European Commission as providing adequate protection. To transfer personal information to a country that does not provide an adequate level of protection, DPA authorization is required or an exception under the law must apply. Exceptions include consent, contractual necessity, vital interests, or legal requirement.

Data Protection/Security Officer

Large controllers (with six or more persons engaged in data processing) must authorize in writing one or more persons responsible for the internal data security supervision. One of the people appointed will serve as the contact person, registered

with the Commissioner. Small controllers (with less than six persons engaged in data processing) may, but are not required to, authorize in writing, one or more persons responsible for the internal security supervision.

Data Security

Different organizational and technical data security measures are provided by law, depending on whether the controller is large or small. For example, small controllers must carry out a risk assessment procedure as a minimum standard measure of data security. Large controllers must apply and maintain an information security management system (SMSI). SMSI is based on the identification, assessment and mitigation of risks threatening personal information security while taking into consideration: (i) the information technology and communication system used to process personal information, (ii) all manual forms of processing personal information and (iii) the physical security of premises and the security of the personnel, electronic and moveable equipment. The risk assessment and treatment are part of the mandatory Information Security Policy (PSI) of the controller. Large controllers must carry out information security audits at least once per year and provide security training to employees. In addition, there are encryption requirements in connection with transfers of sensitive information and equipment used to process information through cloud computing platforms.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legal requirement, legitimate interests, or vital interests.

Registration

The Albanian Law requires that controllers notify the DPA of all categories of personal information they process for all purposes unless one of the limited exemptions applies. However, even when a notification exemption applies, minimum information on the data processing activities must be provided such as: name and address of controller, categories and purposes of processed information and categories of recipients. Depending on the category of information, the controller must either register the processing or obtain an authorization from the DPA prior to processing.

ANDORRA

The Protection of Personal Data Law (Andorran Law), which became effective in 2004, regulates public and private sector processing of all personal information of natural persons, except where the information relates to their business, professional or commercial activities. Andorra is regarded as providing an adequate level of protection for personal information transferred from the EU/EEA.

In Brief

The Andorran Law requires database registration and the appointment of a DPO and restricts cross-border transfers to countries that do not provide adequate protection. In addition, the period of time within which organizations must respond to access requests is exceedingly short and there is no provision for processing personal information on the basis of legitimate interests. However, there are no special security and data breach notification requirements.

Special Characteristics

Data Protection Authority

The Andorran Agency for Data Protection (DPA), an independent public authority, is responsible for overseeing compliance with the Andorran Law

Access and Correction

Organizations must respond to access requests within five working days and correction requests within one month.

Cross-Border Transfers

Personal Data may not be transferred to third countries that do not provide an equivalent level of protection unless consent or another of one of the limited exceptions such as contractual obligations, vital interests or legal requirements applies. Countries that provide an equivalent level of protection are the EU Member States and countries found by the European Commission or the Andorran DPA to provide equivalent protection.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legal requirement, or vital interests.

Registration

Controllers must register their databases with the DPA and update their registration records whenever there is a change in the information listed.

ARMENIA

The Law on Personal Data (Armenian Law), which became effective in 2015, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

The Armenian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security and breach notification obligations. In addition, the period of time within which organizations must respond to correction requests is exceedingly short and there are limited legal bases provided for the collection and use of personal information. However, there is no DPO obligation.

Special Characteristics

Data Protection Authority

The Law provides for the establishment of the Authorized State Body for the Protection of Personal Data Processing (Armenian DPA); however, it is not yet established.

Access and Correction

The Armenian Law does not specify a time period for responding to access requests. Corrections should be carried out (or refused) within five days after receiving the written request.

Cross-Border Transfers

Personal Data may be transferred cross border either with the consent of the individual or where the transfer is necessary to carry out processing previously consented to by the individual. In addition, DPA authorization is required to transfer to those countries that are not on the DPA's approved list of countries that provide adequate protection. A transfer permit is required in such cases. The DPA must also approve the organization's contractual clauses governing the transfer.

Data Breach Notification

The controller must make a public announcement without delay and notify the police and the DPA when a data security breach occurs.

Data Security

Encryption measures are required to protect information systems containing personal information from loss, unauthorized access, illegal use and destruction, and illegal copying and disclosure. The law also provides for the government to set security standards in information systems, physical records of biometric data and personal data storage technologies other that electronic information systems.

Legal Basis for Collection and Use

Personal information may be processed only with the consent of the individual or where such processing is provided for or required by law or where the data are publicly available.

Registration

The DPA has the right to require controllers to notify the DPA about the collection or processing of personal information; otherwise such notification is voluntary.

AZERBAIJAN

The Law on Personal Data (Azerbaijani Law), which became effective in 2010, regulates the processing of all personal information of natural persons by both the public and private sectors. The Azerbaijani Law differentiates personal information according to public and confidential categories. Public data are: (i) data that are depersonalized or anonymized, (ii) data that are declared public by the individual or (iii) data that are included in an information system created for general use with the consent of the individual. A natural person's name, last name, and patronymic will always be considered as public data.

In Brief

The Azerbaijani Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security obligations. In addition, the period of time within which organizations must respond to access and correction requests is exceedingly short and there are limited legal bases provided for the collection and use of personal information. However, there is no data breach notification or DPO obligations.

Special Characteristics

Data Protection Authority

The State Register at the Ministry of Communications and Information Technologies (DPA) is responsible for registering information systems and ensuring compliance with the Azerbaijani Law.

Access and Correction

Organizations must respond to access and correction requests within seven days.

Cross-Border Transfers

Cross-border transfers are be prohibited where: (i) such transfer creates a threat to the national security of the Azerbaijan Republic, or (ii) the laws of the countries to which the personal information is transferred do not provide the same level of protection as that provided by Azerbaijani laws. However, personal information can be transferred across the border to a country regardless of the level of legal protection of personal information where the individual expressly agrees to the transfer. In addition, although not expressly stated in the Law, cross border transfers are permitted where the transfer is necessary to protect the life or health of the individual. DPA authorization is not required; however, information on such transfer and the categories of the personal information transferred must be provided to the DPA at the time of the registration of the information system. The DPA has stated informally that the cross-border transfer provisions apply to the transfer of databases (i.e. personal information of a significant number of individuals); transfers of personal information limited to one or several individuals across the border would likely trigger the rules for transfers to third parties, not the cross border transfer rules.

Data Security

Controllers and processors must implement organizational and technical measures to guarantee the security of personal information during its collection, use and disclosure (including cross-border transfer). They must determine the risks for the security of the personal information and based on such risks must continually improve the information system in order to neutralize possible risks. There are regulations that prescribe a long list of technical organizational safety requirements. Organizations must encrypt all transmitted records. The length of the encryption key used during the transfer may not be less than 256 bit.

As is evident from the registration card for information systems approved by the Regulations on the Registration and Deregistration of Information Systems, organizations must have control and audit mechanisms for the collection and processing of personal information; however, the frequency of such audits and their substance have not been specified.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, legal requirement, or vital interests.

Registration

Information systems containing personal information must be registered with the State Register unless an exemption applies. The State Registry is maintained by the Data Computing Center at the Ministry of Communication and Information Technologies.

BELARUS

The Law On Information, Informatization and Protection of Information (Belarusian Law), which became effective in 2008, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

Under the Belarusian Law, consent is the only permissible basis on which to process (and transfer cross-border) personal information. In addition, the law imposes special security obligations; however, there are no registration, breach notification, or DPO obligations.

Special Characteristics

Data Protection Authority

There is no DPA in Belarus akin to the DPAs found in other jurisdictions. The state authority that performs any data protection-related functions is the Operative Analytics Center of the President of the Republic of Belarus (OAC). However, to date, OAC's competence is more technical in nature and does not include only data protection-related competence. For example, the OAC is empowered to certify information technology (IT) systems, hardware and software data protection solutions, and regulate general IT and Internet relations.

Access and Correction

The Belarusian Law does not specify a time period for responding to access requests and is silent on correction rights.

Cross-Border Transfers

There are no specific limitations on cross-border transfers. By general rule, each transfer, including cross-border transfers, require the consent of the individual.

Data Protection/Security Officer

A special individual or department for security measures must be appointed.

Data Security

Controllers must take effective measures to ensure security of personal information from the moment of receipt until its destruction. Under the Belarusian Law and implementing regulations, this obligation includes various organizational and technical security measures. In particular, controllers must maintain a data protection system certified by the certification centers accredited by the DPA. Organizations must file annual reports on their security measures to the OAC by Dec. 30.

In addition, there are cryptographic regulations that define legal and organizational basics of technical and cryptographic measures of information security. Controllers must comply with these regulations which among others things require that personal information be encrypted in transit. [1]

---

[1] Regulation on Technical and Cryptographic Security of Information in the Republic of Belarus, approved by the Edict of the President of the Republic of Belarus N 196 On Certain Measures for Improving Information Security, 2013, available here (in Russian).

Regulation On the Technical Security of Information and Regulation On the Technical and Cryptographic Protection of Information, both approved by the Order of Operative Analytics Center of the President of the Republic of Belarus of 30 August 2013 N 62, available here (in Russian)

Legal Basis for Collection and Use

Consent is required to process Personal Data. The Belarusian Law does not provide for any other legal bases such as

contractual necessity, vital interests or legal requirements.

BOSNIA AND HERZEGOVINA

The Law on the Protection of Personal Data (Bosnia and Herzegovina Law), which became effective in 2006, regulates the processing of all personal information of natural persons by the public and private sectors. [2]

[2] The 2011 amendments to the Bosnia and Herzegovina Law is available in English here.

In Brief

The Bosnia and Herzegovina Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security obligations. However, there are no data breach notification or DPO obligations.

Special Characteristics

Data Protection Authority

The Personal Data Protection Agency (DPA), an independent administrative organization, is responsible for enforcement of the Bosnia and Herzegovina Law.

Access and Correction

Access requests must be responded to within 30 days; there is no specified time period for responding to correction requests.

Cross-Border Transfers

Personal Data may not be transferred to another country that does not guarantee adequate safeguards for personal information that are equivalent to those under the Bosnia and Herzegovina Law, unless the prior consent of the individual has been obtained or another exception applies, such as contractual necessity or vital interests. Exceptionally, the DPA may authorize such transfers. Neither the Bosnia and Herzegovina Law nor the DPA provide a specific list of “adequate” countries, so the controller is responsible for assessing whether the country to which personal information are transferred guarantees protections equivalent to those provided for under the Bosnia and Herzegovina Law.

Data Security

In addition to the general security obligations under the Bosnia and Herzegovina Law, regulations issued in 2009 set forth more detailed security requirements. In particular, the regulations require controllers and processors, among other things, to have a written security plan, data protection training for employees and additional technical and organizational security measures for sensitive information such as encryption or equivalent “crypto-protection” when the data are in transit.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, legal requirement, or vital interests.

Registration

Controllers must register all processing of personal data with the DPA prior to the establishment of the personal data filing system or any processing, unless one of the very narrow registration exemptions applies.

GEORGIA

The Law on the Protection of Personal Data (Georgian Law), which went into effect in 2012 and amended in 2014, regulates the processing of all personal information of natural persons by the public and private sectors.

In Brief

The Georgian Law requires database registration and restricts cross-border transfers to countries that do not provide

adequate protection. However, there are no data breach notification, DPO, or special security obligations.

Special Characteristics

Data Protection Authority

The Personal Data Protection Inspector (DPA), an independent authority, is responsible for enforcing the Georgian Law.

Access and Correction

Organizations must respond to access requests within 10 days and correction requests within 15 days.

Cross-Border Transfers

Transfers of personal information outside Georgia are permitted to countries that provide adequate protection. The DPA issued a list of approved countries that include: the EEA countries, Australia, Albania, Andorra, Argentina, New Zealand, Bosnia and Herzegovina, Israel, Canada, Croatia, Macedonia, Moldova, Monaco, Montenegro, Serbia, Ukraine and Uruguay. Where transfers are to jurisdictions that are not recognized as providing adequate protection, DPA-approved contracts are required.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration

Controllers must register with the DPA prior to creation of filing systems and inclusion of new categories of data in those filing system.

KOSOVO

The Law on the Protection of Personal Data (Kosovo Law), which went into effect 2010, regulates the processing of all personal information of natural persons by the public and private sectors.

In Brief

The Kosovo Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security obligations. However, there are no data breach notification or DPO obligations.

Special Characteristics

Data Protection Authority

The National Agency for the Protection of Personal Data (DPA), an independent agency, is responsible for enforcing the Kosovo Law.

Access and Correction

Organizations must respond to access requests within 15 days and provide access within 30 days. They must comply with correction requests within 15 days.

Cross-Border Transfers

Personal Data may only be transferred to countries outside Kosovo that ensure an adequate level of data protection, unless one of the legal bases for data transfer applies (e.g., consent, contractual necessity, or vital interests). Adequate countries include the EEA countries and the other jurisdictions recognized by the EU as providing adequate protection. The DPA must be notified about all transfers to inadequate countries; authorization is required for such transfers.

Data Security

Among other requirements, controllers and processors must have internal documentation that describes the personal information security measures that are in place. Sensitive personal information must be specifically protected and classified in order to prevent unauthorized access and use. Sensitive personal information that is transmitted over telecommunications networks will be considered suitably protected if the information is encrypted to ensure that it is rendered incomprehensible or unrecognizable.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration

Registration is required. The controller must keep a record of all processing of personal information, the "Filing System Catalogue," a copy of which must be filed with the DPA prior to establishment of the filing system.

MACEDONIA

The Law on Personal Data Protection ("Macedonian Law"), which went into effect in February 2005, regulates the processing of all personal information of natural persons by the public and private sectors.

In Brief

The Macedonian Law requires database registration and the appointment of a DPO, restricts cross-border transfers to countries that do not provide adequate protection and imposes special security obligations. However, there is no data breach notification obligation.

Special Characteristics

Data Protection Authority

The Directorate for Personal Data Protection (DPA), an independent state authority, is responsible for enforcing the Macedonian Law.

Access and Correction

Organizations must respond to access requests within 15 days and correction requests within 30 days.

Cross-Border Transfers

Personal information may be transferred to countries that provide adequate protection, such as EEA countries. For all other transfers, one of the transfer exemptions must apply (e.g., consent, contractual necessity, or vital interests) or prior DPA authorization is required. In order to obtain approval of the Directorate, a written data transfer agreement must be in place between the controller and the recipient, preferably based on the EU standard contractual clauses.

Data Protection Officer

The appointment of a DPO is required except where the controller a) has a collection of personal information that only refers to ten employees or less; or b) processes personal information of members of associations founded for political, philosophical, religious or trade-union purposes.

Data Security

There are special security rules that together with the security provisions under the Macedonian Law require, among other things, the adoption and implementation of written security programs, carrying out risk assessments, conducting annual internal and triannual external audits, providing employee security training and encrypting data in transit, data stored on portable devices, and back-up copies.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests and legal requirements.

Registration

All data must be registered by controllers for all purposes, unless one of the limited exemptions applies.

MOLDOVA

The Law on Personal Data Protection (Moldovan Law), which took effect in April 2012, regulates the processing of all personal information of natural persons by the public and private sectors.

In Brief

The Moldovan Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes data breach notification and special security obligations. However, there is no DPO obligation.

Special Characteristics

Data Protection Authority

The National Centre for Personal Data Protection (DPA), an independent agency, is responsible for enforcing the Moldovan Law.

Access and Correction

Access and correction requests must be responded to without delay (no time period is specified).

Cross-Border Transfers

Personal Data may not be transferred to countries outside Moldova unless that country ensures an adequate level of protection. If the proposed transfer is to a country that is not considered adequate, one of the transfer exceptions must apply, such as consent, contractual necessity, or vital interests. DPA authorization is also required in such cases.

Data Security

The Moldovan Law and implementing regulations prescribe detailed security requirements which include the need to maintain and reevaluate annually the organization's data security policy and implement specific physical and electronic security measures, including encryption. Regular data security audits must be carried out. These audits must include an assessment of the organization, its security measures and use of communication partners and suppliers. The results of the security audit must be documented.

Data Security Breach Notification

All controllers must submit to the DPA an annual report on any security incidents involving information systems during that year.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests and legal requirements.

Registration

Controllers and processors must register their processing for all purposes unless one of the limited exemptions applies.

MONACO

The Protection of Personal Data Act (Monaco Law), which took effect in December 1993, regulates the processing of personal data of natural persons by the public and private sectors.

In Brief

The Monaco Law requires database registration and the appointment of a DPO and restricts cross-border transfers to countries that do not provide adequate protection. However, there are no data breach notification or special security obligations.

Special Characteristics

Data Protection Authority

The Personal Data Protection Supervisory Commission (DPA) is responsible for enforcement compliance with the Monaco Law.

Access and Correction

Access and correction requests must be responded to within one month.

Cross-Border Transfers

Personal information may not be transferred outside Monaco unless the recipient country provides an adequate level of protection. Parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) are recognized as providing adequate protection. Where the transfer is to a country which does not provide adequate protection, one of the specified legal bases, such as consent, vital interests or contractual necessity must apply. In addition, the DPA may authorize transfers on the basis of appropriate contractual clauses.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, and legal requirements.

Registration

Controllers must register all automatic processing of personal information with the DPA unless one of the limited exceptions applies. Certain processing is also subject to DPA authorization (e.g., biometric data).

MONTENEGRO

The Personal Data Protection Law (Montenegrin Law), which took effect in 2012, regulates the processing of personal data of natural persons by the public and private sectors.

In Brief

The Montenegrin Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO and special security obligations. However, there is no data breach notification obligation.

Special Characteristics

Data Protection Authority

The Personal Data Protection Agency (DPA), an independent regulatory authority, is responsible for enforcing the Montenegrin Law.

Access and Correction

Organizations must respond to access and correction requests within 15 days.

Cross-Border Transfers

Personal Data may be transferred from Montenegro to an EEA country or a country deemed adequate by the EU, or where the transfer is based on EU standard contractual clauses. Alternatively, the transfer may take place where another legal basis

applies such as consent, contractual necessity, or vital interests. Otherwise, DPA authorization is required.

Data Protection Officer

Where the controller has 10 or more employees performing data protection activities, the controller must designate a person who will be responsible for the data protection matters immediately after establishing a personal data filing system.

Data Security

Detailed security requirements are set forth in the Regulation on the Form and Manner of Maintaining of Personal Data Filing System, covering areas such as the form, the manner of keeping data in personal data filing systems, the content of the records, the types of personal information contained in the filing system, the data retention periods, the manner of collection of personal information, and the transfer of data. For example, the Regulations require that sensitive information be kept separately, according to the type of data and that the legal basis on which the personal information is being processed is noted in the data filing system.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests and legal requirements.

Registration

Prior to establishing a personal data filing system, the controller must inform the DPA by submitting the notification containing all the prescribed elements. Personal data filing systems required by law do not require registration.

RUSSIA

The Federal Law No. 152-FZ On Personal Data (Russian Law), which took effect January 2007, regulates the processing of all personal information of natural persons by the public and private sectors. The Russian Law was recently amended in 2014, imposing controversial data localization requirements.

In Brief

The Russian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO, data breach notification, special security and data localization obligations. In addition, the period of time within which organizations must respond to correction requests is exceedingly short and there is no provision for processing personal information on the basis of legitimate interests.

Special Characteristics

Data Protection Authority

The Federal Service for Supervision in the Field of Communication Information Technology and Mass Communications, comm only known as Roscomnadzor, (DPA) is responsible for enforcement of the Russian Law.

Access and Correction

Organizations must respond to access requests within 30 days, and correction and deletion requests within 10 days.

Cross-Border Transfers

Personal Data may only be transferred to a country that provides a sufficient level of protection. The countries recognized by the DPA as providing adequate protection include: all of the signatories to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Armenia, Azerbaijan, Bosnia & Herzegovina, Georgia, Moldova, Montenegro, Macedonia, San Marino, Serbia, Turkey, Ukraine, Uruguay and the EEA Member States), Angola, Argentina, Australia, Benin, Canada, Cape Verde, Chile, Israel, Hong Kong, Malaysia, Mexico, Mongolia, Morocco, New Zealand, Peru, Senegal, South Korea, Switzerland and Tunisia.

Transfers to countries that do not provide adequate protection are permitted where there is a legal basis such as consent,

contractual necessity, or vital interests. Prior DPA approval or authorization is not required; however, if the organization is subject to the registration requirements, it must indicate in its registration the countries to which it transfers the information.

Data Protection Officer

The appointment of an internal data protection officer is required.

Data Localization

Under the amended law, organizations that collect and process personal information of Russian citizens (in electronic and paper form) must store that information in Russia. Organizations must notify the DPA of their server locations. The DPA will maintain a register of violators and will block any infringing websites. These localization requirements only apply to deliberate activities to collect information from Russians.

Data Breach Notification

In the event of a data security breach, organizations must take measures to remedy the breach (or, if that is not possible, to destroy the affected data) within three days and then notify affected individuals about such measures. The DPA must be notified (about rectification of the breach) only if it has issued a request to the organization to remedy the breach. The requirements to notify individuals about a security breach apply to any situation where an organization has processed the wrong data or there was any unauthorized processing of personal information. Such a breach may be detected by the organization itself or as a result of an access or correction request by the individual concerned.

Data Security

Organizations must take all reasonable organizational and technical measures to protect personal information, which include adopting internal data protection rules that are mandatory for all employees and conducting risk assessments, audits and oversight of compliance with the Russian Law. In addition, organizations must maintain special IT systems for protecting Personal Data (software and hardware measures) that comply with the technical requirements of the Russian Federal Security Service (FSB) and the Federal Service for Technical and Export Control (FSTEK), and in particular with the Order of FSTEK No. 21 dated Feb. 18, 2013.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legal requirements, or vital interests.

Registration

Organizations must notify the DPA of their intent to process personal information, unless an exception applies. For example, registration is not required to process employee data or where personal information was obtained through an agreement between the organization and the individual concerned, and such information is not distributed or transferred to third parties without the consent of the individual. They are used by the organization solely for the purposes of performance of the agreement or for entering into new agreements with the individual in the future.

Organizations must also register the location of databases that contain personal information of Russian citizens.

SAN MARINO

The Law Regulating the Collection of Personal Data (San Marino Law), which went into effect in 1995, regulates the processing of all personal information of natural and legal persons by the public and private sectors.

In Brief

The San Marino Law requires DPA authorization to process personal information unless one of the limited legal bases applies. There is no provision for processing personal information on the basis of consent (except in the case of sensitive information) or legitimate interests. DPA authorization is always required for crossborder transfers. However, there are no DPO, data breach notification, or special security obligations.

Special Characteristics

Data Protection Authority

The Garante for the Protection Of Confidentiality of Personal Data (DPA) is responsible for enforcement of the San Marino Law. There is no website for the DPA.

Access and Correction

The San Marino Law does not prescribe a time frame to comply with access and correction requests.

Cross-Border Transfers

DPA authorization is required to transfer cross-border personal information of San Marino citizens or companies. The San Marino Law does not set out any specific requirements or conditions that must be met to obtain DPA authorizations for such cross-border transfers.

Legal Basis for Collection and Use

To collect and use personal information in a private data bank, prior DPA authorization is required unless an exception applies such as contractual necessity, legal requirement or the information is publicly available. The San Marino Law does not set out consent obligations for the use of personal information except where such information concern political, union or religious opinions and activities. In such cases, express consent is required.

Registration

Prior DPA approval is required for the collection, processing and use of personal information by private owners of data banks unless an exception applies such as such as contractual necessity, legal requirement, the information is publicly available, or the personal information is processed by a political, social or cultural organization and relate to the members of that organization.

SERBIA

The Law on Personal Data Protection (Serbian Law), which went into effect in 2009, protects all personal data of natural persons processed by the public and private sectors.

In Brief

The Serbian Law requires database registration and restricts cross-border transfers. In addition, the period of time within which organizations must respond to correction requests is exceedingly short. However, there are DPO, data breach notification, or special security obligations.

Special Characteristics

Data Protection Authority

The Commissioner for Information of Public Importance and Personal Data Protection (DPA) is responsible for enforcing the Serbian Law.

Access and Correction

Organizations must respond to access requests within 30 days and correction and deletion requests within 10 days.

Cross-Border Transfers

Data can be transferred from Serbia to a country that is a signatory to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Data may be transferred to a state that is not a party to the Convention if such state has a regulation or a data transfer agreement in force which provides a level of data protection equivalent to that envisaged by the Convention. In cases of data transfers that do not provided an equivalent level of protection, the DPA authorization is required.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration

Controllers must register their processing with the DPA for all purposes. Very limited exceptions apply.

TURKEY

The Law on the Protection of Personal Data (Turkish Law), which was enacted in March 2016, regulates the processing of personal information of natural persons by individuals and private sector organizations. Some provisions of the Turkish Law took effect in April while others, such as cross-border transfers, access and correction, registration, and penalties, do not enter into force until October 2016. With respect to personal information processed by organizations before the publication of the Turkish Law in April 2016, the organizations must make such information compliant with the Turkish Law within two years or they must delete, destroy or anonymize the data. However, the consents lawfully received before the date of publication of the Turkish Law will be deemed to be compliant with this Law if the individuals concerned have not objected to the processing within one year.

In Brief

The Turkish Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, expansively defines and limits processing of sensitive information, and imposes breach notification and special security obligations. However, there is no DPO obligation.

Special Characteristics

Data Protection Authority

The Turkish Data Protection Board (DPA), which will be established within six months of the Turkish Law's publication date, is responsible for enforcement of the Turkish Law. Its powers include the ability to impose administrative sanctions for law violations.

Cross-Border Transfers

To transfer personal information outside of Turkey, express consent of the individual must be provided unless one of the exceptions applies (e.g., contractual necessity, vital interests, legitimate interests, or legal requirement). In addition, the transfer of personal information may only be to countries that provide adequate protection (the DPA will provide a list). If the transfer is to a country that does not provide adequate protection, there must be a contract in place between the parties and the DPA must authorize the transfer. These cross-border transfer rules will take effect Oct. 7, 2016.

Data Breach Notification .

Organizations must notify individuals and the DPA “as soon as possible” if personal information is obtained by third parties “in an illegal manner.”

Data Security

The data controller must take every necessary technical and administrative precaution to prevent unlawful processing of and access to personal information and ensure the safeguarding of that information. In addition, the data controller must carry out the necessary internal inspections/audits to ensure compliance with the Turkish Law. If the personal information will be processed by third party processor, the data controller will be jointly responsible for taking of the necessary security measures.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as explicit consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration

Data controllers will need to register their processing activities before they begin processing. Exceptions may be specified by the DPA. The Turkish Law provides for the establishment of the DPA within six months (October 2016). The registration provisions enter into force at the same time; however, the Turkish Law states that the DPA set the date by which data controllers must be registered.

Sensitive Information

The Turkish Law defines special categories of personal information (sensitive information) as information related to a person's racial, ethnic origins, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, membership with associations, foundations or trade-unions, health or sexual life, criminal convictions and biometric and genetic data related to security measures. Processing of this information is prohibited except with the explicit consent of the individual. However, such information—with the exception of health and sexual life—may be processed without explicit consent where such processing is envisaged under Turkish laws. Health and sexual information may be processed by persons or authorized institutions and organizations that are bound by confidentiality obligations, solely for the purpose of protecting public health, preventive medicine, medical diagnosis, treatment and care, healthcare services and healthcare financial planning and management.

UKRAINE

The Law On the Protection of Personal Data (Ukrainian Law), which went into effect in 2011, regulates the processing of all personal data of natural persons by public and private sectors. The Ukrainian Law was recently amended in September 2015.

In Brief

The Ukrainian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO and special security obligations. In addition, the period of time within which organizations must respond to correction requests is exceedingly short. However, there is no breach notification obligation.

Special Characteristics

Data Protection Authority

The Ukrainian Parliament Commissioner for Human Rights (DPA) is responsible for enforcement of the Law.

Access and Correction

Organizations must respond to access and correction requests within 10 days.

Cross-Border Transfers

Personal Data may be transferred to third countries that provide sufficient protection for personal information which include the EEA countries, signatories to the Council of Europe Convention and states on the DPA approved list (which is not yet adopted). Personal information can also be transferred to countries that do not provide adequate protection if a legal basis applies such as consent, contractual necessity, or vital interests. DPA authorization is not required; however, information regarding cross-border transfers of the personal information must be included in the original registration/negotiation filed with DPA .

Data Protection Officer

Organizations must appoint a department or a person responsible for the protection of personal information during the processing of that information.

Data Security Breach Notification

There is no obligation on any entities to give notice in the event of a data security breach; however, the controller must document/log violations of in course of Processing and develop plan of actions in case of unauthorized access to personal information.

Data Security

The Ukrainian Law and implementing regulations require organizations to, among other things, establish an internal security policy and implement specific security measures including employee training, data disposal measures and documentation requirements involving access and control procedures.

Legal Basis for Collection and Use

To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration

Controllers must file a notification with DPA about processing of certain categories of sensitive personal information such as health, biometrical and genetic data, geolocation, trade union or political or religious memberships, race ethnic or national origin, criminal records.

Privacy Law Watch™

June 17, 2016

Data Protection

Global Perspectives: Privacy Laws in East, Central and South Asia and the Pacific

Legislation

In this article of a four-part series on the status of international data protection laws, the author explores developments in East, Central and South Asia and the Pacific where 13 jurisdictions now have comprehensive privacy laws.

By Cynthia Rich

Cynthia Rich is a senior advisor at the Washington office of Morrison & Foerster LLP. As a member of the firm's international Privacy and Data Security Practice since 2001, she works with clients on legal issues relating to privacy around the world.

Introduction/Region at-a-Glance

Privacy legislation in East, Central and South Asia and the Pacific (Asia) has been extremely active in the past few years, and the level of activity and enforcement does not show any signs of slowing down. Thirteen jurisdictions in Asia now have comprehensive privacy laws: Australia, Hong Kong, India, Japan, Kazakhstan, Kyrgyzstan, Macao, Malaysia, New Zealand, the Philippines, Singapore, South Korea and Taiwan. New Zealand is the only jurisdiction in the region that has been recognized by the European Commission as providing adequate protection (244 PRA, 12/20/12).

Notably absent from this list are countries such as China, Thailand, Vietnam and Indonesia. China is slowly moving toward a privacy regime, taking a piecemeal, sectoral approach. (For a detailed discussion of recent privacy law and network security developments in China, see Paul D. McKenzie & Jing Bu, China Update: Privacy Law and Network Security Developments, 1 4 Bloomberg BNA Privacy & Sec. L. Rep. 677 (Apr. 20, 2015).) (82 PRA, 4/29/15). The governments of Thailand and Indonesia have drafted legislation but the bills have yet to be introduced and/or approved by their respective legislatures. Vietnam also appears to be moving slowly in the development of privacy legislation.

This article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments.

Common Elements Found in Asian Laws

Notice:

All of the laws in Asia include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, why it is collected and with whom it is shared.

Choice:

Every privacy law also includes some kind of choice element. The level or type of consent varies significantly from country to

country. For example, South Korea has a much stronger emphasis on affirmative opt-in consent than does New Zealand, but all of the laws include choice as a crucial element in the law.

Security:

Furthermore, all of the laws require organizations that collect, use and disclose personal information to take reasonable precautions to protect that information from loss, misuse, unauthorized access, disclosure, alteration and destruction. Some of the countries—particularly South Korea—have very detailed rules regarding data security that may set the standard for the entire region and also influence the rest of the world.

Access and Correction:

One of the core elements of every privacy law is the right of all individuals to access the information that organizations have collected about them and where possible and appropriate, correct, update or suppress that information. In contrast to their Latin American counterparts, which require organizations to respond to access and correction requests in very short periods of time, many countries in Asia either do not specify specific time frames or provide organizations with a more reasonable time frames, similar to those found in European countries. Notable exceptions include Kazakhstan, Kyrgyzstan, Malaysia, South Korea and Taiwan which have time frames that range from 1-21 days.

Data Integrity:

Organizations that collect personal information must also ensure that their records are accurate, complete and kept up-to-date for the purposes for which the information will be used.

Data Retention:

Generally these laws require organizations to retain the personal information only for the period of time required to achieve the purpose of the processing. Some laws may mandate specific retention periods of time, while others set limits on how long data may be retained by an organization once the purpose of use has been achieved.

Differences in Approaches

While the core data protection principles and requirements are embodied in all of these laws, specific requirements, particularly with respect to cross-border transfers, registration, data security, data breach notification and the appointment of a data protection officer (DPO), vary widely from each other and from laws in other regions of the world.

Japan, New Zealand, Australia and Hong Kong encourage disputes to be resolved voluntarily without resorting to fines, except in large data breach cases or to signal the regulator's intent to enforce recently enacted rules.

For example, two-thirds of the countries in this region restrict cross-border transfers of personal information to countries that do not provide adequate protection. Generally a contract, consent or a contract and consent are required to transfer outside the country. In almost all cases, the data protection authorities (DPAs) have not specified what must be contained in these contracts or rules. Most of the DPAs in the region also have not issued lists of countries that they believe provide adequate protection, and thus companies are left to assume that all countries are deemed to be inadequate and must put in place mechanisms (such as consent or contracts) to satisfy the rules. In addition, unlike their European counterparts, registration is not required in all but three of the jurisdictions in the region.

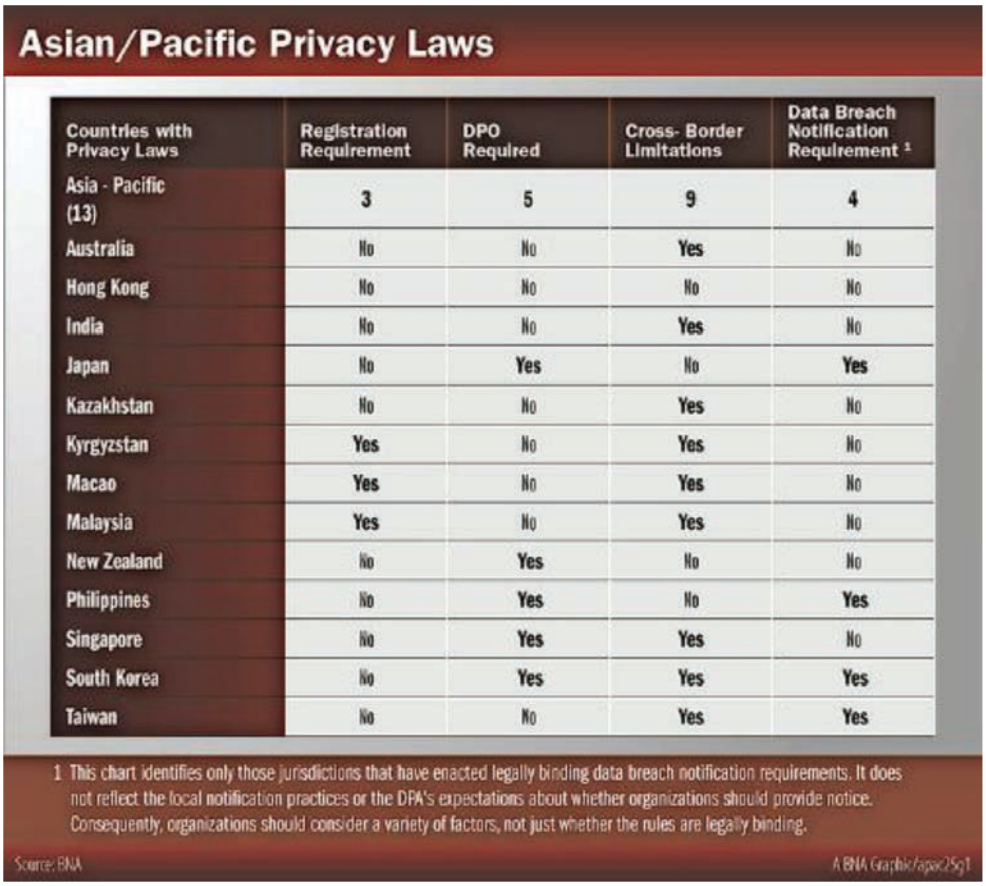
The differences widen when comparing their respective rules on data breach notification, security and DPO obligations: one-third require notification in the event of a data breach and the appointment of a DPO.

Lastly, three of the countries, Kazakhstan, South Korea and Singapore, rely more heavily on consent to legitimize collection, use and disclosure of personal information.

A careful read of these laws is imperative, therefore. These differences pose challenges to organizations, with respect to the adjustments that may be required to global and/or local privacy compliance practices, as well as privacy staffing requirements. Compliance programs that comply with only European Union and Latin American obligations will run afoul of many of the Asian country obligations.

A country-by-country summary of the obligations in these key areas is provided below. Other noteworthy characteristics are also highlighted and, where applicable, the responsible enforcement authority is identified. In addition, a chart is provided at

the end to show at a glance the countries with mandatory cross-border, DPO, data security breach notification and registration obligations.



Asian/Pacific Privacy Laws

Countries with Privacy Laws	Registration Requirement	DPO Required	Cross- Border Limitations	Data Breach Notification Requirement [1]
Asia - Pacific (13)	3	5	9	4
Australia	No	No	Yes	No
Hong Kong	No	No	No	No
India	No	No	Yes	No
Japan	No	Yes	No	Yes
Kazakhstan	No	No	Yes	No
Kyrgyzstan	Yes	No	Yes	No
Macao	Yes	No	Yes	No
Malaysia	Yes	No	Yes	No
New Zealand	No	Yes	No	No
Philippines	No	Yes	No	Yes
Singapore	No	Yes	Yes	No
South Korea	No	Yes	Yes	Yes
Taiwan	No	No	Yes	Yes

1 This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

Source: BNA

A BNA Graphic/apac25g1

Trends

Enforcement:

Violations of these laws can result in significant criminal and civil and/or administrative penalties being imposed; however, the enforcement approaches vary widely from one jurisdiction to another. Japan, New Zealand, Australia and Hong Kong encourage businesses and individuals to resolve disputes voluntarily without resorting to the imposition of fines, except in large data breach cases or to signal the regulator's intent to actively enforce recently enacted rules. In contrast, authorities in South Korea are quick to investigate and impose fines for violations. In Taiwan, the enforcement approach is more varied because enforcement is largely carried out by the competent industry-specific regulators, so the level of enforcement, as well as the interpretations of the compliance obligations under the law, often vary from one regulator to another. In jurisdictions such as Singapore and Malaysia, the regulators are still working with industry to encourage compliance with these new laws, although Singapore recently initiated its first data protection-related enforcement actions, almost two years after the Singapore Law went into effect.

Data Breaches:

Requirements in this region related to cross-border transfers, registration, data security, data breach notification and the appointment of a data protection officer, vary widely and fromlaws in other regions of the world.

The growing number of data breaches in the region has resulted in legislative changes, such as in South Korea, to increase punitive and statutory damages for data breaches, and increased enforcement efforts, particularly against organizations that suffer repeated or massive breaches. For example, in April 2016, the Singapore DPA took enforcement actions against 11organizations for data protection violations involving data breaches and/or unauthorized disclosures of personal information.
In Australia, the Australian DPA entered into its first enforceable undertaking with Singtel Optus Pty Ltd., Australia's second-largest telecommunications

company, after it suffered three significant data security breaches (61 PRA, 3/31/15). After a massive data breach involving three major Korean credit card companies in January 2014, South Korea's Financial Supervisory Service (FSS) issued a three-month business suspension order against the credit card companies, and several employees of the companies are under investigation by the FSS (07 PRA, 1/10/14). The Financial Services Commission also ordered the companies to cover any financial losses suffered by their customers.

Data breaches have also resulted in increased civil litigation, particularly in Japan and South Korea. For example, in January 2015, a large multi-plaintiff litigation (involving 1,789 plaintiffs) was filed in court in connection with a data breach that affected 48.6 million customers of Benesse Holdings Inc., a Tokyo-based company that operates Shinkenzemi correspondence education courses for schoolchildren (21 PRA, 2/2/15). In addition, hundreds of civil actions are now pending for claims arising from the January 2014 credit card breach in South Korea.

Direct Marketing:

There has also been increased enforcement of direct marketing rules in Hong Kong. Since Hong Kong's new directing marketing provisions of Personal Data (Privacy) Ordinance (Ordinance) took effect in April 2013, the DPA has, as of January 2016, referred 53 cases for criminal investigation and prosecution. Four of these cases resulted in criminal convictions in 2015.

While the fines imposed in these four cases were relatively low compared to the maximum fines possible under the Ordinance (up to HK$500,000 ($64,343) and 3 years imprisonment), these cases demonstrated the DPA's determination to vigorously enforce the direct marketing rules.

New Privacy Legislation:

There have been significant changes to the legislative landscape in the region over the past year, particularly in Japan, South Korea and Taiwan. In September 2015, Japan enacted legislation to amend the country's Personal Information Protection Act (173 PRA, 9/8/15). Provisions of the amended law provide for the creation of the Personal Information Protection Commission (PIPC), an independent authority charged with overseeing data protection compliance, as well as other changes such as new rules for processing and handling anonymously processed information and cross boarder transfers of personal data.

South Korea also amended its Personal Information Protection Act in July 2015 and then again in March 2016 (131 PRA, 7/9/15) (58 PRA, 3/25/16). Among other things, the 2015 amendments strengthened remedies available to individuals in the event of a data breach by introducing punitive and statutory damages awards and added disgorgement of profits as an available criminal penalty. The March 2016 amendments impose new notice requirements on selected organizations that process large volumes of personal information received from sources other than the individual concerned (e.g., services involving Big Data, Internet of things).

Lastly, in December 2015, Taiwan enacted amendments to its Personal Data Protection Act (PDPA), which took effect on March 15, 2016, to address concerns about the rules for processing sensitive personal data and the notice requirements for processing personal data collected prior to the entry into force of the PDPA (01 PRA, 1/4/16).

Legislation Under Development:

New privacy laws are being debated in Thailand and Indonesia (146 PRA 146, 7/30/15). In January 2015, the Thai Cabinet announced that it had approved "in principle" a draft privacy bill that would impose basic data privacy obligations on organizations such as notice, consent, access, data retention and security (11 PRA, 1/16/15). Transfers to countries that do not provide adequate protection would be restricted. The Minister of Digital Economy and Society is the designated agency responsible for enforcement of the law. At present, there are no obligations in the bill that would require registration, the appointment of a DPO or data breach notification.

There have been significant changes to the legislative landscape in the region over the past year, particularly in Japan, South Korea and Taiwan.

In October 2015, the Indonesian government issued a draft data protection law, prepared by the Ministry of Communication and Informatics for the 2016 Priority National Legislative Program. Lastly, in December 2015, the Australian Government released an exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the Draft Bill) for public consultation (233 PRA, 12/4/15). The government's proposed breach notification bill follows on the heels of the enactment of a data retention law in March 2015 that requires telecommunications and Internet

service providers to collect and retain certain types of communications data for a period of two years. Australia has been discussing the possibility of enacting data breach notification rules since 2008 when the Australian Law Reform Commission first proposed mandatory notification rules; however, concerns about the increased potential for data breaches in light of these new data retention requirements appears to have prompted the government to act.

Under the Draft Bill, which is expected to be introduced into the legislature sometime in 2016, companies will be required to notify the Office of the Australian Information Commission (OAIC) and affected individuals of “serious data breaches.” Failure to comply with the notification obligation set forth in the Bill will be deemed to be an interference with the privacy of an individual for purposes of the Privacy Act, which may result in an investigation and enforcement action by the Privacy Commissioner, and is subject to civil penalties for serious or repeated interferences with privacy.

Country-by-Country Review of Differences

AUSTRALIA

Australia's Privacy Act 1988 (Cth) (Australian Law) has been amended twice since it was enacted, first in 2000 and most recently in 2012 (231 PRA, 12/3/12) (231 PRA, 12/3/12) . As part of the most recent changes to the law, a single set of privacy principles, referred to as the Australian Privacy Principles (APPs), covering both the public and private sectors was adopted. In addition, a comprehensive credit reporting system that provides for codes of practice under the APPs and a credit reporting code were implemented. The privacy commissioner was also given the authority to develop and register codes that are binding on specified agencies and organizations. The 2012 amendments also clarify the functions and powers of the commissioner and improve the commissioner's ability to resolve complaints; recognize and encourage the use of external dispute resolution services; conduct investigations; and promote compliance with privacy obligations. Two more rounds of amendments are expected; however, there is no time table for their development and enactment.

In Brief

Like most of the jurisdictions in the region, the Australian Law does not require the appointment of a DPO, registration and data security breach notification; however, the privacy commissioner recommends that organizations appoint a DPO and provide notice in the event of a data security breach. Under the amended law, there are more detailed rules on cross-border transfers, and the application of the law has been expanded to cover all organizations with “Australian links.” Lastly, the exemption for employee records remains intact.

Special Characteristics

Data Protection Authority

The Australian Law is administered by the privacy commissioner in the Office of the Australian Information Commissioner (DP A). The DPA has the power to conduct privacy compliance assessments of Australian government agencies and some private sector organizations, accept enforceable undertakings and seek civil penalties in the case of serious or repeated breaches of privacy. In May 2014, the Australian government announced plans to disband the Office of the Australian Information Commissioner (OAIC) for budgetary reasons by Jan. 1, 2015, but the position and responsibilities of the privacy commissioner would remain intact. However, the necessary legislation was not enacted by the end of 2014, so, for the moment, the OAIC remains operational.

Application of the Act

One of the significant changes to the Australian Law is the extension of the APPs to cover overseas handling of personal information by an organization if it has an “Australian link.” An organization has an Australian link if the organization is:

- an Australian citizen;
- a person whose continued presence in Australia is not subject to a limitation as to time imposed by law;
- a partnership formed in Australia or an external territory;
- a body corporate incorporated in Australia or an external territory; or
- an unincorporated association that has its central management and control in Australia or an external territory.

An organization that does not fall within one of the above categories will also have an Australian link where:

- the organization carries on business in Australia or an external territory; and
- the personal information was collected or held by the organization in Australia or an external territory, either before or at the time of the act or practice.

According to the DPA's guidelines, activities that may indicate that an entity with no physical presence in Australia carries on business in Australia include:

- the entity collects personal information from individuals who are physically in Australia;
- the entity has a website that offers goods or services to countries including Australia;
- the entity includes Australia as one of the countries on the drop-down menu of its website; or
- the entity is the registered proprietor of trademarks in Australia.

Where an entity merely has a website that can be accessed from Australia is generally not sufficient to establish that the website operator is “carrying on a business” in Australia.

Employee Records

The existing exemption for employee records covering “acts or practices in relation to employee records of an individual if the act or practice directly relates to a current or former employment relationship between the employer and the individual” remains intact; the intention is to revisit this issue in subsequent rounds.

Cross-Border Transfers

Before disclosing personal information to a recipient overseas, organizations must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information received, except where one of the following situations applies:

- the recipient is subject to a law or binding scheme that protects the information in a substantially similar manner, and there are mechanisms available to the individual to enforce that protection;
- the individual is expressly informed that, if he or she consents to the disclosure of the information, the organization is relieved of its obligation to take the required reasonable steps above to ensure that the overseas recipient does not breach the APPs, and, after being so informed, the individual consents to the disclosure;
- the disclosure of the information is required or authorized by or under an Australian law or a court/tribunal order; or
- there is an exception under the law that covers the disclosure of the information by the organization.

The cross-border rules apply to transfers by the organization to its overseas affiliates but not an overseas office.

Data Protection Officer

There is no obligation to appoint a DPO; however, there is a general obligation to implement appropriate practices, procedures and systems to comply with the APPs. The APP guidelines cite the example of designated privacy officers as a possible governance mechanism to ensure compliance with the APPs.

Data Security Breach Notification

There is no obligation under the Australian Law and the APPs to provide notice in the event of a data security breach; however, the DPA has issued voluntary breach notification guidance which recommends that notice be provided to the DPA and affected individuals where the breach creates a real risk of serious harm to individuals. As discussed above, the government has proposed mandatory breach notification legislation which is expected to be introduced into the legislature sometime in 2016.

HONG KONG

Hong Kong was the second jurisdiction in Asia to enact a comprehensive data protection law, in 1995. The Personal Data (Privacy) Ordinance (Hong Kong Law) protects all personal information of natural persons and applies to both the private and public sectors. The Hong Kong Law was amended in 2012, and one of the most significant changes was to more closely regulate the use and provision of personal information in direct marketing activities (128 PRA, 7/5/12). In addition, certain changes to the data protection principles were made, new offenses and penalties were introduced, the authority of the Office of the Privacy Commissioner for Personal Data (DPA) was enhanced and a new scheme whereby the DPA may provide legal assistance to individuals was introduced. The majority of the changes went into effect Oct. 1, 2012; the new direct marketing and the legal assistance provisions took effect April 1, 2013.

In Brief

The Hong Kong Law does not require the appointment of a DPO, data security breach notification or registration; however, the DPA does recommend that organizations appoint a DPO and provide notice in the event of a data security breach. The Hong Kong Law contains a provision that restricts cross-border transfers to countries that do not provide adequate protection; however, the provision is not in force.

Special Characteristics

Data Protection Authority

The Office of the Privacy Commissioner for Personal Data is responsible for enforcement.

Cross-Border Transfers

While the Hong Kong Law contains a provision (Section 33) that limits the transfer of personal information to a place outside Hong Kong that does not provide data protection similar to that under Hong Kong Law, it is not yet in force, and there is no schedule as to when it will come into force. Consequently, transfers both within and outside Hong Kong are governed by general legal restrictions on data collection and data use.

In December 2014, the DPA issued voluntary guidance to help organizations understand their compliance obligations under Section 33. The guidance contains a set of recommended model data transfer clauses for such transfers. The DPA has called upon the government to implement Section 33 and has also developed and submitted to the administration a white list of 50 jurisdictions that, in his view, provide similar protection. If and when Section 33 is implemented, the transfers to jurisdictions on the white list would be exempted from the requirements under Section 33.

Data Protection Officer

There is no statutory requirement to appoint a DPO. However, the DPA recommends it. Appointment of a DPO is a common business practice in Hong Kong.

Data Security Breach Notification

There is no legal obligation on any entities to give notice in the event of a data security breach under the Hong Kong Law; however, the DPA issued voluntary guidance which recommends that organizations “seriously consider” notifying individuals affected by a breach where there is a real risk of harm. Organizations may also choose to notify the privacy commissioner.

Marketing

One of the most significant changes was to more closely regulate the use and provision of personal information in direct marketing activities. Under the new direct marketing rules (seehere for guidance on the rules), an organization can only use or transfer personal information for direct marketing purposes if that organization has provided the required information (notice) and consent mechanism to the individual concerned and has obtained his or her consent. “Consent” in the direct marketing context includes an indication of no objection to the use (or provision); however, written consent is required prior to providing personal information to others for their direct marketing purposes. Failure to comply with these requirements is a criminal offense, punishable by fines of HK$500,000 ($64,343) and three years' imprisonment. In cases involving transfer of personal data for gain, a fine of HK$1 million ($128,686) and five years' imprisonment are possible.

INDIA

In 2011, India issued final regulations implementing parts of the Information Technology (Amendment) Act, 2008 dealing with protection of personal information (88 PRA, 5/6/11). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Indian Privacy Rules) prescribe how personal information may be collected and used by virtually all organizations in India, including personal information collected from individuals located outside of India.

In Brief.

The Indian Privacy Rules do not require the appointment of a DPO, data security breach notification or registration. There are limitations on cross-border transfers, but they apply only to sensitive personal information. Furthermore, as explained below, outsourcing providers are subject to a narrower set of obligations, the consent obligations only apply to sensitive information and sensitive information is very broadly defined.

Special Characteristics

Data Protection Authority

The Ministry of Communications & Information Technology is responsible for enforcement of the Indian Privacy Rules.

Application of the Rules

The Indian Privacy Rules raised significant issues and caused concern among organizations that outsource business functions to Indian service providers. As drafted, the Indian Privacy Rules apply to all organizations that collect and use personal information of natural persons in India, regardless of where the individuals reside or what role the company that is collecting the information plays in the process of handling the information. In particular, the provisions apply to a “body corporate,” which is defined as “any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities,” as well as, in many instances, “any person on its behalf.” As a result, industry both within and outside India expressed concern that the Indian Privacy Rules would decimate the outsourcing industry.

In response to these concerns, on Aug. 24, 2011, the Indian Ministry of Communication & Technology issued a clarification of the Indian Privacy Rules (Clarification), stating that the Indian Privacy Rules apply only to organizations in India (166 PRA, 8/26/11). Therefore, if an organization in India receives information as a result of a direct contractual relationship with an individual, all of the obligations under the Indian Privacy Rules continue to apply. However, if an organization in India receives information as a result of a contractual obligation with a legal entity (either inside or outside India), e.g., is acting as a service provider, the substantive obligations of notice, choice, data retention, purpose limitation, access and correction do not apply, but the security obligations and the obligations relating to the transfer of information do apply.

Consent

The consent rules apply only to sensitive information.

Sensitive Information

Sensitive information is very broadly defined and includes information that is not generally regarded as sensitive in other jurisdictions. In particular, it is defined as information relating to: (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise; provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Cross-Border Transfers

An organization may transfer sensitive personal information to any organization or person in India or to another country that ensures the same level of data protection; however, the government has not issued a list of countries that, in its view, provide such protection. The transfer may only be allowed if it is necessary for the performance of the contract between the organization (or its agent) and the individual or where the individual has consented to the transfer.

JAPAN

In September 2015, Japan enacted legislation to amend the country's 2005 Personal Information Protection Act which regulates the handling of personal information of natural persons by private sector organizations (Japanese Law). Provisions of the amended law that provide for the creation of the Personal Information Protection Commission (PIPC), an independent authority charged with overseeing data protection compliance, came into force on Jan. 1, 2016; the remaining provisions will take effect in August 2017. The creation of the PIPC represents a significant change in the approach to enforcement which, until now, has been the responsibility of national administrative agencies and local governments. As part of their supervision responsibilities, these agencies have issued to-date 39 data protection guidelines covering 27 different areas or sectors.

In Brief

After the amendments take effect in September 2017, the Japanese Law will impose restrictions on cross-border transfers; however, currently there are no such restrictions. There are special notice rules for sharing with third parties and, under some of the ministry guidelines, there are requirements to appoint a DPO and provide notice in the event of a data security breach. There are no registration requirements, however.

Special Characteristics

Data Protection Authority

Under the 2015 amendments, the Personal Information Protection Commission (DPA), an independent government authority, has been established to unify authority relating to data protection under a single governmental agency. Up until now, the data protection rules have been enforced and interpreted by the ministries responsible for enforcement in their individual sectors: the Ministry of Economy, Trade and Industry (METI); the Ministry of Internal Affairs and Communications (MIC) (formerly the Ministry of Public Management, Home Affairs, Posts and Telecommunication); the Ministry of Finance (FSA); the Ministry of Health, Labor and Welfare (MHLW); and the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) (a complete list of the guidelines and responsible ministries is available here.

Each ministry issued guidelines detailing specific obligations and recommendations. As a result, businesses operating in Japan have to carefully examine the guidelines issued by the competent ministries under whose jurisdiction they operate. A business may be subject to multiple guidelines depending on the scope of its business operations, and the provisions of such guidelines may not be the same. In fact, they may actually conflict. When the remaining provisions of the law come into force on Sept. 9, 2017, supervision of compliance with the law will transfer from the competent Ministers to the DPA.

Cross-Border Transfers

Prior to the 2015 amendments, the law did not impose limitations on cross-border transfers; however, the rules for disclosures to third parties did apply. These current rules require that personal information not be provided to third parties without prior consent of the individual unless an opt-out notice of third-party sharing has been provided prior to the personal information being collected. Once the amended rules take effect, individuals' consents will be required to transfer personal information to foreign third parties unless the DPA recognizes that the country has the same level of protection as the Japan Law or a foreign third party has a system that meets the DPA's specified standard.

Data Protection Officer

There is no requirement for a DPO under the Japanese Law; however, under some of the ministry guidelines, a DPO is required or recommended. In particular, a DPO is required in the financial and credit sectors and recommended in other sectors.

Data Security

Organizations must adopt measures necessary and appropriate for preventing the divulgence, loss or damage of personal information and otherwise control the security of that information. In addition, some of the guidelines impose more extensive security requirements, including encryption and service provider supervision. When the amendments take effect, organizations that create anonymized information will be required to sanitize the personal information in accordance with standards to be issued by the DPA.

Data Security Breach Notification

Data security breach notification is not explicitly addressed in the Japanese Law but is addressed in the ministry guidelines. Citing the Japanese Law's security control measures as the basis for their notification obligations, some of the ministry guidelines require or expect notification whenever there is a loss of personal information.

Joint Use Notice

If an organization intends to jointly use personal information with third parties (including corporate affiliates), it must provide information on the scope of joint users, items of personal information to be jointly used, purpose of joint use and the name of the individual or entity primarily responsible for the management of the data. The information must be provided through a notice to the individual or by placing the individual in circumstances whereby he or she can easily find out. Any change in purposes of joint use and/or the name of the individual or entity primarily responsible for the management of the data must also be notified to the individuals or publicly announced.

KAZAKHSTAN

The Law on Personal Data and Protection (Kazak Law), which went into effect in November 2013, protects all personal information of natural persons and applies to both the private and public sectors. The law was amended in November 2015 to impose new data localization requirements, effective January 2016.

In Brief

The Kazak Law restricts cross-border transfers to countries that do not protect personal information. It also imposes data localization requirements and exceedingly short timeframes for responding to access and correction requests. However, there are no data breach notification, special security, DPO, or registration requirements.

Special Characteristics

Data Protection Authority

There is no independent data protection authority responsible for enforcement of the Kazak Law. In practice, the General Prosecutor's Office and its territorial bodies are authorized to investigate and initiate administrative cases involving data protection law violations; the Ministry of Internal Affairs and the Ministry of Finance are responsible for investigating and initiating criminal cases involving data protection law violations.

Access and Correction

Access requests must be acted upon within three working days; correction requests must be acted upon within one day.

Cross-Border Transfers

Personal information may be transferred without restriction to a country that protects personal information. However, to transfer personal information to a country that does not provide such protection, consent or another one of the very limited exceptions must apply.

Data Localization

Effective Jan. 1, 2016, companies established in Kazakhstan as well as representative offices and branches of foreign companies that own or operate databases containing personal information must store personal information in Kazakhstan. It is unclear, however, if this storage requirement applies to foreign companies without any legal presence in Kazakhstan, whose operations are aimed at Kazakhstan and whose websites are accessible in the territory of Kazakhstan (e.g. Internet companies).

KYRGYZSTAN

The Law on Personal Data (Kyrgyz Law) (available in Russian here), which went into effect in April 2008, protects all personal information of natural persons and applies to both the private and public sectors.

In Brief

The Kyrgyz Law restricts cross border transfers, requires database registration (not yet in force), and imposes exceedingly short timeframes for responding to access and correction requests. In addition, similar to laws in the EU, the Kyrgyz Law requires organizations to have a legal basis for processing personal information such as consent, legitimate interests, vital interests, or legal requirements. However, the Kyrgyz Law does not impose data breach notification, special security, or DPO requirements.

Special Characteristics

Data Protection Authority

The Kyrgyz Law requires the government to designate a specific state body to regulate the collection and use of personal information, handle registrations, maintain records of personal data files and holders of such files, and make international agreements on the cross-border transfer of personal information. The State Registration Service, the public authority responsible for, among other things, implementing the country's informatization policy and supervising business activities and programs in this sector, has some but not all of the DPA functions set forth in the law. In particular, the State Registration Service has not been given authority over the registration process for personal data holders.

Access and Correction Requests

Access and correction requests must be fulfilled within seven days.

Cross-Border Transfers

Personal information may not be transferred to countries that do not provide an adequate level of protection unless one of the limited exceptions applies such as consent or vital interests.

Legal Basis for Collection and Use

Similar to EU law, the Kyrgyz Law requires organizations to have a legal basis for processing personal information such as: the individual has consented to the processing (consent); the processing is necessary to pursue a legitimate interest of the organization (legitimate interests), the processing is necessary to protect the vital interests of the individual (vital interests) or the processing is necessary to comply with a legal requirement (legal requirement).

Registration

Companies must register with their personal data files with the DPA; however, as of April 2016, the government has yet to designate a state authority responsible for registration.

MACAO

The Personal Data Protection Act (Macao Law), which took effect in 2006, was the first jurisdiction in Asia to adopt an EU-style data protection law. Virtually all of the provisions (notice, consent, collection and use, data security, data integrity, data retention, access and correction, cross-border limitations and registration) closely follow the requirements found in EU member state laws. The Macao Law applies to both the public and private sector processing of personal information of natural persons. Macao was the first jurisdiction in the region to require registration and impose EU-style cross-border restrictions.

In Brief

The Macao Law imposes restrictions on cross-border transfers that mirror EU member state cross-border border restrictions and requires registration of databases. It does not require the appointment of a DPO or data security breach notification.

Special Characteristics

Data Protection Authority

The Office for Personal Data Protection (DPA) is responsible for enforcement.

Registration

Registration is required unless an exemption applies.

MALAYSIA

The Personal Data Protection Act (Malaysian Law) was enacted in 2010 but did not come into effect until November 2013 (22 5 PRA, 11/21/13); organizations were given three months (until Feb. 15, 2014) to comply. The Malaysian Law protects all personal information of natural persons processed in respect to "commercial transactions" (explained below) that are (i) processed in Malaysia and (ii) processed outside Malaysia where the data are intended to be further processed in Malaysia. The Malaysian Law does not apply, however, to personal information processed by federal and state governments.

In Brief

The Malaysian Law restricts cross-border transfers and requires registration. It does not require the appointment of a DPO or data security breach notification.

Special Characteristics

Data Protection Authority

The Department of Personal Data Protection (DPA), located within the Ministry of Communication and Multimedia, is responsible for regulating and overseeing compliance with the Malaysian Law.

Application of the Law

A "commercial transaction" is defined as "any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a Credit Reporting Business carried out by a Credit Reporting Agency under the Credit Reporting Agencies Act 2009." Given this definition, there has been much speculation about whether this law would apply to the processing of human resources data. While no official guidance has been issued, all indications are that the Malaysian Law does apply to human resources data.

Cross-Border Transfers

Organizations may only transfer personal information to countries outside Malaysia that have been approved by the minister of communication and multimedia unless an exception applies. The exceptions largely mirror those found in many European laws, such as:

- the individual has consented to the transfer;
- the transfer is necessary to perform a contract with or at the request of an individual;
- the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
- the transfer is necessary in order to protect the vital interests of the individual; or
- the organization has taken all reasonable precautions and exercised all due diligence to ensure that the personal information will not be processed in any manner which, if the data were processed in Malaysia, would be a contravention of the act.

As of April 2016, no countries have been approved. Approved countries will be published by the minister in the official Gazette.

Registration

Data users (mainly licensed organizations) from the following sectors are required to register: communications, banking and financial institutions, insurance, health, tourism and hospitalities, transportation, education, direct selling, services (such as legal, audit, accountancy, engineering or architecture and retail or wholesale dealing as defined under the Control Supplies Act 1961), private employment agencies, real estate and utilities.

NEW ZEALAND

New Zealand was the first country in the region to enact a data protection law. The Privacy Act 1993 (New Zealand Law), which regulates the processing of all personal information of natural persons by both the public and private sectors, is also the first and only law in Asia to be recognized by the EU as providing an adequate level of protection for personal data transferred from the EU/European Economic Area . This adequacy determination was issued after New Zealand amended its law in 2010 to establish a mechanism for controlling the transfer of personal information outside of New Zealand in cases where the information has been routed through New Zealand to circumvent the privacy laws of the country from where the information originated (173 PRA, 9/9/10).

In Brief

The New Zealand Law requires the appointment of a DPO but does not restrict cross-border transfers or require registration. There are no mandatory requirements to provide notice in the event of a data security breach; however, such notice is recommended by the DPA.

Special Characteristics

Data Protection Authority

The Office of the Privacy Commissioner (DPA) regulates and administers the New Zealand Law.

Data Protection Officer

A DPO must be appointed regardless of the size of the agency. One DPO per agency is required.

Data Security Breach Notification

There are no mandatory notification obligations; however, the DPA has issued voluntary guidelines that recommend notice be provided to individuals and/or the DPA in the event of a security breach that presents a risk of harm to the individuals whose personal information is involved in the breach. Necessity to provide notice should be assessed on a case-by-case basis.

THE PHILIPPINES

Philippine President Benigno Aquino III signed the Data Privacy Act of 2012 (Philippine Law) into law Aug. 15, 2012 (164 PRA, 8/24/12). The law entered into force Sept. 8, 2012. Organizations have one year from when the implementing rules and regulations become effective (or another period determined by the DPA) to come into compliance with the law. Implementing regulations have yet to be issued; however, with the President's appointment of the three members of the National Privacy Commission in March 2016, the expectation is that the implementing rules and regulations will be issued soon.

In Brief

The Philippine Law imposes the same rules for both domestic and international (cross-border) transfers and requires the appointment of a DPO and data security breach notification. It does not require registration. In addition, the Philippine Law contains an exemption for outsourcing providers.

Special Characteristics

Data Protection Authority

The Philippine Law establishes the National Privacy Commission (the Commission) as a DPA located within the Department of Information and Communications Technology (DICT). The Commission, whose leadership was appointed by the President in March 2016, will be responsible for administering, implementing and monitoring compliance with the Philippine Act, as well as investigating and settling complaints. However, unlike many other data protection authorities, it will not have the power to directly impose penalties; it can only recommend prosecution and penalties to the Department of Justice.

Application of the Law

The Philippine Law applies to the processing of all personal information of individuals by public and private sector organizations with some important exceptions. For example, personal information that is collected from residents of foreign jurisdictions in accordance with the laws (e.g., data privacy laws) of those jurisdictions and that is being processed in the Philippines is excluded. This exception is relevant for companies that outsource their processing activities to the Philippines.

As a result, outsourcing providers in the Philippines will not need to comply with the Philippine Law's requirements for information collected as part of their outsourcing operations relating to personal information received from outside the Philippines.

In addition, the Philippine Law also applies to organizations and service providers that are not established in the Philippines but that use equipment located in the Philippines or maintain an office, branch or agency in the Philippines. It also applies to processing outside the Philippines if the processing relates to personal information about a Philippine citizen or a resident and the entity has links to the Philippines. This last provision seeking to extend the obligations of the law based on the citizenship of the individuals is very unusual in data protection laws.

Cross-Border Transfers/Transfers to Third Parties

Organizations are responsible for personal information under their control or custody, including information that has been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. Organizations are accountable for complying with the requirements of the Philippine Law and must use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party. This approach to domestic and international transfers is similar to the approaches found in Canadian and Japanese laws that are based on the concept of accountability.

Data Protection Officer

While registration is not required for private sector organizations, organizations must designate one or more individuals to be accountable for the organization's compliance with the Philippine Law.

Data Security Breach Notification

Organizations must promptly notify the Commission and affected individuals when sensitive personal information or other information that might lead to identity fraud has been, or is reasonably believed to have been, acquired by an unauthorized person, and the Commission or the organization believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected individual. Notification must describe the nature of the breach, the sensitive personal information believed to be involved and measures taken to address the breach. The Commission may exempt an organization from the requirement to provide notice to individuals if he or she decides that notification is not in the interest of the public or the affected individual.

SINGAPORE

Singapore's Personal Data Protection Act 2012 (Singapore Law) came into force in January 2013 (200 PRA, 10/17/12). The Singapore Law governs the collection, use and disclosure of personal information by private sector organizations. It also prohibits the sending of certain marketing messages to Singapore telephone numbers, including mobile, fixed-line, residential and business numbers registered with the Do Not Call (DNC) Registry. The Singapore Law was implemented in phases, with the DNC Registry provisions coming into force in January 2014 and the data protection rules coming into force in July 2014 (1 01 PRA, 5/27/14).

The following summarizes the special characteristics of data protection provisions only. It does not address the DNC Registry provisions contained in the Singapore Law.

In Brief

The Singapore Law restricts cross-border transfers and requires the appointment of a DPO. Data security breach notification and registration are not required. The Singapore Law provides special exemptions for outsourcing providers and the collection, use and disclosure of business contact information.

Special Characteristics

Data Protection Authority

The Personal Data Protection Commission is responsible for enforcement of the Singapore Law.

Application of the Law

The Singapore Law applies to all private sector organizations incorporated or having a physical presence in Singapore; however, service providers that process on behalf of other organizations are exempted from all but the security and data retention provisions. All personal information of natural persons is protected with some important exceptions. For example, business contact information—defined as an individual's name, position name or title, business telephone number, address, e-mail or fax number and other similar information—is exempted from the provisions pertaining to the collection, use and disclosure of personal information.

Cross-Border Transfers

Transferring organizations are required to take appropriate steps to determine whether, and ensure that, the recipient outside Singapore is bound by legally enforceable obligations to provide the transferred information with a comparable standard of protection. To satisfy these requirements, consent, a transfer contract, binding corporate rules or another exception under the Singapore Law must apply.

Data Breach Notification

There is no express obligation under the Singapore Law on any entities to give notice in the event of a data security breach. However, in May 2015, the DPA issued a Guide to Managing Data Breaches which recommends that individuals whose personal information has been compromised, be notified immediately if a data breach involves sensitive Personal Data. The DPA should be notified of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals.

Data Protection Officer

Organizations must designate one or more data protection officer(s) responsible for ensuring the organization's compliance with the Singapore Law.

SOUTH KOREA

The Data Protection Act (PIPA or Korean Law), which took effect in September 2011 and was subsequently amended in 2015, regulates public and private sector processing of personal information of natural persons. PIPA serves as the umbrella privacy law in South Korea; however, there are various sector-specific laws, such as the Act on the Promotion of IT Network Use and Information Protection (the Network Act), the Use and Protection of Credit Information Act, the Electronic Financial Transactions Act and the Use and Protection of Location Information Act, that also regulate privacy and cybersecurity. The Network Act, enacted before PIPA, regulates the processing of personal information in the context of services provided by telecommunications service providers and commercial website operators. While the privacy-related provisions are similar to PIPA, the Network Act regulates issues not covered by PIPA, such as spam.

In Brief

The Korean Law restricts cross-border transfers and requires the appointment of a DPO and data security breach notification. It also imposes extensive obligations in such areas as notice, consent and data security. Registration is not required, however.

Special Characteristics

Data Protection Authority

The Ministry of the Interior (MOI), formerly the Ministry of Government Administration and Home Affairs, is the authority responsible for enforcing the Korean Law.

Notice and Consent

Prior notice and express consent are required to collect, use and transfer personal information. The notice must separately detail the collection and use of personal information, third-party disclosures (including any cross-border disclosures), processing for promotional or marketing purposes, processing of sensitive information or particular identification data (such as resident registration number and passport number), disclosures to third-party outsourcing service providers and transfers in connection with a merger or acquisition. The individual must consent separately to each item. The uses that do not require consent must be distinguished from those that do require consent.

Cross-Border Transfers

If an organization intends to provide personal information to a third party across the national border, it must give notice and obtain specific consent to authorize the cross-border transfer.

Data Protection Officer

Organizations must appoint a DPO with specified responsibilities.

Data Security

The Korean Law and subsequent guidance issued by the regulatory authorities also impose significant data security obligations. These data security requirements are some of the most detailed in the world. For example, organizations are required to encrypt particular identification data, passwords and biometric data when such data are in transit or at rest. If personal information is no longer necessary after the retention period has expired or when the purposes of the processing have been accomplished, the organization must, without delay, destroy the personal information unless any other law or regulation requires otherwise. In addition, under the recent amendments, organizations that process “Particular Identification Information” (i.e., resident registration numbers, passport numbers, driver's license numbers, and alien registration numbers) will be subject to regular inspections by the Minister of the Interior (or a designated specialized agency) to determine whether they have implemented measures necessary to ensure the security of the Particular Identification Information.

Data Security Breach Notification

When becoming aware of a leak of personal information, organizations must, without delay, notify the relevant individuals, prepare measures to minimize possible damages and, when the volume of affected data meets or exceeds a threshold set by executive order (i.e., in the case of a leak involving 10,000 or more individuals), notify the regulatory authorities concerned or certain designated specialist institutions. Individuals who suffer damages resulting from a data breach caused by an organization's willful misconduct or gross negligence may be entitled to punitive damages of up to three times the actual damages. In addition, individuals whose personal information has been lost, stolen, or leaked due to a data breach caused by negligence or willful misconduct may request statutory damages of up to 3 million won ($2,520).

TAIWAN

Taiwan's Personal Data Protection Act (Taiwanese Law) entered into effect in October 2012 (169 PRA, 8/31/12). The Taiwanese Law, which replaces the 1995 Computer Processed Personal Data Protection Act that regulated computerized personal information in specific sectors such as the financial, telecommunications and insurance sectors, now provides protection to personal information of natural persons across all public and private entities and across all sectors. In December 2015, the Taiwanese Law was amended to address concerns about the rules for processing sensitive personal data and the notice requirements for processing personal data collected prior to the entry into force of the PDPA. Those amendments went into effect on March 15, 2016.

In Brief

The Taiwanese Law requires data security breach notification but does not restrict cross-border transfers or require the appointment of a DPO or registration of databases.

Special Characteristics

Data Protection Authority

The Ministry of Justice has overall responsibility for the Taiwanese Law; however, the individual government agencies that regulate specific industry sectors are authorized to regulate compliance by organizations under their regulatory jurisdiction.

Cross-Border Transfers

There are no restrictions imposed on cross-border transfers; however, the central competent authority for a specific industry may restrict cross-border transfers in certain circumstances, such as if the recipient country does not yet have proper laws and regulations to protect personal information so that the rights and interests of the individual may be damaged or personal information is indirectly transferred to a third country to evade the Taiwanese Law.

Data Security Breach Notification

Individuals must be notified when their personal information has been stolen, divulged or altered without authorization or infringed upon in any way.

Privacy Law Watch™

June 21, 2016

Western Hemisphere

Global Perspectives: Data Privacy Laws in the Western Hemisphere (Latin America, Caribbean and Canada)

Data Protection

Data Protection In this third article of a four-part series on the status of data protection laws around the world, the author explores developments in the Western Hemisphere (Latin America, the Caribbean and Canada), where 15 jurisdictions now have comprehensive data protection laws.

By Cynthia Rich

Cynthia Rich is a senior advisor at the Washington office of Morrison & Foerster LLP. As a member of the firm's international Privacy and Data Security Practice since 2001, Ms. Rich works with clients on legal issues relating to privacy around the world.

Introduction and Region at-a-Glance

Fifteen jurisdictions in the Western Hemisphere (Latin America, Caribbean and Canada) now have comprehensive privacy laws including: Antigua and Barbuda, Argentina, Aruba, Bahamas, Canada, Chile, Colombia, Costa Rica, Curacao, Dominican Republic, Mexico, Nicaragua, Peru, Trinidad and Tobago (currently, the only provisions in force pertain to the establishment of the data protection authority) and Uruguay. Saint Lucia adopted legislation in 2011, but the law hasn't yet gone into effect. The laws in Argentina (127 PRA, 7/2/03), Canada and Uruguay (172 PRA, 9/6/12) have been deemed by the European Commission to provide adequate protection.

Other countries such as Bermuda, Brazil (95 PRA, 5/17/16), Ecuador, Jamaica and Panama, and territories such as the Cayman Islands have draft bills that have either been or are expected to be introduced to their legislatures. In addition, Chile, which has had a high-level data protection law since 1999, may amend its existing law to include registration, impose cross-border restrictions and establish a data protection regulator (108 PRA, 6/6/16).

This article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments.

Common Elements Found in Latin American Laws

Notice:

All of the laws in this region include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, why it is collected and with whom it is shared.

Choice:

Every privacy law also includes some kind of choice element. The level or type of consent varies significantly from country to country. For example, Colombia has a much stronger emphasis on affirmative opt-in consent than Canada and Mexico, but all of the laws include choice as a crucial element in the law.

Security:

Furthermore, all of the laws require organizations that collect, use and disclose personal information to take reasonable precautions to protect that information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Some of the countries, such as Argentina and Mexico, have specified in greater detail how these obligations are to be met. The Argentina requirements are quite similar to Spain.

Access and Correction:

One of the core elements of every privacy law is the right of all individuals to access the information that organizations have collected about them and, where possible and appropriate, correct, update or suppress that information. Interestingly, compared to their European and Asian counterparts, most countries in the region require organizations to respond to access and correction requests in a much shorter period of time.

Data Integrity:

Organizations that collect personal information must also ensure that their records are accurate, complete and kept up-to-date for the purposes for which the information will be used.

Data Retention:

Generally, these laws require organizations to retain the personal information only for the period of time required to achieve the purpose of the processing. Some laws may mandate specific retention periods, while others set limits on how long data may be retained by an organization once the purpose of use has been achieved.

Differences in Approaches.

While core data protection principles and requirements are embodied in all of these laws, specific requirements, particularly with respect to cross-border transfers, registration, data security, data breach notification and the appointment of a data protection officer (DPO) vary widely from each other and from laws in other regions.

For example, two-thirds of the countries in this region restrict cross-border transfers of personal information to countries that do not provide adequate protection. However, unlike the European approach (and more like the approach in countries such as Kazakhstan, Singapore or South Korea), there is a heavy reliance on consent to legitimize transfers to inadequate countries. Some permit the use of contracts or internal rules in lieu of consent, and some require both. In almost all cases, the data protection authorities (DPAs) haven't specified what must be contained in these contracts or rules. Most of the laws in this region do permit companies to transfer data to another country if it is a contractual necessity. But transfers in most countries can't be legitimized based on the legitimate interests of the company (unlike in many European countries). From a practical point of view, most of the DPAs in the region have not issued lists of countries that they believe provide adequate protection, thus, companies are left to assume that all countries are deemed to be inadequate and must put in mechanisms (such as consent or contracts) to satisfy the rules.

Compared to their European and Asian counterparts, most countries in the region require organizations to respond to access and correction requests in a much shorter period of time.

The differences widen when comparing their respective rules on registration, data breach notification, security and DPO obligations: More than one-third of the countries require registration and notification in the event of a data breach and one-quarter require the appointment of a DPO. In addition, almost two-thirds of the laws in the region require that access and/or correction requests be responded to within 10 days (an exceedingly short time frame), and almost one-quarter protect personal information of both natural and legal persons.

Lastly, two of the countries, Nicaragua and Costa Rica, have unusual provisions. In Costa Rica, organizations that register databases with the DPA must provide the regulator with an access profile so that the DPA may access and consult the database, at any time and without restriction. In Nicaragua, the law provides for the right to be forgotten, a provision that is beginning to pop up with greater frequency in privacy litigation and proposed legislation.

A careful read of these laws is imperative, therefore. These differences pose challenges to organizations with respect to the adjustments that may be required to global and/or local privacy compliance practices as well as privacy staffing requirements. Compliance programs that comply with only European Union and Asian obligations will run afoul of many of the country obligations in this region.

A country-by-country summary of the obligations in these key areas is provided below. Other noteworthy characteristics are also highlighted and, where applicable, the responsible enforcement authority is identified. In addition, a chart is provided at the end to show at a glance the countries with mandatory cross-border, DPO, data security breach notification and registration obligations.

Trends

Enforcement

Violations of these laws can result in significant criminal and civil and/or administrative penalties being imposed; however, the level of enforcement by the authorities within the region has been relatively low, in part because it has taken time for some of the authorities to establish themselves. Of all of the authorities in the region, the DPA in Mexico has been the most active in issuing fines, some of which have been quite high. For example, in September 2015, the DPA announced its plans to impose three fines amounting to 32 million Pesos (approx. $2 million) on banking institution Grupo Financiero Banorte for, among other things, collecting sensitive personal information without obtaining the individual's express written consent, maintaining personal databases that contain present and future health data of persons without a legal justification to process this information, and failing to provide notice.

DPAs in Colombia and Peru are also starting to become more active, and there have been recent cases in which they have imposed large fines for privacy violations. For example, in September 2015, the Colombian DPA fined a shopping mall $22,503 for violating its notice obligations; in September 2014, it fined an umbilical cord stem cell bank $50,000 for privacy law violations involving the use of sensitive personal information for marketing purposes without the individual's consent. In 2014, the Peruvian DPA fined the Peruvian company datosperu.org approximately $78,600 for publishing sensitive personal information of two citizens on it Web page without their consent.

These differences in Western Hemisphere privacy laws pose challenges to organizations with respect to the adjustments that may be required to global and/or local privacy compliance practices as well as privacy staffing requirements.

The other country in the region that actively protects privacy rights is Brazil, despite the fact that it doesn't yet have in place a comprehensive privacy law. Private lawsuits and government enforcement actions are actively pursued whenever an individual's rights to privacy, as provided for under the Constitution, Civil Code, Consumer Protection Law and the recently enacted I nternet Bill of Rights (Internet Law), are perceived to have been violated (83 PRA, 4/30/14). In particular, the enactment of the Internet Law in April 2014 has sparked enforcement actions by the Consumer Protection Agency and the Public Attorney's Offices at the federal and state levels. The Internet Law prohibits Internet service providers, search engines, social media websites and online retailers who collect personal information from Brazilian consumers from sharing personal information as well as connection and application access logs with third parties, except with the user's express consent. In addition, there is a provision that allows the government to enforce against offshore businesses that collect, maintain or store data from Brazilian users.

In 2014, the Consumer Protection Agency fined the Brazilian telecommunications company Oi SA 3.5 million Reals ($1.2 million) for recording and selling subscriber browser data (146 PRA, 7/30/14). Oi partnered with a U.K.-based online advertising company Phorm to develop profiles of users' browsing practices, which were then sold to online advertising firms to generate customized advertisements.

Of all of the authorities in the region, the Data Protection Authorities in Mexico has been the most active in issuing fines, some of which have been quite high.

Privacy Legislation Under Development

Several jurisdictions in the region that do have laws in place are currently developing legislation. Three of these jurisdictions have held public consultations: Bermuda, Brazil and the Cayman Islands. During its public consultation in July 2015, the Bermuda government unveiled its draft model law which, in addition to the basic privacy law elements discussed above, would require organizations that transfer personal information to third parties to remain accountable for such transfers by ensuring that the third party

provides a comparable level of protection. The provisions resemble somewhat those found in the Australian law but with some additional flexibility.

The Brazilian Ministry of Justice held its public consultation in January 2015 (21 PRA, 2/2/16). If adopted, Brazil's proposed law would apply to the processing of personal information by public and private sector organizations, regardless of the country in which the organizations are headquartered and the country in which the databases are located, provided that the processing is carried out in Brazil or the personal information is collected within Brazil (e.g., the individual is located in Brazil at the time the data are collected).

The proposed scope of the law appears to cover outsourced data processing in Brazil and, as a result, may impose a complex and burdensome set of rules on such activities. Moreover, the proposed law would restrict cross-border transfers to countries that don't provide similar protection unless one of the limited exceptions applied or the individual specifically consented to the transfer after being given information on the international character of the operation and the risks involved in the transfer, based on the vulnerabilities specific to the destination country. The regulator would identify which countries don't provide similar protection. The draft law also would require the appointment of a DPO and the regulator to be notified about data breaches. Individuals would have to be given immediate notice of a data breach involving their personal information in cases where the incident jeopardized their personal safety or could cause them damage.

The Cayman Islands conducted its public consultation in late 2014. Its proposed law would establish a DPO, require registration and data breach notification and restrict cross-border transfers.

Elsewhere in the region, legislation is reportedly under development in Ecuador, El Salvador, Jamaica, and Panama. In Jamaica, the State Minister for Science, Technology, Energy and Mining announced in November 2015 that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of the 2016 legislative year.

Amendments to Existing Privacy Laws

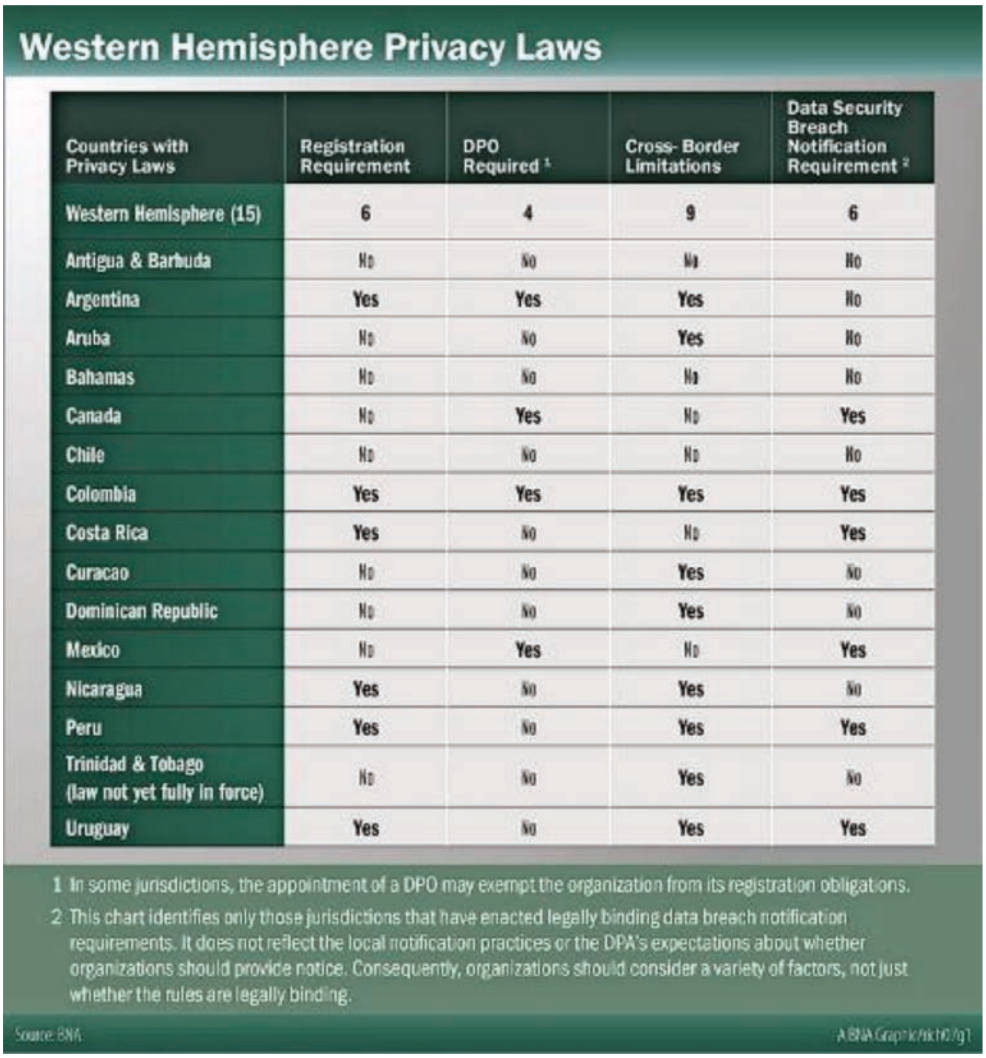
There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. Late in 2014, the government of Chile held a public consultation on its proposed legislation. The proposed legislation was submitted to Congress but no action has been taken yet. If adopted, the bill would, among other things, create a data protection authority, require registration of databases and impose restrictions on cross-border transfers.

In Costa Rica, amendments are under consideration to address concerns about certain provisions in the implementing regulations. In particular, the amendments seek to better define the transferring of personal data within companies belonging to the same economic group, as well as providing that not all transferring of data entails an economic profit for any of the parties. Furthermore, the proposed amendment seeks to remove the provisions regarding the Super User.

There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws.

Canada amended its data privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), with the enactment of the Digital Privacy Act in June 2015. Certain amendments took effect immediately such as the narrowing of the exceptions for business contact information, the addition of several new consent exceptions, including for disclosures to investigate law violations or carry out fraud detection and prevention. In addition, the Privacy Commissioner was given additional authority to enter into a compliance agreement with an organization if the Commissioner reasonably believes that the organization has committed, is about to commit or is likely to commit a breach of PIPEDA.

Lastly, in Mexico, there are plans to introduce a privacy bill in 2016 that combines regulation over the public and private sectors. According to an official at Mexico's data protection authority, the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI), the bill is expected to, among other things, provide for extra-territorial jurisdiction over companies that aren't located in Mexico but that handle data in Mexico, establish the right to data portability that will enable individuals to be able to migrate their data from the cloud, e-mails or social media activities from one company to the other, strengthen employee privacy rules (e.g., prohibit “excessive monitoring” of employees at or outside of work), specify data security measures for large and mid-size companies, require appointment of a DPO, and strengthen the INAI's enforcement authority.



Western Hemisphere Privacy Laws

Countries with Privacy Laws	Registration Requirement	DPO Required [1]	Cross- Border Limitations	Data Security Breach Notification Requirement [2]
Western Hemisphere (15)	6	4	9	6
Antigua & Barbuda	No	No	No	No
Argentina	Yes	Yes	Yes	No
Aruba	No	No	Yes	No
Bahamas	No	No	No	No
Canada	No	Yes	No	Yes
Chile	No	No	No	No
Colombia	Yes	Yes	Yes	Yes
Costa Rica	Yes	No	No	Yes
Curacao	No	No	Yes	No
Dominican Republic	No	No	Yes	No
Mexico	No	Yes	No	Yes
Nicaragua	Yes	No	Yes	No
Peru	Yes	No	Yes	Yes
Trinidad & Tobago (law not yet fully in force)	No	No	Yes	No
Uruguay	Yes	No	Yes	Yes

1 In some jurisdictions, the appointment of a DPO may exempt the organization from its registration obligations.

2 This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

Source: BNA

Country-by-Country Review of Differences

ANTIGUA AND BARBUDA

The Data Protection Act (Antigua and Barbuda Law), enacted in 2013, protects personal data processed by public and private sector organizations.

In Brief

The Antigua and Barbuda Law does not require database registration, impose mandatory DPO, data security breach, or detailed security obligations, or restrict cross-border transfers.

Special Characteristics

Data Protection Authority

The Information Commissioner pursuant to the Freedom of Information Act 2004 is responsible for enforcement of the Antigua and Barbuda Law. There is no website available for the Information Commissioner.

Consent

Consent is required to process personal data unless an exception applies (e.g., contractual necessity, legal obligation, or vital interests). Explicit consent is required to process sensitive personal data.

Definition of Personal Data

Personal data are defined as any information processed in the context of “commercial transactions”. Such commercial transactions, whether contractual or not, include any matters relating to the supply or exchange of goods or services, investments, financing, banking and insurance. Sensitive personal data are defined as any personal data relating to the physical or mental health or condition of an individual, sexual orientation, political opinions, religious beliefs, or commission of criminal offenses (proven or alleged).

ARGENTINA

The Personal Data Protection Act (Argentine Law (in Spanish)), enacted in 2000, protects all personal information of natural persons (living and deceased) and legal entities recorded in public or private data files, registers and data banks, established for the purpose of providing reports. Argentina was the first country, and currently only one of two countries in Latin America, to be recognized by the European Union as providing an adequate level of protection for personal information transferred from the EU/European Economic Area (127 PRA, 7/2/03).

In Brief

The Argentine Law restricts cross-border transfers to countries that don't provide adequate protection, requires registration and imposes detailed security requirements. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.

Special Characteristics

Data Protection Authority

The National Directorate for Personal Data Protection, located within the Justice and Human Rights Ministry, is responsible for enforcement of the Argentine Law.

Cross-Border Transfers

The transfer of personal information to countries outside Argentina that do not provide an adequate level of data protection is prohibited, unless the individual has provided his/her express consent to the transfer or another exception applies. However, the DPA hasn't officially recognized any jurisdiction as having an adequate or inadequate level of data protection.

Consent is not required to transfer to a service provider in an inadequate country, provided that there is an appropriate contract in place. The DPA has approved specific clauses for certain contracts, but it has done so on a case-by-case basis. Until recently, there were no models issued by the DPA. Now, however, the DPA has made available text clauses that it will use as a parameter for assessing international transfer agreements.

Data Security

After the Argentine Law was enacted, regulations imposing additional security requirements were issued. See Disposition 11/2006 (Security Measures), Sept. 20, 2006, available in English (unofficial translation), and in Spanish. The security measures are divided into three levels: basic or low level measures for all databases containing personal information; medium level measures for private companies acting as public utilities or public companies, and the owner of the database is bound by a duty of secrecy imposed by law (e.g., bank secrecy); and high level or critical level measures for all databases containing sensitive personal information.

Registration

Organizations must register their databases with the DPA. The registration covers the processing of all personal information for all purposes.

ARUBA

The Personal Data Protection Ordinance (Aruba Law), enacted in 2011, establishes rules for the protection of privacy in connection with the collection and disclosure of personal information of natural persons by both the public and private sectors. The Aruba Law applies to all files of data controllers established in Aruba, regardless of where such files are located (in or outside Aruba), provided that the files contain personal information of individuals settled in Aruba.

In Brief

The Aruba Law imposes restrictions on cross-border transfers but doesn't require database registration, the appointment of a DPO or data security breach notification.

Special Characteristics

Data Protection Authority

The Minister of Justice is responsible for enforcement of the law.

Cross-Border Transfers

The Aruba Law prohibits transfers of personal information into the files to which the law isn't applicable, to the extent that the Minister has declared that such transfers would result in a serious disadvantage for individuals' privacy. The Minister can issue a waiver for files located outside Aruba if the law of the country in which the file is located provides an equivalent level of privacy and data protection.

BAHAMAS

The Data Protection (Privacy of Personal Information) Act 2003 (Bahamas Law) protects the personal information of natural persons and applies to processing of such data by both the public and private sectors.

In Brief. The Bahamas Law does not require database registration, impose mandatory DPO and data security breach obligations or restrict cross-border transfers. However, with respect to the latter three areas, the DPA has issued nonbinding guidance. In addition, the Bahamas Law is unusual because there are no explicit notice and consent requirements.

Special Characteristics

Data Protection Authority

The Office of the Data Protection Commissioner is responsible for investigating any contraventions of the Bahamas Law, either of its own volition or as a result of a complaint by an individual concerned.

Notice and Consent

While there are no explicit notice and consent requirements set forth in the Bahamas Law, the DPA interprets the obligation to collect and process personal information fairly to mean that individuals must be made aware of certain information regarding the processing of their personal information and must consent to that processing, or one of the other conditions specified in the Bahamas Law must apply.

Cross-Border Transfers

The DPA has the authority to prohibit the transfer of information outside the Bahamas where there is a failure to provide protection either by contract or otherwise equivalent to that provided under the Bahamas Law. The DPA has issued nonbinding guidance listing the conditions, similar to those found in EU laws, which need to be met to transfer personal information cross-border.

Data Protection Officer

There is no obligation under the Bahamas Law to appoint a DPO; however, the DPA recommends it.

Data Security Breach Notification

There is no obligation on organizations to give notice in the event of a data security breach; however, there is voluntary DPA Guidance on Managing a Data Security Breach. The guidance states that organizations may choose to provide notice in the event of a breach of security resulting in unauthorized access to; alteration, disclosure or destruction; or accidental loss or destruction of personal information.

CHILE

Law No. 19.628 of Protection of Personal Data (Chilean Law), the first privacy law enacted in Latin America in 1999, regulates the processing of personal information of natural persons by both the public and private sectors.

In Brief

The Chilean Law doesn't restrict cross-border transfers or impose data security breach notification, DPO or registration requirements. Unlike most privacy laws, the Chilean Law doesn't establish a DPA to oversee enforcement; civil courts are responsible for enforcing the law.

CANADA

The Personal Information Protection and Electronic Documents Act regulates the collection, use, and disclosure of personal information of natural persons by private sector organizations for commercial purposes, with limited exceptions (e.g., where the organization is handling personal information in a province with substantially similar provincial legislation and the organization is provincially regulated).

In the context of an employment relationship, the collection, use and disclosure of employees' personal information by an employer is covered only where the employer is a private-sector Federal Work, Business or Undertaking, meaning a federally-regulated entity (e.g., organizations in the transportation, communications, broadcasting and banking sectors). Canada is regarded as providing an adequate level of protection for personal data transferred from the EU/EEA.

In Brief

The Canadian Law requires the appointment of a DPO and will require breach notification when the July 2015 amendments take effect. However, there are no cross border restrictions or special security or registration requirements.

Special Characteristics

Data Protection Authority

The Privacy Commissioner of Canada (DPA) is responsible for investigating complaints, conducting audits and pursuing court action under two federal laws. It also publicly reports on the personal information-handling practices of public and private sector organizations and promotes public awareness and understanding of privacy issues. The DPA doesn't have the authority to order compliance, award damages or levy penalties.

Cross-Border Transfers

There are no express limitations in the Canadian Law on cross-border transfers. In fact, the Canadian Law does not distinguish between domestic and international transfers of data. However, any organization that has transferred personal information to a third party (including an affiliate) for processing generally remains responsible for that personal information. The organization that transfers personal information to any foreign service provider must use contractual or other means to provide comparable level of protection while personal information is in possession of foreign entity.

Data Breach Notification

In June 2015, Parliament passed amendments to the Canadian Law requiring mandatory breach notification (120 PRA, 6/23/15), which will come into force on a future date as yet to be specified. Organizations will be required to report to the Commissioner and notify affected individuals of a breach where the breach poses a “real risk of significant harm” to affected individuals. Organizations must also notify government institutions and other organizations in prescribed circumstances, including where the organization believes that the government institution or other organization may be able to reduce or mitigate the risk of harm to affected individuals. Until these amendments come into force, there is currently no legal obligation to give notice in the event of a data security breach; however, the DPA has issued voluntary breach notification guidelines.

The Guidelines recommend that notice be given when there is unauthorized access to or collection, use or disclosure of personal information that creates a risk of harm to the individual, based on a case-by-case basis approach. The organization that has the direct relationship with the individual customer, client, or employee should notify the affected individuals, including when the breach occurs by a third party service provider, unless in the given circumstances direct notice by the third party service provider is more appropriate.

Data Protection Officer

Organizations must appoint an individual or individuals who are accountable for the organization's compliance with the Canadian Law. Although other individuals within the organization may be responsible for the day-to-day processing of personal information, accountability rests with the designated individual.

COLOMBIA

Enacted in October 2012, Law No. 1581 “Introducing General Provisions for Personal Data Protection” (Colombian Law) sets forth general rules for the protection of personal information of natural persons by both the public and private sectors, including special protections for children (205 PRA, 10/24/12). The Colombian Law is intended to complement a law enacted in 2008 that applies to personal credit information only. Organizations had six months (until April 17, 2013) to come into compliance with the Colombian Law.

In Brief

The Colombian Law imposes DPO, data security breach notification and registration requirements and restricts cross-border transfers to countries that don't provide adequate protection. In addition, some additional data security measures are required.

Special Characteristics

Data Protection Authority

The Personal Data Protection Division, the organization within the Superintendence of Industry and Commerce responsible for performing the functions of the DPA, is authorized to carry out investigations on the basis of complaints or on its own initiative.

Cross-Border Transfers

The transfer of personal information to countries outside Colombia that do nott provide an adequate level of data protection is prohibited, unless the individual has provided his/her express consent to the transfer, the transfer is necessary to execute a contract between the individual and the organization or another exception applies. The DPA may approve transfers to non-adequate countries that don't fall under one of the above-listed exceptions by issuing a conformity declaration (declaración de conformidad). The additional requirements and obligations that must be satisfied before the DPA may issue such declarations are expected to be addressed in the forthcoming implementing regulations.

Data Protection Officer

Every organization and service provider must appoint a person or department responsible for protecting personal information and processing requests from individuals who seek to exercise their rights under the law.

Data Security

The DPA is required to issue instructions related to the security measures for processing personal information. If an organization breaches its duties and obligations under the law and the DPA has to decide whether or not to impose penalties, it will take into account the extent to which the organization has in place the proper security policies and measures for the proper handling of the personal information.

Data Security Breach Notification

Both the organization and the service provider must inform the DPA about any violations of security codes and any risks in the administration of information of individuals. There is no obligation to give notice of such breaches directly to individuals.

Registration

Organizations and service providers that carry out processing of personal information in Colombia must register with the DPA. It is quite unusual to require service providers to file registrations with the DPA. The National Registry was officially launched in November 2015.

COSTA RICA

Law No. 8968 on the Protection of the Person Concerning the Treatment of Personal Data (Costa Rican Law) came into force Sept. 5, 2011 (183 PRA, 9/21/11). It applies to automatic and manual processing of personal information of natural persons by both public and private entities. Companies had until March 5, 2013 to bring their practices into compliance with the Costa Rican Law.

In Brief

The Costa Rican Law requires data security breach notification and registration. It also imposes special data security and "Super User" obligations but doesn't require the appointment of a DPO or restrict cross-border transfers. However, there are general rules that apply to all data transfers.

Special Characteristics

Data Protection Authority

Prodhab, established in March 2012, is responsible for creating a database registry, ensuring compliance with the Costa Rican Law and issuing implementing regulations.

Cross-Border Transfers

There are no limitations on cross-border transfers; however, the general rules for any transfer of databases and/or personal information apply. In particular, express written consent (or a contract) is required to share or transfer personal information. The Costa Rican Law does not include any other legal bases for transferring data, and this rule applies broadly to all transfers without explicit indication of whether the transfer occurs within or outside Costa Rica.

Data Security

In addition to the basic security obligations, the Costa Rican Law requires organizations to issue a "Performance Protocol" that will regulate all the measures and rules to be followed in the collection, management and handling of the personal information. In order to be considered valid, the Performance Protocol (and any subsequent amendments) must be registered with the DPA.

Data Security Breach Notification

Organizations must inform individuals about any irregularities in the processing or storage of their personal information, or when the organization becomes aware of such irregularities. Irregularities include but are not limited to loss, destruction and/or misuse that result from a security vulnerability or breach. They must inform individuals within five working days from the time the vulnerability occurs so the individuals may take appropriate action.

Registration

Every database that is established for distribution, promotion or commercialization purposes must be registered with the DPA. According to a FAQ posted on the DPA website, human resources databases that are used for the exclusive use of the company do not need to be registered.

'Super User'

The Costa Rican Law has a very unusual requirement not found in any other privacy law worldwide. Organizations that registered databases with the DPA must provide the regulator with an access profile so that the DPA may access and consult the database, at any time and without restriction. In FAQs issued by the DPA on its website, the DPA states that it will only access databases in response to a complaint or when there is evidence of possible law violations. It further states that the "Super User" provision should not be interpreted as providing the DPA with absolute power to access all information contained in these databases. In particular, the DPA does not have the ability to access databases containing information on banking

transactions, suppliers and corporate financial statements.

CURACAO

The Personal Data Protection Act (Curacao Law), which took effect Oct. 1, 2013, regulates the processing of personal information of natural persons by both the public and private sectors. The Curacao Law is modeled on the Dutch Data Protection Law.

In Brief

The Curacao Law restricts the cross-border transfer of personal information to countries that don't provide adequate protection. However, there are no DPO, data security breach notification and registration requirements. There is also no required time frame specified for responding to access or correction requests.

Special Characteristics

Data Protection Authority

The College Bescherming Persoonsgegevens supervises compliance with the Curacao Law.

Cross-Border Transfers

Personal information may only be transferred to a country outside the Kingdom of the Netherlands (Editor's note: the Kingdom of the Netherlands consists of the Netherlands, Aruba, Curacao and Sint Maarten) if that country ensures an adequate level of protection. Where there is no adequate level of protection, the data transfer may take place provided that:

- the individual has provided his/her explicit consent;
- the transfer is necessary for the performance of a contract between the individual and the data controller or for actions to be carried out at the request of the individuals and which are necessary for the conclusion of a contract;
- the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the data controllers and third parties in the interests of the individuals;
- the transfer is necessary on account of an important public interest, or for the establishment, exercise or defense in law of any right;
- the transfer is necessary to protect the vital interests of individuals;
- the transfer is carried out from a public register set up by law or from a register that can be consulted by anyone or by any persons who can invoke a legitimate interest, provided that in the case concerned the legal requirements for consultation are met; and
- the transfer has been approved by the DPA.

DOMINICAN REPUBLIC

The Organic Law 172-13] on the Protection of Personal Data (Dominican Law), which took effect Dec. 13, 2013, is the most recent law enacted in the region. The Dominican Law protects personal information filed in public or private archives, public records and data banks intended to provide reports. The Dominican Law also regulates credit information companies, the provision of credit reference services and the supply of information on the market to ensure respect for privacy and the rights of the information owners.

In Brief

In contrast to the cross-border rules found in other countries in the region, the Dominican Law imposes a common set of legal bases for all international transfers, regardless of their destination. Registration/supervision requirements apply only to public or private data banks that are intended to provide credit reports. Such data banks are subject to the inspection and supervision of the Superintendence of Banks. There is also no obligation to appoint a DPO or to notify individuals or the regulator in the event of a data security breach. The Dominican Law does not establish a DPA to oversee compliance;

however, the Superintendence of Banks is the entity authorized to regulate credit information companies.

Special Characteristics

Cross-Border Transfer

Personal information may only be transferred internationally in certain circumstances such as:

- the individual consents to authorize the transfer of information or when the laws so allow;
- the transfer is necessary for the execution of a contract between the individual and the organization, or for the execution of pre-contractual measures;
- the transfer concerns bank or security transfers with regard to the respective transactions and in accordance with the applicable legislation;
- the transfer has been agreed or considered in the framework of international treaties or conventions, or in free-trade treaties of which the Dominican Republic is a part; or
- the transfer of legally required information is to safeguard public interest or for the acknowledgement, exercise or defense of a right in a judicial process, or is required by a tax or customs administration to fulfill its duties.

MEXICO

The Federal Law on Protection of Personal Data Held by Private Parties, enacted in 2010, regulates the processing of personal information of natural persons by private sector organizations but doesn't apply to duly licensed credit reporting companies (128 PRA, 7/7/10).

In Brief

The data protection rules in the Mexican Law have a number of important differences from those found elsewhere in the region. For example, the notice and data security obligations are subject to detailed rules. Unlike many laws in the region, the Mexican Law does not require registration, but it does require the appointment of a DPO and data security breach notification. In addition, domestic and international transfers are largely subject to the same requirements.

Special Characteristics

Data Protection Authority

The Federal Institute for Access to Information and Data Protection (IFAI) is responsible for disseminating information on data protection and compliance with the Mexican Law.

Notice

In 2013, the DPA issued Guidelines that provide for three different types of privacy notices: comprehensive, simplified and short. A comprehensive privacy notice must always be made available; however, depending on the circumstances of the data collection, a simplified or short privacy notice may be provided first. The Guidelines state expressly that provision of a simplified or short privacy notice doesn't relieve the organization of its obligation to make available a comprehensive privacy notice.

Simplified or Short Privacy Notice. Where personal information is obtained directly from the individual by any electronic, optical, audio or visual means, or through any other technology, the organization must immediately provide the individual with at least the information regarding the identity and domicile of the organization and the purposes of the data processing, as well as provide the mechanisms for the individual to obtain the full text of the privacy notice. Where cookies, Web beacons or similar technologies are used, a communication or warning must be placed in a conspicuous place to inform the individual about the use of these technologies and how the technologies can be disabled by the individual.

Data Protection Officer or Office

The Mexican Law requires any entity that collects personal information to appoint a DPO or office to promote the protection of

personal information within its organization and process requests (such as access and correction requests) received from individuals who wish to exercise their rights under the Mexican Law.

Data Security

The Regulations, issued in 2011 (249 PRA, 12/29/11), define what constitutes physical, technical and administrative measures and, in particular, require: the establishment of an internal supervision and monitoring system; implementation of a training program for personnel to educate and generate awareness about their obligations to protect personal information; and external inspections or audits to check compliance with privacy policies. The list of security measures must be updated when security improvements or changes are made or there are breaches of the systems. In addition, the organization is encouraged to consider undertaking a risk analysis of personal information to identify dangers and estimate the risks for the personal information, conduct a gap analysis and prepare a work plan to implement the missing security measures arising from the gap analysis.

Whenever there is a security violation involving personal information, the DPA may take into account the organization's compliance with DPA recommendations to determine the attenuation of the corresponding sanction.

Data Security Breach Notification

Security breaches that occur “at any stage of processing that materially affect the property or moral rights” of the individual must be reported to the individual by the organization so the individual can take appropriate action to protect his or her rights. The Mexican Law does not require notice to any public authority or regulator.

NICARAGUA

Nicaragua enacted the Law on Personal Data Protection March 21, 2012 (Act No. 787) and the Regulation of the Law on Personal Data Protection (Decree No. 36-2012) (Nicaraguan Law) Oct. 17, 2012. The Nicaraguan Law protects the personal information of natural and legal persons in private and public databases.

In Brief

The Nicaraguan Law restricts cross-border transfers and requires registration; however, the registration procedure is not yet established. Data security, breach notification and the appointment of a DPO are not required. Unlike other laws in the region, the Nicaraguan Law has a provision of the right to “digital oblivion.”

Special Characteristics

Data Protection Authority

The Nicaraguan Law calls for the creation of a Directorate for Personal Data Protection within the Ministry of Finance that will be responsible for the regulation, supervision and protection of the processing of personal information; however, as of March 2015, the Directorate has not yet been established. The Directorate will be responsible for a wide range of data protection-related activities, including issuing regulations, monitoring compliance and imposing administration sanctions in the event of violations.

Cross-Border Transfers

The assignment and transfer of personal information to countries or international organizations that do not provide adequate security and protection for personal information are prohibited except in very limited circumstances, such as where:

- the transfer is for the purposes of international judicial cooperation;
- the exchange of personal information is for health matters;
- the transfer is necessary to carry out epidemiological investigations, wire transfers or exchanges;
- the transfer is required by law;
- the transfer is agreed upon under any international treaties ratified by Nicaragua; or

• the transfer pertains to international cooperation with intelligence agencies or to criminal matters covered by specified laws.

Such transfers must be carried out at the request of a legally authorized person; the request must state the object and purpose of the intended processing; the organization must comply with the data security and confidentiality measures and verify that the receiving organization complies equally with these measures; and the individual must be informed about and consent to the transfer by the organization and the intended purposes of the processing.

Right to Digital Oblivion

The Nicaraguan Law is one of the first laws to include the right to be forgotten, which has been so controversial in the EU. In particular, the individual has the right to request that social networks, browsers and servers suppress or cancel his or her personal information contained in their databases. In the case of databases of public and private institutions that offer goods and services and collect personal information for contractual reasons, individuals may request that their personal information be canceled once the contractual relationship ends. This provision isn't particularly detailed, and it is not clear how organizations will implement these obligations.

PERU

The Law for Personal Data Protection (Peruvian Law), which protects the personal information of natural persons processed by public and private sector organizations, entered into force July 4, 2011; however, many of the provisions and its Regulations did not become effective until May 2013 (57 PRA, 3/25/13). Organizations had until March 2015 to conform their existing personal data banks to the Peruvian Law.

In Brief

The Peruvian Law requires registration and restricts cross-border transfers. The DPA has also established data security breach notification requirements. There is no obligation to appoint a DPO.

Special Characteristics

Data Protection Authority

The Peruvian Law established the National Authority for Protection of Personal Data to oversee compliance and, in particular, administer and keep up-to-date the National Register of Personal Data Protection, hear and investigate complaints lodged by individuals, issue provisional and/or corrective measures and impose administrative sanctions in cases of violations.

Cross-Border Transfers

Cross-border transfers of personal information are allowed if the recipient has adequate data protection as may be determined by the DPA. Thus far, the DPA hasn't issued a list of adequate recipients. The Peruvian Law provides certain exceptions to this provision, including where the transfer of personal information is necessary to complete a contract to which the individual whose information is being transferred is a party; where the individual has given consent; or where otherwise established by regulation issued under the Peruvian Law.

The Regulations additionally provide that cross-border transfers are permitted when the importer assumes the same obligations as the exporting organization. The exporter may transfer personal information on the basis of contractual clauses or other legal instruments that prescribe at least the same obligations to which the exporter is subject as well as the conditions under which the individual consented to the processing of his or her personal information. Therefore, if a contract is in place, consent or one of the other legal bases listed above would not be required.

Authorization for cross-border transfers is not required; however, the organization and the service provider may request the opinion of the DPA as to whether the proposed transfer of personal information cross-border meets the provisions of the Peruvian Law.

Data Security Breach Notification

The Peruvian Law itself doesn't impose data security breach notification requirements; however, it authorizes the DPA to establish the security requirements and conditions to be met by data controllers. In October 2013, the DPA issued an Informat ion Security Directive that instructs data controllers to notify individuals of “any incidents that significantly affect their proprietary or moral rights.”

Registration

All organizations must register with the DPA. In addition, organizations that voluntarily adopt codes of conduct to govern their transfers to affiliated entities must register them with the DPA.

URUGUAY

Law No. 18.331 on the Protection of Personal Data and Habeas Data Action (Uruguayan Law), enacted in 2008 and amended in 2010, regulates the processing of personal information of natural and legal persons by both the public and private sectors (166 PRA, 8/30/10). Uruguay was the second country in South America to be recognized by the EU as providing an adequate level of protection for personal information transferred from the EU/EEA (172 PRA, 9/6/12).

In Brief

The Uruguayan Law requires data security breach notification and registration and restricts cross-border transfers to countries that do not provide adequate protection. There is no requirement to appoint a DPO; however, the person responsible for the database is liable for violations of the provisions of the law, and his or her name will be identified in the registration.

Special Characteristics

Data Protection Authority

The Regulatory and Control Unit for the Protection of Personal Data was created as an entity decentralized from the Agency for the Development of Government of Electronic Management and Information Society and Knowledge (AGESIC).

Cross-Border Transfers

The transfer of personal information of any kind to countries or international organizations that fail to provide adequate levels of protection according to the standards of regional or international law in this area is prohibited except where the following cases apply:

- international judicial cooperation, according to the relevant international instrument, whether treaty or convention, subject to the circumstances of each case;
- exchange of medical data, when necessary for the treatment of the sick person and due to reasons of public health or hygiene;
- bank or stock exchange transfers, in regard to the corresponding transactions and pursuant to the applicable legislation;
- agreements within the framework of international treaties to which the Republic of Uruguay is a party; and
- international cooperation between intelligence agencies fighting against organized crime, terrorism and drug trafficking.

It also is possible to make international transfers of data in the following cases:

- the interested party has given his or her consent to the proposed transfer;
- the transfer is necessary for the execution of a contract between the interested party and the person responsible for the processing or to implement pre-contractual measures taken at the interested party's request;
- the transfer is necessary to execute an agreement entered into now or hereafter on behalf of the interested party, between the person responsible for the processing and a third party;
- the transfer is necessary or legally required to safeguard an important public interest, or for the recognition, exercise or defense of a right in a legal procedure;

- the transfer is necessary for safeguarding the vital interests of the interested party; or

- the transfer is effected from a record which, by virtue of legal or regulatory provisions, is designed to provide information to the public and is open to consultation by the general public or any person who can prove a legitimate interest, provided that the conditions established by law for consultation are met in each particular case.

Regardless of the cases listed above, the DPA may authorize a transfer or a series of transfers of personal information to a third country that does not guarantee an adequate level of protection when the person responsible for the processing offers sufficient guarantees regarding the protection of privacy, fundamental rights and freedoms of individuals as well as to the exercise of the corresponding rights.

Such guarantees may arise from appropriate contractual clauses.

Data Security Breach Notification

When the data controller or the data processor realizes that there has been a data security breach that could affect the individual's rights in a significant way, the data controller or the data processor must inform the individual.

Registration

All organizations that create, modify or eliminate databases of personal information must register their databases.

Privacy Law Watch™

June 24, 2016

Data Protection

Privacy Laws in Africa and the Near East

Legislation

In the fourth and final article of a series on the status of data protection laws around the world, the author explores developments in Africa and the Near East, where 18 jurisdictions have comprehensive privacy laws.

By Cynthia Rich

Cynthia Rich is a senior advisor at the Washington office of Morrison & Foerster LLP. As a member of the firm's international Privacy and Data Security Practice since 2001. Rich works with clients on legal issues relating to privacy around the world.

Introduction/Region at-a-Glance

The privacy landscape in Africa and the Near East has changed remarkably in the past few years. Eighteen countries have enacted comprehensive privacy laws: Angola, Benin, Burkina Faso, Cape Verde, Cote D'Ivoire—also known as the Ivory Coast—Gabon, Ghana, Israel, Madagascar, Mali, Mauritius, Morocco, Qatar/Qatar Financial Centre, Senegal, Seychelles, South Africa, Tunisia and the United Arab Emirates/Dubai International Financial Centre. All but the South African law, which has not yet entered into force, are in effect. With the adoption in June 2014 of the African Union (AU) Convention on cybersecurity and data protection, more countries in the region are likely to enact their own comprehensive privacy laws regulating the collection and use of personal information by the private sector. In fact, there are indications that countries such as Kenya, Tanzania, Uganda, and Zimbabwe in Africa and Qatar and Saudi Arabia in the Near East may be close to adopting legislation.

Several of the existing regimes in the region are still in their formative stages, in large part because the regulators are either not yet in place or have been recently appointed; however, in some of the countries with the more established privacy regimes, the regulators have been stepping up their enforcement efforts.

This article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments.

Common Elements Found in African/Near Eastern Laws

Notice:

All of the laws in Africa and the Near East include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, why it is collected and with whom it is shared.

Choice:

Unlike countries in Asia and Latin America, not all of the laws in this region include some kind of choice element. For example, the Mali law only states that notice must be provided; there are no explicit rules regarding consent, but there is a right to

oppose processing. In Benin, consent is not required to process non-sensitive data, but express consent is required for sensitive personal information. All of the other countries require consent in some form to process personal information, unless an exception applies. The level or type of consent varies, particularly depending on whether non-sensitive or sensitive information is being processed.

Security:

Furthermore, all of the laws require organizations that collect, use and disclose personal information to take reasonable precautions to protect that information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Some of the countries, such as Cote D'Ivoire, have specified in greater detail how these obligations are to be met.

Access & Correction:

One of the core elements of every privacy law is the right of all individuals to access the information that organizations have collected about them and where possible and appropriate, correct, update or suppress that information. Unlike their Latin American and Asian counterparts which require organizations to respond to access and correction requests within specified periods of time, most countries in Africa and the Near East do not prescribe a specific timetable for responding to such requests. Those that do, such as Ghana and Mauritius, have more reasonable timetables than as those typically found in Asia.

Data Integrity:

Organizations that collect personal information must also ensure that their records are accurate, complete and kept up-to-date for the purposes for which the information will be used.

Data Retention:

Generally these laws require organizations to retain the personal information only for the period of time required to achieve the purpose of the processing. In most cases, specific retention periods of time are not prescribed in the laws in this region.

Unlike countries in other regions which require organizations to respond to access and correction requests within specified periods of time, most countries in Africa and the Near East do not prescribe a specific timetable for responding to such requests.

Differences in Approaches

While most of the core data protection principles and requirements are embodied in these laws, specific requirements, particularly with respect to registration, cross-border transfers, data security, data breach notification and the appointment of a data protection officer (DPO) vary widely from each other and from laws in other regions of the world.

For example, all of the countries in the region require registration of processing, and all but one country restrict cross-border transfers; however, the reality is that there are 18 different registration and 17 different cross-border rules and procedures. Generally a contract, consent (or another legal basis) and/or data protection authority (DPA) authorization are required to transfer to countries that do not provide adequate protection. In almost all cases, the DPAs have not specified what must be contained in these contracts or rules. Most of the DPAs in the region also have not issued lists of countries that they believe provide adequate protection, and thus companies are left to assume that all countries are deemed to be inadequate and must put in place mechanisms (such as consent or contracts) to satisfy the rules.

The differences widen when comparing their respective rules on data breach notification, security and DPO obligations: One quarter require the appointment of a DPO; one quarter impose detailed security obligations for all processing while another quarter of the group impose special security rules for processing sensitive information only; and only 3 of the 18 require notification in the event of a data breach.

Sorting through these differences raises questions about the adjustments that may be required to global and/or local privacy compliance practices as well as privacy staffing requirements. Compliance programs that comply with only EU, Asian and/or Latin American obligations will run afoul of many of the African and Near Eastern country obligations. The slow pace at which several of these countries are proceeding to establish DPAs and issue implementing regulations makes the process all the more challenging.

A country-by-country summary of the obligations in these key areas is provided below. Other noteworthy characteristics are

also highlighted and, where applicable, the responsible enforcement authority is identified. In addition, a chart is provided at the end to show at a glance the countries with mandatory cross-border, DPO, data security breach notification and registration obligations.

Trends

Enforcement:

The most mature regimes in the region, such as Israel and Mauritius, have the most active enforcement. For example, over the past few years, the Israeli DPA has imposed fines for law violations. For example, in 2015, the Israeli DPA reported nine cases of law violations that resulted in the imposition of administrative fines (the amounts of the fines were not disclosed). The violations pertained to the failure to comply with the requirement to employ adequate data security measures, limit the use of database information for purposes other than those for which the database was established and holding more than five databases without applicable notification.

For many of the other countries in the region, there have been very few reports of enforcement actions or initiatives; however, in some countries such as Morocco, Senegal, Tunisia and UAE, there are recent indications that the regulators are stepping up their enforcement activities. In particular, the DPA in Morocco conducted in 2015 a “privacy sweep” of websites and apps used by children in coordination with the Global Privacy Enforcement Network (GPEN) to assess privacy concerns about the type of personal information collected by these online services.

In Senegal, the DPA issued warnings, one to a mobile content provider for failing to provide an unsubscribe mechanism for unsolicited SMS and e-mails and one to an online food service for repeated, illegal direct marketing activities, as well as a Formal Notice against an oil company in connection with its use of monitoring software in the workplace. The DPA ordered the oil company to uninstall the monitoring software on all work stations, delete all data collected using the software, and register its processing with the DPA within one month. In Tunisia, the DPA announced in January 2016 that it would be filing lawsuits against 12 public and private organizations for privacy law violations. Lastly, in the United Arab Emirates, the DPA for the Dubai International Financial Centre issued 11 monetary fines to organization in 2013 and 14 in 2014 for their failure to renew their registrations. The fine for failing to register is $25,000 and $5,000 for failing to notify the DPA of any amendments in personal data operations.

In some of the countries such as Angola, Cape Verde, Ghana, Madagascar, Mali and South Africa there has been no enforcement because the regulator either has not been appointed yet or is focused on implementing the law and/or raising public awareness about the law. For example, the DPA in Ghana, which became operational in late 2014, just launched its registration process in May 2016. Prior to that, the DPA, which remains without staff other than the Commissioner, had been focused on educating individuals and organizations about their respective legal rights and responsibilities. In Cape Verde, the DPA Commissioners were just appointed in April 2016 and in South Africa, the regulator has not been appointed yet, delaying the entry into force of the law. However, in April 2016, the South African Parliament reportedly developed a short list of candidates for the position so it is possible that the regulator will be established in 2016.

The most mature regimes in the region, such as Israel and Mauritius, have the most active enforcement.

Privacy Legislation Under Development:

Several countries such as Kenya, Tanzania, Uganda and Zimbabwe in Africa and Qatar and Saudi Arabia in the Near East may be close to adopting legislation. For example, in late April 2016, the Ugandan government introduced its Data Protection and Privacy Bill in Parliament, after conducting a public consultation in late 2014. If enacted, the Bill would regulate the collection, processing, use and disclosure of personal information by imposing obligations on data collectors, data processors and data controllers. The requirements include obtaining consent prior to processing unless an exception applies such a contractual necessity, legal obligation or medical purposes. There are also rules on the use of sensitive information, cross-border transfers, data breach notification and database registration.

Legislation is also under consideration in Kenya's Parliament. Kenya's Data Protection Bill, which was approved by the government's cabinet in September 2014, covers both the public and private sectors and sets forth basic privacy principles. Obligations include notice, consent, data retention, data integrity, security and access and correction rights but there are no registration or data breach notification requirements. Tanzania is also reportedly working on data protection legislation; however, no draft texts have been made public.

In the Near East, legislation is pending before the legislatures in Saudi Arabia and, most recently, Qatar. The Qatari Cabinet announced in January 2016 that it approved a draft privacy law and has referred it to its legislative body for review and

adoption. Finally, Tunisia may be revising its law in the near future to comply with Convention 108 of the Council of Europe.

AU Convention:

The adoption in June 2014 of the African Union (AU) Convention on cybersecurity and data protection (AU Convention) is likely to encourage more countries in the region to enact their own comprehensive privacy laws. Although the AU Convention does not take effect until it has been ratified by 15 of the 54 member states, it does provide a comprehensive model legislative framework upon which countries can base their national laws (20 PRA, 1/30/15). The legislative framework mirrors the European approach and requires, among other things, consent or another legal basis to legitimize the processing of personal information. The processing of sensitive personal information is prohibited unless the individual consents in writing or another exception applies. Moreover, the processing of certain types of sensitive information, such as genetic information, biometric data and criminal records, would require special authorization. The framework also provides for the establishment of independent authorities at the national level with the power to conduct audits, impose administrative and monetary sanctions and authorize cross-border transfers. Organizations must register their processing with these national authorities.

Once the AU Convention is ratified by 15 member states, it will enter into force 30 days later. However, member states may ratify the document with reservations. While it will likely be a few years before the Convention is ratified, it may spur more countries in the region to begin work on developing privacy laws modeled after the AU Convention.

Africa and Near East Privacy Laws

Countries with Privacy Laws	Registration Requirement	DPO Required [1]	Cross-Border Limitations	Data Security Breach Notification Requirement [2]
Africa/Middle East (18)	18	5	17	3
Angola	Yes	No	Yes	No
Benin	Yes	No	Yes	No
Burkina Faso	Yes	No	Yes	No
Cape Verde	Yes	No	Yes	No
Cote D'Ivoire	Yes	Yes	Yes	No
Gabon	Yes	No	Yes	No
Ghana	Yes	No	No	Yes
Israel	Yes	Yes	Yes	No
Madagascar	Yes	Yes	Yes	No
Mali	Yes	No	Yes	No
Mauritius	Yes	No	Yes	No
Morocco	Yes	No	Yes	No
Qatar/QFC	Yes	No	Yes	No
Senegal	Yes	No	Yes	No
Seychelles	Yes	No	Yes	No
South Africa[3]	Yes	Yes	Yes	Yes
Tunisia	Yes	Yes	Yes	No
United Arab Emirates/DIFC	Yes	No	Yes	Yes

1. In some jurisdictions, the appointment of a DPO may exempt the organization from its registration obligations.
2. This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.
3. South Africa's Protection of Personal Information Act, 2013 was signed into law by the president in November 2013; however, the law does not take effect until the president proclaims a commencement date. It is unknown when the president will set a commencement date.

Source: BNA

BNA Graphics/Privacy Law Watch

Country-by-Country Review of Differences

ANGOLA

The Personal Data Law, Law no. 22/11 (Angolan Law), which became effective in June 2011, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

The Angolan Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration and imposes some additional security requirements. However, there is no obligation to appoint a DPO or give notice in the event of a data security breach. There are, however, breach notification obligations under an electronic communications law as discussed below.

Special Characteristics

Data Protection Authority

The Angolan Law provides for the establishment of the Data Protection Agency (DPA). The DPA will be responsible for supervising and monitoring compliance with data protection laws and regulations. However, the DPA has not yet been established.

Cross-Border Transfers

The transfer of personal information to countries that do not ensure an adequate level of protection requires, as a rule, the individual's unambiguous, explicit and written consent, and prior authorization from the DPA.

Data Security

In addition to the usual data security obligations, there are specific rules for processing sensitive information. Moreover, the Angolan Law specifies that the processing systems must separate data concerning health or sex life, including genetic data, and other personal information. In addition, where such data are transmitted via a network, in specific cases the DPA may require the data to be “encoded.”

Data Security Breach Notification

While there are no breach notification requirements under the Angolan Law, there are, however, breach notification obligations under the Law on Electronic Communications and Information Society Services, which requires operators in the electronic communications sector to give notice in the event of a data security breach. An “operator” is an undertaking that provides or is authorized to provide a communications network or electronic communications services. In particular, where there is a violation of security measures that, intentionally or recklessly, results in the destruction, loss, whole or partial alteration or unauthorized access to personal information transmitted, stored, retained or otherwise processed in connection with the provision of electronic communications services in Angola, the operator must, without undue delay, notify the DPA and the INACOM (Regulatory Authority for Electronic Communications in Angola; Instituto Angolano das Comunicações).

Registration

The Angolan Law requires that all personal information to be processed be registered for all purposes, prior to the beginning of processing, unless an exemption applies. Certain types of processing require prior DPA authorization. For example, the processing of sensitive information and personal credit video surveillance data, as well as transfers to countries that do not provide an adequate level of protection, require DPA authorization. The registration process is not yet operative, pending the establishment of the DPA.

BENIN

Law no. 2009-09 on the Protection of Personal Data (Benin Law), enacted in 2009, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

The Benin Law restricts cross-border transfers to countries that do not provide adequate protection and requires registration. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO; however, if a DPO is appointed, registration is not required.

Special Characteristics

Data Protection Authority

The Commission Nationale de l'Informatique et des Libertés (DPA), an independent administrative authority, is charged with overseeing compliance with the Benin Law.

Cross-Border Transfers

Organizations may only transfer personal information to countries outside Benin that provide an adequate level of protection. DPA authorization is required for all processing of personal information that includes transfers to countries outside Benin, particularly where transfers are based on contractual clauses or internal rules.

Data Protection Officer

There is no requirement to appoint a DPO; however, registration is not required if a DPO is appointed to maintain a registry of the organization's processing activities.

Registration

Organizations must register the processing with the DPA for all data and all purposes except where such processing is carried out for certain purposes, such as general accounting, personnel payroll management or supplier management purposes. Registration is not required if the organization appoints a person to maintain a registry of the processing activities.

BURKINA FASO

Law no. 010-2004 on the Protection of Personal Data (Burkina Faso Law), enacted in 2004, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

Databases must be registered with the DPA, and transfers of personal information to countries outside Burkina Faso are only permitted where they are carried out in a manner that ensures an equivalent level of protection. There are also special security rules for certain types of health-care data. However, there is no obligation to appoint a DPO or give notice in the event of a data security breach.

Special Characteristics

Data Protection Authority

The Commission de l'informatique et des libertés (DPA) is responsible for enforcement of the Burkina Faso Law.

Cross-Border Transfers

Transfers of personal information to countries outside Burkina Faso are only permitted where the transfers are carried out in a manner that ensures an equivalent level of protection for the personal information. Specific DPA authorization is not required for cross-border transfers, but such transfers must be included in the prior registration with the DPA.

Data Security

Nominative data disclosed by health-care professionals through automated processing must be coded before they are transmitted, except where the processing of data is associated with drug monitoring studies (pharmacovigilance) or research agreements concluded in the context of national and international cooperative studies, or when the distinct feature of the

research requires it.

Registration

Organizations must register all processing of personal information with the DPA prior to commencement of the processing. The recipients or categories of recipients to whom personal information is or may be disclosed must be included in the registration with the DPA.

CAPE VERDE

The Law on Protection of Personal Data, enacted in 2001 and amended in 2013 (Cape Verde Law), regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

The Cape Verde Law restricts cross-border transfers of personal information, requires registration of data processing and imposes some additional data security obligations; however, there is no obligation to appoint a DPO or give notice in the event of a data security breach.

Special Characteristics

Data Protection Authority

The Comissão Nacional de Protecção de Dados (DPA), an independent administrative authority working with the National Assembly of Cape Verde, is responsible for the supervision of the protection of the personal information of individuals and for monitoring compliance with the terms of the Cape Verde Law. The DPA was established in April 2015.

Cross-Border Transfers

Personal information may only be transferred to a country that ensures an adequate level of protection unless an exception applies. Such exceptions include: the individual's consent, contractual necessity, legal requirement and vital interests. Transfers to countries that do not ensure an adequate level of protection require prior DPA authorization. International transfers based on the individual's consent also require prior DPA authorization.

Data Security

In addition to the usual data security obligations, there are specific rules for processing sensitive information. Moreover, where such data are transmitted via a network, in specific cases the DPA may require the data to be “encoded.”

Registration

Organizations must register all personal information for all purposes, prior to the beginning of the processing, unless an exemption applies.

COTE D'IVOIRE

The Law 2013-450 on Protection of Personal Data (Cote D'Ivoire Law), enacted in August 2013, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

The Cote D'Ivoire Law restricts cross-border transfers, requires registration, imposes additional security measures and establishes the right to be forgotten. Data security breach notification is not required, and the appointment of a DPO is voluntary.

Special Characteristics

Data Protection Authority

Enforcement of the Cote D'Ivoire Law and the other missions of the Data Protection Authority (DPA) are conferred on the

Telecommunications/ICT Regulatory Body of Côte d'Ivoire, an independent administrative authority.

Cross-Border Transfers

Organizations may only transfer personal information to a “third country” that provides an equivalent level of protection. Prior DPA authorization is required for such transfers. The Cote D'Ivoire Law defines a “third country” as any country outside the Economic Community of West African States (ECOWAS). The 15 ECOWAS member states currently are: Benin, Burkina Faso, Cape Verde, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, the Togolese Republic and Cote d'Ivoire. There are no limitations on the transfer of personal information to other ECOWAS member states.

Data Protection Officer

The appointment of a DPO is voluntary; however, the appointment of a DPO relieves the organization of general registration requirements, but not of the requirement to obtain prior authorization for the transfers to third countries.

Data Security

The Cote D'Ivoire Law specifies in greater detail than other laws the technical and organizational measures required. In particular, there are 10 specific obligations imposed on organizations, such as an organization must:

- guarantee that it is possible to know and verify the identity of any third parties to whom the data are transmitted by transmission installations;

- guarantee that it is possible to know and verify, a posteriori, the identity of persons who have had access to the information system; the nature of the data that have been entered, modified, altered, copied, erased or read in the system; and the time at which they were manipulated;

- prevent the unauthorized reading, copying, modification, alteration or deletion of data when the data are communicated or transported in storage media; and

- prevent the use of processing systems for money laundering or terrorist financing.

Organizations must also prepare an annual report for the DPA on their compliance with the security measures required under the law.

Registration

Organizations must register all processing of personal information with the DPA prior to the commencement of processing, unless a DPO has been appointed or another exception applies. Prior authorization is required for certain types of processing of personal information. Registrations may be submitted to the DPA by e-mail, postal mail or any in other form that allows a receipt to be issued. The DPA will make a decision in response to the registration/request for prior authorization within one month from the day it is received (the one-month period may be extended once upon the reasoned decision of the DPA); the data organization may begin the processing once it has received such receipt. The absence of a receipt from the DPA means that the DPA has rejected the registration/request for prior authorization. The data controller may appeal such decision in the competent court.

Right to Be Forgotten

Where an organization has authorized a third party to publish personal information, the organization is deemed responsible for the publication and must take all appropriate measures to implement the digital “right to be forgotten” and the right to have one's personal information deleted. The organization must put in place appropriate mechanisms to ensure the respect of the “right to be forgotten” in a digital context.

GABON

Law no. 001/2011 on the Protection of Personal Data (Gabon Law), enacted in 2011, regulates the processing of all personal information of natural persons by both the public and private sectors. The DPA was established in November 2012.

In Brief

The Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration and imposes additional security requirements and health rules. The appointment of a DPO is not required, but the appointment of one may relieve the organization of some, but not all, of its registration obligations. There is no obligation to give notice in the event of a data security breach or appoint a DPO.

Special Characteristics

Data Protection Authority

The National Commission for the Protection of Personal Data (DPA), an independent administrative authority, is responsible for enforcement. The DPA was established in November 2012; however, there is no website established yet.

Cross-Border Transfers

Organizations may not transfer personal information to countries that do not provide a sufficient level of the protection, unless an exception applies. Exceptions include consent, contractual necessity, vital interests and the establishment of legal claims. If none of the exceptions applies, the organization may apply to the DPA for authorization, particularly where the transfer relies on the use of contractual clauses or internal rules. The DPA will publish a list of countries that provide sufficient protection for personal information.

Data Protection Officer

There is no obligation to appoint a DPO; however, the appointment of a DPO exempts the organization from registration requirements but only where the processing does not involve cross-border transfers. The appointment of a DPO must be notified to the DPA and must be brought to the attention of employee representative bodies (e.g., works councils or labor unions). The DPO may not be sanctioned by his/her employer as a result of performing his/her duties. If the DPO encounters difficulties while performing his/her duties, he/she must apply to the DPA. In cases of where the DPO does not carry out his required duties, the DPO may be discharged after consultation with the DPA.

Data Security

Like the Cote D'Ivoire Law, the Gabon Law also imposes detailed security requirements. However, the Gabon requirements are potentially more onerous because organizations must:

- guarantee that unauthorized persons cannot access automated processing systems or the personal information contained therein;
- guarantee that any third parties to which personal information is or can be transferred can be identified and verified;
- guarantee that it is possible to identify and verify any access to and entry of data into the system after such access has taken place, as well as what data were accessed or entered, at what time and by whom;
- prevent unauthorized access to the premises and equipment used for the processing of personal information;
- prevent storage media from being read, copied, modified, destroyed or moved by unauthorized persons;
- prevent the unauthorized entry of any data into the information system, as well as any unauthorized knowledge, modification or deletion of personal information;
- prevent systems from being used by unauthorized persons with the aid of data transmission equipment;
- prevent the unauthorized reading, copying, modification or deletion of any personal information or storage media containing personal information while in transit;
- save personal information (make backup copies); and
- refresh, and if necessary, convert data for permanent storage.

Health professionals may transfer personal information they use within the framework of the authorized processing of personal information. Where such data permit the identification of individuals, they must be encrypted before they are

transmitted, unless the data are associated with pharmacovigilance studies or research protocols carried out in the context of cooperative national or international studies, or where necessitated by the specificity of the research.

Personal information transferred to another country in the context of health research must be encrypted, unless the processing and transfer is in compliance with all the requirements for the lawful processing of personal information.

Registration

Organizations must register all processing with the DPA, unless a DPO has been appointed or an exception applies. Authorization is required for certain types of processing, such as the processing of sensitive information.

Special Health Rules

The publication of the results of processing of personal information for health research purposes must not, under any circumstances, permit the direct or indirect identification of individual. The person responsible for the research must ensure that the processing respects the purposes for which the information was collected.

Data from medical files retained by health professionals and health insurance systems to carry out their functions cannot be communicated for purposes of statistical evaluation or analysis of medical treatment and prevention practices unless (i) the data are aggregated or organized in such a way that the individuals cannot be identified, or (ii) a specific authorization from the DPA is obtained. Exceptions to these requirements may only be authorized by the DPA and, in such cases, may not include the name, first name or national identification number of individuals. The results of the processing of such data must not, under any circumstances, be published in a form that permits the direct or indirect identification of individuals.

GHANA

The Data Protection Act (Act 843) (Ghana Law), enacted in May 2012 (152 PRA, 8/8/12), regulates the processing of all personal information of natural persons by both the public and private sector organizations. The Ghana Law is one of the few data protection laws around the world that contains a carve-out for outsourcing. In particular, the Ghana Law states that when personal information of foreign individuals is to be sent to Ghana for processing, the information must be processed in compliance with the data protection legislation of the foreign jurisdiction of the individual.

In Brief

The Ghana Law requires data security breach notification and registration. The appointment of a DPO is voluntary, and there are no restrictions imposed on cross-border transfers.

Special Characteristics

Data Protection Authority

The Data Protection Commission (DPA), established in November 2014 (192 PRA, 10/3/14), is responsible for enforcement of the Ghana Law. The DPA is governed by a board consisting of representatives from different government agencies, industry and academia. It is unusual to have industry officials sit on the governing board.

Data Protection Officer

The appointment of a DPO is voluntary. The Ghana Law provides for the DPA to establish qualifications criteria for DPOs and states that organizations should not appoint someone as a DPO unless he or she satisfies such criteria.

Data Security Breach Notification

Ghana was the first African country to include a breach notification obligation in its law. Under the Ghana Law, an organization, or the third party that processes personal information under the authority of the organization, must provide notice to the DPA and the affected individuals where there are reasonable grounds to believe that the personal information has been accessed or acquired by an unauthorized person. The organization must take steps to ensure the restoration of the integrity of the information system.

Registration

Organizations must register all processing of personal information with the DPA. The processing of personal information without a registration is prohibited. The recipients and countries to which personal information is intended to be transferred must be listed in the organization's database registration. The registration process opened in May 2015 and data controllers were given until July 31, 2015 to register with the DPA. Failure to register is an offense under the Ghana Law.

ISRAEL

The Protection of Privacy Law 5471-1981 (Israeli Law), enacted in 1981, regulates the processing of all personal information of natural persons by both the public and private sectors. Israel is the first and only country in the region to be recognized by the EU as providing an adequate level of protection for personal information transferred from the EU/European Economic Area (22 PRA, 2/2/11).

In Brief

The Israeli Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration and imposes detailed security requirements. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.

Special Characteristics

Data Protection Authority

The Israeli Law, Information and Technology Authority (DPA), established in the Ministry of Justice, is responsible for enforcement of the Israeli Law.

Cross-Border Transfers

To transfer to third parties outside Israel, consent or another legal basis is required unless the transfer is to affiliates that are under the corporate control of the Israeli company. Prior authorization of cross-border transfers is not required.

Data Security

There are comprehensive security rules that include specific requirements for outsourcing activities. In addition, organizations with five or more databases that require registration, banks, insurance companies and companies engaged in ranking or evaluating credit ratings must appoint a security officer. The identity of the security officer must be reported to the DPA.

Registration

Databases that fall into specific categories (e.g., databases containing personal information on more than 10,000 people or databases containing sensitive information) must be registered with the DPA.

MADAGASCAR

Law no. 2014-038 on the Protection of Personal Data (Madagascar Law), enacted in January 2015, regulates the processing of personal information of natural persons by both public and private sector organizations.

In Brief.

The Madagascar Law restricts cross-border transfers to countries that do not provide adequate protection. It also requires registration and the appointment of a DPO. However, there is no obligation to give notice in the event of a data security breach.

Special Characteristics

Data Protection Authority

The Madagascar Law provides for the establishment of the Malagasy Commission on Informatics and Liberty (DPA), an independent regulator, which is charged with enforcement of the law. The DPA is not yet established.

Cross-Border Transfers

Organizations may not transfer personal information to countries that do not provide adequate protection unless the DPA authorizes the transfer based on, for example, contractual clauses or internal rules that provide sufficient guarantees of adequate protection. Alternatively, such transfers can take place where an exception applies, such as consent, contractual necessity, vital interests or a legal requirement. The Madagascar Law also prohibits subsequent transfers except with the approval of the organization responsible for the original processing and the DPA.

Data Protection Officer

A DPO must be appointed. The appointment of a DPO relieves the organization of its registration obligations, except in cases where the processing requires DPA authorization. The DPA will maintain a list of the designated DPOs.

Registration

The processing of personal information must be registered with the DPA. The processing of personal information that poses special risks to individuals requires DPA authorization before such processing can begin.

MALI

Law no. 2013/015 on the Protection of Personal Data (Mali Law) was adopted in May 2013. It regulates the processing of all personal information of legal and natural persons by both the public and private sectors. The Mali Law is unusual because it protects the personal information of both individuals and companies, and, as discussed below, there are no explicit rules regarding consent.

In Brief

The Mali Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration and imposes some additional security requirements. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.

Special Characteristics

Data Protection Authority

The Authority for the Protection of Personal Data (DPA) became operational in March 2016.

Consent

There are no explicit rules regarding consent. The Mali Law only states that notice must be provided and the natural or legal person must be advised that they have the right to refuse to be included in a personal data file. Moreover, both legal and natural persons have a general right to oppose the processing of their personal information on legitimate grounds. In addition, the processing of sensitive personal information is prohibited unless one of the narrow exceptions apply; consent is not one of the legal bases listed.

Cross-Border Transfers

Organizations may transfer personal information to a third country where the third country to which the information is transferred provides an adequate level of protection for personal information, as determined by the DPA. Transfers of personal information to a third country that does not provide an adequate level of protection may be authorized by the DPA, where both the transfer and the processing by the recipient guarantee an adequate level of protection for privacy, notably by the use of contractual clauses or internal rules.

Registration

Organizations must register all processing operations for a specific purpose with the DPA.

MAURITIUS

The Data Protection Act 2004 (Mauritius Law) regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

The Mauritius Law restricts cross-border transfers to countries that do not provide adequate protection and requires registration. However, there is no obligation to appoint a DPO or give notice in the event of a data security breach. The DPA has issued voluntary data security and data security breach notifications guidelines, however.

Special Characteristics

Data Protection Authority

The Data Protection Commissioner (DPA) is responsible for monitoring and enforcing compliance with the Mauritius Law. While the DPA operates under the aegis of the prime minister's office, the DPA was guaranteed functional independence after an amendment was enacted in 2009.

Cross-Border Transfers

Written authorization from the DPA is required for all transfers of personal information to countries outside Mauritius. In addition, personal information may only be transferred to countries that do not provide an adequate level of protection where the individual has consented to the transfer or another exception applies. Other exceptions include contractual necessity and DPA-approved contracts or binding corporate rules.

Data Security

The DPA has published detailed guidelines on security practices and privacy impact assessments.

Data Security Breach Notification

There is no mandatory obligation to give notice in the event of a data security breach under the Mauritius Law; however, the DPA has issued Guidelines for Handling Privacy Breaches, which recommend that organizations provide notice to individuals and/or the DPA in the event of a security breach that presents a risk of harm to the individuals whose personal information is involved in the breach.

Registration

All organizations must register with the DPA prior to the commencement of the processing of any personal information.

MOROCCO

Law no. 09-08 on the Protection of Individuals in Relation to the Processing of Personal Data (Moroccan Law), which took effect in 2009 (67 PRA, 4/10/09), regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief.

The Moroccan Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration and imposes some additional security requirements. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.

Special Characteristics

Data Protection Authority

The National Supervisory Authority (DPA) is responsible for supervising compliance with the Moroccan Law.

Cross-Border Transfers

Personal information may only be transferred to a foreign country that does not ensure an adequate level of protection, where an exception applies, such as vital interests or contractual necessity, or where there are DPA-authorized contractual clauses or binding corporate rules (BCRs) in place. All jurisdictions that have been found by the EU as proving adequate protection are similarly recognized by the Morocco.

Data Security

There are specific requirements on organizations that process sensitive information, including health data, as well as provisions related to encryption and the supervision of service providers. According to the DPA, organizations have the obligation to ensure through contractual means and compliance audits that their service providers comply with security requirements. The DPA has issued template language that organizations may use in their contracts with data processors.

Registration

Organizations must register all partially or wholly automatic processing of personal information with the DPA prior to the commencement of processing, unless an exception applies. In addition to registration, prior authorization must be obtained for certain types of processing, such as the processing of sensitive information including genetic, health and criminal data.

QATAR/QATAR FINANCIAL CENTRE

Financial services organizations licensed by the Qatar Financial Centre (QFC) in Doha, Qatar are subject to the Data Protection Regulations 2005 (Regulations) that regulate their processing of personal information of natural persons. The QFC is a financial and business center located in Doha that was established by the government of Qatar in 2005 to attract international financial services and multinational corporations to grow and develop the market for financial services in the region. The QFC has no physical boundaries. It is an onshore jurisdiction established in the State of Qatar, which operates alongside of, but separate from, the civil and commercial laws of the state.

The Qatari cabinet announced in January 2016 that it approved a draft privacy law and has referred it to its legislative body for review and adoption.

In Brief

The Regulations restrict cross-border transfers to countries that do not provide adequate protection and require registration. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.

Special Characteristics

Data Protection Authority

The Qatar Financial Centre Authority (QFC Authority) is the regulatory body responsible for overseeing the implementation of compliance with the Regulations.

Cross-Border Transfers

Personal information may not be transferred to countries outside the QFC unless the recipient country provides an adequate level of personal data protection, the individual has provided his/her consent to the transfer or another exception applies. Alternatively, organizations may apply to the QFC Authority for a permit for the transfer. The QFC Authority does not provide a list of countries it considers to provide adequate protection for personal data.

Registration

Organizations must register with the QFC Authority prior to or immediately upon the processing of any personal information. Organizations may also apply for a permit to process sensitive personal information and/or transfer personal information to inadequate countries.

SENEGAL

Act no. 2008-12 on the Protection of Personal Data (Senegal Law), which took effect in 2008, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

The Senegal Law restricts cross-border transfers to countries that do not provide adequate protection and requires registration. However, there is no obligation to give notice in the event of a data security breach or appoint a DPO.

Special Characteristics

Data Protection Authority

The Commission for the Protection of Personal Data (DPA) is responsible for enforcement of the Senegal Law.

Cross-Border Transfers

Organizations may only transfer personal information to a third country if that third country provides a sufficient level of protection. However, organizations may transfer personal information to a third country without adequate protection if the transfer is occasional and not massive, and if the individual has provided his/her express consent to the transfer, or if another exception applies, such as contractual necessity or vital interests. The DPA may authorize a transfer or group of transfers to a third country without adequate protection where the organization provides sufficient guarantees.

Registration

Organizations must register all automatic processing of personal information with the DPA unless an exception applies. In addition to registration, certain processing is subject to DPA authorization, such as where the information is transferred to countries that do not provide adequate protection or where certain types of data such as sensitive information is processed.

SEYCHELLES

The Data Protection Act, 2003 (No. 9 of 2003) (Seychelles Law), which took effect in 2003, regulates the processing of all personal information of natural persons.

In Brief.

The Seychelles Law requires registration with the DPA. There are no restrictions on cross-border transfers set forth in the law; however, the DPA has the authority to prohibit such transfers as explained below. There is no requirement to appoint a DPO or give notice in the event of a data security breach.

Special Characteristics

Data Protection Authority

The Seychelles Law provides for the establishment of a Data Protection Commissioner (DPA); however, there is no indication that one has been established.

Cross-Border Transfers

The DPA has the power to prohibit cross-border transfers if it believes such transfers will violate the data protection principles under the act.

Registration

Processing must be registered with the DPA.

SOUTH AFRICA

South Africa's Protection of Personal Information Act (South African Law) was published in the official gazette Nov. 26, 2013 (234 PRA, 12/5/13); however, it will only commence on a date to be proclaimed by the president. One of the reasons for the delay is the need to nominate the Information Regulator, empowered to enforce the new law. In April 2016, it was reported that the Parliament developed a short list of candidates for the position so it is possible that the Information Regulator will be established in 2016. If that happens, then this POPI might commence later this year. Organizations will have one year from the date of commencement to comply with the South African Law. The South African Law regulates the processing of all personal information of natural and legal persons by both the public and private sectors.

In Brief

The South African Law restricts cross-border transfers to countries that do not provide adequate protection. It also requires

data security breach notification, the appointment of a DPO and registration.

Special Characteristics

Data Protection Authority

The South African Law provides for the establishment of the Information Regulator (DPA), which will be responsible for enforcement of the law. The DPA is not yet established.

Cross-Border Transfers

Organizations may not transfer personal information to a third party in a foreign country unless the individual consents to the transfer; the recipient is subject to a law, contract or BCRs that provide an adequate level of protection; or another exception applies. Prior DPA authorization is required to transfer sensitive personal information or personal information of children to a third party in a foreign country that does not provide an adequate level of protection, unless a code of conduct is applicable.

Data Protection Officer

A DPO must be appointed. Each organization must also ensure that it appoints as many deputy DPOs as necessary to fulfill its access obligations under the law. Deputy DPOs will have the same powers and duties as the DPO.

Data Security Breach Notification

Organizations must notify the DPA and the individual when there are reasonable grounds to believe that personal information has been accessed or acquired by any unauthorized person. Notice must be given as soon as reasonably possible after the discovery of the beach.

Registration

The South African Law imposes limited registration obligations, requiring organizations to notify the DPA about any processing that is subject to authorization requirements under the law. Authorization is required prior to processing information such as unique identifiers, sensitive information and children's information transferred to a third party in a foreign country that does not provide an adequate level of protection.

TUNISIA

The Organic Law no. 2004-63 on Personal Data Protection (Tunisian Law), which took effect in 2004 (170 PRA, 9/2/04), regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief

The Tunisian Law restricts cross-border transfers to countries that do not provide adequate protection. It also requires registration and the appointment of a DPO.

Special Characteristics

Data Protection Authority

The National Authority for Protection of Personal Data (DPA) is responsible for enforcement of the Tunisian Law.

Cross-Border Transfers

Personal information may not be transferred to countries outside Tunisia unless that country ensures an adequate level of protection. Moreover, transfers outside Tunisia must be approved by the DPA.

Data Protection Officer

Organizations must list on the registration/notification forms the name of the DPO. The DPO must have Tunisian nationality, reside in Tunisia and have a clean criminal record.

Registration

The Tunisian Law provides for two kinds of registrations: notifications that are applicable to all kinds of data and authorizations that are applicable to sensitive data. The processing of sensitive information may not begin without an affirmative authorization from the DPA. Prior authorization is required for the cross-border transfer of personal information to countries outside Tunisia.

UNITED ARAB EMIRATES/DUBAI INTERNATIONAL FINANCIAL CENTER (DIFC)

Private sector organizations located in the Dubai International Financial Center (DIFC), a 110-acre area within the city of Dubai, are subject to the DIFC Data Protection Law (DIFC Law), which was enacted in 2007 (16 PRA, 1/25/07) and amended in 2012. [34] The DIFC is a federal financial free zone established in 2004 for the conduct of financial services. It has its own civil and commercials laws, court system and judges and financial regulator, separate from the United Arab Emirates.

---

[34] The DIFC Law is available at .

The DIFC Law regulates the processing of all personal information of natural persons.

In Brief

The DIFC Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration and imposes data security breach notification obligations. There is no requirement to appoint a DPO.

Special Characteristics

Data Protection Authority

The Commissioner of Data Protection (DPA) is responsible for enforcement of the DIFC Law.

Cross-Border Transfers

Personal information may not be transferred to countries outside the DIFC that do not provide an adequate level of protection unless the individual has consented in writing, the DPA has authorized the transfer or another exception such as contractual necessity or vital interests applies.

Data Security Breach Notification

In the event of an unauthorized intrusion, whether physical, electronic or otherwise, to any personal information database, organizations must notify the DPA. Notice to individuals is not legally required.

Registration

Organizations must file a notification with the DPA concerning any processing of sensitive personal information and any transfers of personal information to a recipient in a territory outside the DIFC that is not subject to laws and regulations that ensure an adequate level of protection.

Bloomberg Law®