Bloomberg Law

Privacy and Security Law Report®

Data Protection

A Look at New Trends in 2017: Privacy Laws in Africa and the Near East

Data Protection

In this final article of a four-part series on the status of international data protection laws, the author explores developments in Africa and the Near East, where 21 jurisdictions have comprehensive privacy laws. Other parts of the series cover East, Central, and South Asia and the Pacific; the Western Hemisphere; and Europe and Eurasia (non-EEA).

By Cynthia Rich

Introduction/Region at-a-Glance

The privacy landscape in Africa and the Near East has changed remarkably in the past few years. Twenty-one countries have enacted comprehensive privacy laws: Angola, Benin, Burkina Faso, Cape Verde, Chad, Côte d'Ivoire—also known as the Ivory Coast—Equatorial Guinea, Gabon, Ghana, Israel, Lesotho, Madagascar, Mali, Mauritius, Morocco, Qatar, Senegal, Seychelles, South Africa, Tunisia, and the United Arab Emirates/Dubai International Financial Centre. Half of these laws were enacted or revised in the past five years. 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, Niger, Tanzania, Uganda, and Zimbabwe in Africa 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 and/or have insufficient funding; 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.

Cynthia Rich is a senior adviser 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.

Developments and Trends

Enforcement Enforcement activity in the region continues to grow. In addition to the data protection authorities (DPAs) in Israel, Mauritius, and Morocco, who have well-established programs, the DPAs in Benin, Ghana, Mali, Senegal, and Tunisia are becoming more outspoken and active. In February 2017, the Mali DPA fined a telecommunications company 15 million CFA francs ($27,457) for violating its security obligations un-

 ISSN 1538-3423

der the Mali data protection law, which resulted in unauthorized access to a customer's cellphone messages by a company employee. The year before, it fined two utility companies 5 million CFA francs ($9,152) each for violating their security and confidentiality requirements under the Mali law. The companies were found to have unlawfully publicized on social media the electricity and water bills of delinquent clients.

In Senegal, the DPA has been carrying out inspections in response to complaints, identifying law violations, and issuing recommendations. The DPA has announced its intention to pay particular attention to cross-border transfers to make sure they comply with the requirements under the law. It also has encouraged citizens to report any law violations to the DPA or simply check and challenge the legality of the processing of their personal information. In Tunisia, the DPA, which generally does not publish information about its enforcement actions, announced last year that it would be filing lawsuits against 12 public and private organizations for privacy law violations. In Ghana, the DPA is going after data controllers who have failed to register their processing activities. The registration process began on May 1, 2015, and organizations were given six months to file their registrations. As of early this year, only a minority of data controllers had registered. After issuing verbal warnings to more than 100 organizations in 2016, the DPA is now working with the police to make sure those who fail to register are sanctioned accordingly. In March 2017, the DPA reported that three organizations had been convicted of violating the law and fined for failing to register, but no specific details regarding those fines were provided.

Also noteworthy is the creation last year of the African Network of Personal Data Protection Authorities (RAPDP) by Cape Verde, Benin, Burkina Faso, Côte d'Ivoire, Mali, Morocco, Senegal, and Tunisia. The purpose of the RAPDP is to organize close cooperation between members, support the drafting of data protection laws, formulate opinions or statements on specific issues, establish a consultative framework on data protection issues and challenges, and promote African data protection instruments. Increased cooperation among these African regulators is likely to encourage other authorities in the region to step up their own enforcement efforts.

New Privacy Laws and Regulations Equatorial Guinea, Qatar, and Chad are the three newest countries in the region to adopt comprehensive privacy legislation. In December 2016, Qatar enacted a national law that became effective in January 2017. The Qatar Law on the Protection of Personal Data applies to personal information that is electronically processed or obtained, collected, or extracted by any other means in preparation for electronic processing by controllers, processors, and website operators. Prior to the enactment of the national law, only organizations licensed to operate in the Qatar Financial Centre (QFC), a financial and business center located in Doha, were subject to data privacy rules. In July 2016, Equatorial Guinea enacted its Law on Personal Data Protection, which regulates the processing of citizens' personal information by the public and private sectors; in 2015, Chad enacted its own law, which regulates the public and private sector processing of personal information.

In addition, in April 2017, Israel's parliament approved new privacy and data security regulations that impose additional obligations in a variety of areas, ranging from breach notification to physical maintenance of IT infrastructure. Under the new security regulations, which take effect in March 2018, databases will be classified into four categories: Individual-Managed Databases, Basic Security Databases, Intermediate Security Databases, and High-Security Databases. Classification is determined primarily by the number of individuals who have access to the database; the number of individuals whose personal information is contained in the database; and the types and the sensitivity of the information that the database contains. The regulations impose the fewest obligations on Individual-Managed Databases and the most obligations on High-Security Databases.

Legislation Under Development Several countries, such as Kenya, Niger, Tanzania, Uganda, and Zimbabwe in Africa and Saudi Arabia in the Near East, are reported to be working on adopting legislation. For example, Kenya, Saudi Arabia, and Uganda have introduced bills in their parliaments. Tanzania is also reportedly working on data protection legislation; however, no draft texts have been made public. Tunisia has issued for public consultation a new draft law to comply with the Convention 108 of the Council of Europe (CoE Convention). Tunisia becomes an official member of the CoE Convention on Nov. 1, 2017.

PVLR ISSN 1538-3423

OVERVIEW OF DATA PRIVACY LAWS IN AFRICA/NEAR EAST COUNTRIES

Countries With Privacy Laws	Year Enacted (Amended)	Registration Requirement	DPO Required[1]	Cross-border Limitations	Data Breach Notification Requirement[2]
Africa/Near East (21)		**20**	**3**	**18**	**6**
Angola	2011	**Yes**	No	**Yes**	No
Benin	2009	**Yes**	No	**Yes**	No
Burkina Faso	2004	**Yes**	No	**Yes**	No
Cape Verde	2001 (2013)	**Yes**	No	**Yes**	No
Chad	2015	**Yes**	No (voluntary)	**Yes**	**Yes**
Cote D'Ivoire	2013	**Yes**	No (voluntary)	**Yes**	No
Equatorial Guinea	2016	**Yes**	No	**Yes**	No
Gabon	2011	**Yes**	No	**Yes**	No
Ghana	2012	**Yes**	No	No	**Yes**
Israel	1981	**Yes**	No	**Yes**	No
Lesotho	2013	**Yes**	No (voluntary)	**Yes**	**Yes**
Madagascar	2014	**Yes**	**Yes**	**Yes**	No
Mali	2013	**Yes**	No	**Yes**	No
Mauritius	2004	**Yes**	No	**Yes**	No (recommended)
Morocco	2009	**Yes**	No	**Yes**	No
Qatar	2016	No	No	No	**Yes**
Senegal	2008	**Yes**	No	**Yes**	No
Seychelles	2003	**Yes**	No	No	No
South Africa[3]	2013	**Yes**	**Yes**	**Yes**	**Yes**
Tunisia	2004	**Yes**	**Yes**	**Yes**	No
United Arab Emirates[4] DIFC ADGM	 2007 (2012) 2015	 **Yes** **Yes**	 No No	 **Yes** **Yes**	 **Yes** **Yes**

[1] In some jurisdictions, the appointment of a Data Privacy Officer (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.

[4] The Dubai International Financial Center (DIFC) is a financial free trade zone established within the city of Dubai. It has its own civil and commercials laws, court system and judges and financial regulator, separate from the United Arab Emirates. The DIFC Law regulates the processing of all personal information by controllers. The Abu Dhabi Global Market (ADGM) is a financial free trade zone in Abu Dhabi. The ADGM Data Protection Regulations (ADGM Regulations regulate the processing of personal information by controllers and processors.

Source: MORRISON & FOERSTER LLP

Bloomberg BNA

Africa and Near East Privacy Laws

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, unauthorized access, disclosure, alteration, and destruction. Some of the countries, such as Israel and the Côte 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.

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 but one of the countries in the region (Qatar) require registration of processing, and all but three country restrict cross-border transfers; however, the reality is that there are 20 different registration and 18 different cross-border rules and procedures. Generally a contract, consent (or another legal basis), and/or 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. Only three countries 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 one quarter 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.

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

  PVLR ISSN 1538-3423

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 require 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. In addition, organizations must register all video surveillance systems and, in some cases, obtain DPA authorization. DPA authorization is also required to process biometric data, health data, and national ID numbers.

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 features of the research require 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. In addition, processing of certain types of data such as sensitive personal information requires prior DPA authorization.

CHAD

Act 007/PR/2015 Regarding The Protection Of Personal Data (Chad Law), enacted in 2015, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief *The Chad Law restricts cross-border transfers of personal information and requires data breach notification and registration of data processing. There is no obligation to appoint a DPO; however, if a DPO is appointed, then the organization may be exempt from registration.*

Special Characteristics

Data Protection Authority The Chad Law provides for the creation of the Agence Nationale de Sécurité Informatique et de Certification Electronique (DPA), which is responsible for enforcing compliance with the Chad Law. The DPA is not yet established.

Cross-Border Transfers Personal information may not be transferred to a country outside the Central African Economic and Monetary Community (CEMAC) and the Economic Community of Central African States (CEEAC) unless that country ensures an adequate level of data protection. The six members of CEMAC are: Gabon, Cameroon, the Central African Republic (CAR), Chad, the Republic of the Congo, and Equatorial Guinea. The 10 members of CEEAC are: Angola, Burundi, Cameroon, Central African Republic, Congo, Democratic Congo, Gabon, Equatorial Guinea, São Tomé & Príncipe, and Chad.

If the transfer is to a country that is not considered adequate, the individual must consent to the transfer or another exemption, such as contractual necessity, must apply. Organizations must notify the DPA in advance of such transfers. The DPA may also authorize transfers to a third country where the organization has in place appropriate contractual clauses.

Data Security Breach Notification Notice must be provided to individuals and the DPA whenever there is any breach of security that affects personal information.

Registration Organizations must register all personal information for all purposes, prior to the beginning of the processing, unless an exemption applies. In addition, processing of certain types of data, such as sensitive personal information, genetic and biometric data, and national ID numbers requires prior DPA authorization.

CŒTE D'IVOIRE

The Law 2013-450 on Protection of Personal Data (Côte 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 Côte d'Ivoire Law restricts cross-border transfers, requires registration, imposes additional security measure,s 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 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 Côte 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.

  PVLR ISSN 1538-3423

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 in any 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.

Equatorial Guinea

Law No. 1/2016, Law on Personal Data Protection (Equatorial Guinea Law), enacted in 2016, regulates the processing of all personal information of citizens by both the public and private sectors.

In Brief *The Equatorial Guinea Law restricts cross-border transfers of personal information and requires registration of data processing. There is no obligation to appoint a DPO or provide notification in the event of a data security breach.*

Special Characteristics

Data Protection Authority The Equatorial Guinea Law provides for the creation of the Personal Data Protection Governing Authority (DPA), which is responsible for enforcing compliance with the Equatorial Guinea Law. The DPA is not yet established.

Cross-Border Transfers Organizations may not transfer any processed personal information to countries that that fail to provide a legally equivalent level of protection, unless the transfer has been previously authorized by the DPA or an exception such as consent or contractual necessity applies.

Registration Organizations must register their processing of personal information with the DPA.

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 apply, 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 Côte 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, 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 individuals. 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 last name, first name, or national ID 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, regulates the processing of all personal information of natural persons by both 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, is responsible for enforcement of the Ghana Law. The DPA is governed by a board consisting of representatives from different government agencies, industries 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

  PVLR ISSN 1538-3423

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. In April 2017, the Israeli Parliament approved new privacy and data security regulations that impose additional obligations in a variety of areas, ranging from breach notification to physical maintenance of IT infrastructure. The regulations take effect in March 2018.

In Brief *The Israeli Law restricts cross-border transfers to countries that do not provide adequate protection, requires registration, and imposes detailed security requirements. Effective March 2018, owners of Intermediate and High Security Databases will be required to report any data breaches to the DPA. While there is no obligation to appoint a DPO, there is an obligation on certain companies to appoint a Security Officer.*

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 Breach Notification Effective May 2018, owners of Intermediate and High Security Databases must immediately report to the DPA any data breaches, as well as any measures they are taking in response to such incidents. The DPA may, after consultation with the Israel National Cyber Bureau, direct the database owner to provide notice to any individual whose personal information may have been compromised.

Data Security The Israeli Law sets forth 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.

When the new security regulations take effect in March 2018, databases will be classified into four categories: Individual-Managed Databases, Basic Security Databases, Intermediate Security Databases, and High Security Databases. Classification is determined primarily by the number of individuals who have access to the database, the number of individuals whose personal information is contained in the database, and the types and the sensitivity of the information that the database contains. The regulations impose the fewest obligations on Individual-Managed Databases and the most obligations on High Security Databases.

The following are some of the new requirements:

- **Specification manual and security procedures.** Each database owner must draft and annually update a specification manual that describes his or her database's contents and objectives, processing mechanisms, cross-border transfer practices, and third-party access, as well as a document, binding on all the owner's employees, outlining the security practices applicable to the database.
- **Data minimization**. Each database owner must annually evaluate whether his or her database contains more information than is necessary to achieve the objectives set forth in the database's specification manual.
- **Risk assessment/penetration testing.** Each owner of a High Security Database must conduct a comprehensive risk assessment with respect to and penetration testing of such database at least once every 18 months.
- **Authentication and Monitoring.** For Intermediate and High Security Databases, access must be authenticated by means of a physical token and automatically monitored by a system that identifies the user accessing the database, the time and date of access, and the information retrieved and/or processed.
- **Security Officer**. The regulations expand on the current requirement under the Israeli Law that certain companies retain a qualified Security Officer. The regulations impose seniority standards and conflict-of-interest rules specifying, among other things, that the Security Officer must be directly subordinate to the individual manager or owner of the database.

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 applies; 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, 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 encryp-

  PVLR ISSN 1538-3423

tion 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

Law no. (13) of 2016 on the Protection of Personal Data (Qatar Law) was enacted in December 2016 and became effective in January 2017. The Qatar Law applies to personal information that is electronically processed or obtained, collected, or extracted by any other means in preparation for electronic processing by controllers, processors, and website operators. Personal information is defined as data of a person whose identity is determined or can be reasonably determined, whether by these data or by collecting them with any other data.

Prior to the enactment of the national law, only organizations licensed to operate in the Qatar Financial Centre (QFC) were subject to data privacy rules. 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.

In Brief *The Qatar Law restricts cross-border transfers in cases where the processing would violate the Qatar Law or harm the privacy of individuals. Notification is required in the event of a data security breach and a permit is required to process sensitive personal information. Registration and the appointment of a DPO, however, are not required.*

Special Characteristics

Data Protection Authority The Minister of Transport and Communications (DPA) is responsible for issuing the decrees necessary to implement the provisions of the Qatar Law.

Collection and Use A controller must not process any personal information, unless the controller obtains the individual's consent or where the processing is necessary for the legitimate purpose of the controller or the other party to whom the data will be sent or an exception applies. Sensitive personal information may only be processed after obtaining a permit from the competent department according to the procedures and controls to be set forth in a ministerial decree.

Cross-Border Transfers A controller must not make any decision or take an action that may reduce the trans border flow of personal information unless the processing of the information violates the provisions of the Qatar Law or would cause a serious harm to the personal information or the privacy of an individual.

Data Security Breach Notification The controller must notify an individual and the competent department of any breach if it may cause serious harm to the personal information privacy of said individual. The processor must notify the controller of any breach or any threat to an individual's personal information as soon as the processor becomes aware of the breach or threat. The Qatar Law does not prescribe what information must be contained in the notice to affected individuals and when notice must be provided.

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) regulates the processing of all personal information of natural persons. The Seychelles Law was enacted in 2002 but has never entered into force.

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; however, it will only commence on a date to be proclaimed by the president. 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 Information Regulator (DPA), established in December 2016, will be responsible for enforcement of the law when the South African Law enters into force.

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, a 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, 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

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 and amended in 2012. 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. The DIFC Law regulates the processing of all personal information by controllers.

In addition, private sector organizations that are licensed to operate in the Abu Dhabi Global Market (ADGM), a financial free zone in Abu Dhabi, are subject to the ADGM Data Protection Regulations (ADGM Regulations). The ADGM Regulations, issued in 2015, regulate the processing of personal information by controllers and processors.

In Brief *The DIFC Law and the ADGM Regulations restrict cross-border transfers to countries that do not provide adequate protection, require registration, and*

  PVLR ISSN 1538-3423

impose 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; the ADGM Registration Authority (DPA) is responsible for enforcement of the ADGM Regulation.

Cross-Border Transfers Personal information may not be transferred to countries outside the DIFC or ADGM 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 in the DIFC and ADGM must notify the DPA. Notice to individuals is not legally required.

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

BY CYNTHIA RICH

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

Links to all of the data privacy laws and DPAs discussed in this article are available in Morrison & Foerster's online Privacy Library at http://src.bna.com/sjr.