Bloomberg BNA

Privacy and Security Law Report®

Data Protection

Privacy Laws in Africa and the Middle East

By Cynthia Rich

Introduction/Region at-a-Glance

The privacy landscape in Africa and the Middle East, which has already changed remarkably in the past few years alone, may be on the verge of another transformation after the adoption in June 2014 of the African Union (AU) Convention on cybersecurity and data protection. The number of countries in the region may multiply far beyond the 18 countries that already have comprehensive privacy laws regulating the collection and use of personal information by the private sector. Currently 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 have such laws in place. Other countries, such as Kenya, Tanzania and Uganda, are working on developing privacy legislation. Now with the adoption of the AU Convention, which still must be ratified by 15 of the 54 member states, more countries in Africa may adopt laws to implement the AU Convention's comprehensive (and European Union-like) privacy framework.

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.

Many of the existing regimes in the region are still in their formative stages, in large part because the regulators are not yet in place; 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/Middle Eastern Laws

Notice: All of the laws in Africa and the Middle 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 Africa 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 Middle 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 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 Middle 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 Israel DPA has imposed fines for law violations. The amount of the fines were not disclosed, however. The violations pertained to such things as the failure to provide notice, comply with the direct mail provisions of Israel's framework privacy law, employ adequate data security measures and comply with the requirements for outsourcing.

In some of the newer and less mature regimes, where there are established DPAs, the authorities generally are focusing on building awareness about the rules and educating organizations about their compliance obligations.

In some of the newer and less mature regimes, where there are established DPAs, the authorities generally are focusing on building awareness about the rules and educating organizations about their compliance obligations. There have been very few reports of enforcement actions or initiatives; however, DPAs in countries such as Morocco, Senegal and the United Arab Emirates are stepping up their enforcement efforts. In January 2014, the Moroccan DPA announced its intention to audit websites that primarily use personal data to drive their content. In particular, it planned to focus on sites offering online sales, the buying and selling of advertisements, job vacancies and hotel rooms to determine whether such websites treat personal data in accordance with the principles of the law and have notified the DPA of their processing activities. During this same period, the Senegal DPA announced the official commencement of compliance activities and enforcement under its data protection law and called on data controllers to take the steps necessary to comply with the law. The DPA for the Dubai International Financial Centre in the United Arab Emirates reported that it issued 11 monetary fines to organization in 2013 and 14 in 2014 (through November) 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.

The situation in Senegal illustrates the challenges that many countries with newly enacted laws in the re-

  PVLR ISSN 1538-3423

gion face. Senegal's data protection law went into effect in 2008, but it was not until 2011 that the DPA was established and not until 2013 that a budget for the agency was finally approved. The registration process did not begin until January 2014, six years after the law went into effect.

Privacy Legislation Under Development

In September 2014, the Kenyan government announced that its Cabinet had approved a data privacy law. The Data Protection Bill, which has not yet been approved by the Parliament, 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. There are no registration or data breach notification requirements. Individuals may lodge complaints about personal data processing with the Commission on Administrative Justice, the organization designated to oversee implementation and enforcement of the act. Violations are punishable by fines up to 100,000 shillings (approximately $1,030) and/or imprisonment up to 2 years.

In late 2014, Uganda's Ministry of Information and Communications Technology (ICT), in conjunction with the Ministry of Justice and Constitutional Affairs (MoJCA) and the National Information Technology Authority, Uganda (NITA-U), launched a public consultation on a draft Data Protection and Privacy Bill. The bill, which applies to both the public and private sectors, would impose the full range of data privacy obligations such as notice, consent, access and correction and data security. In addition, the proposed law would impose data breach notification and database registration obligations.[1]

Tanzania is also reportedly working on data protection legislation; however, no draft texts have been made public.

While it will likely be a few years before the AU Convention is ratified, it may spur more countries in the region to begin work on developing privacy laws modeled after it.

AU Convention

Although the AU Convention on Cyberspace Security and Protection of Personal Data[2] 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 (14 PVLR 148, 1/26/15). 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.

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.[3]

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.''

[1] The Uganda bill is available at http://www.nita.go.ug/sites/default/files/publications/Draft%20Data%20Protection%20and%20PrivacyBill%20-%20Revised%20PDF.pdf.

[2] The AU Convention is available at http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf.

[3] The Angolan Law is available, in Portuguese, at http://www.mwe.com/info/pubs/Law_22_11_Data_Privacy_Law.pdf.

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.[4] 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.[5]

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.[6]

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.[7]

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.[8]

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 healthcare 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.

---

[4] The Law on Electronic Communications and Information Society Services is available, in Portuguese, at http://portalinacom.tecangol.com/Portals/0/Legislacao/lei_23_11.pdf.

[5] The Benin Law is available at http://www.cnilbenin.bj/images/Texte/Loi%20No%202009%20du%2022Mai%202009%20Version%20Anglaise.pdf.

[6] The website of the Benin DPA is at http://www.cnilbenin.bj.

[7] The Burkina Faso Law is available, in French, at http://www.afapdp.org/wp-content/uploads/2012/01/Burkina-Faso-Loi-portant-protection-des-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel-20042.pdf.

[8] The website of the Burkina Faso DPA is at http://www.cil.bf.

  PVLR ISSN 1538-3423

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.[9]

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; however, the DPA has not been established yet.

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. The registration process is not yet operative, pending the establishment of the DPA.

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.[10]

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. The Data Protection Authority (DPA) is responsible for enforcement of the Cote D'Ivoire Law.[11]

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 orga-

[9] The Cape Verde Law is available, in Portuguese, at http://www.dgap.com.cv/phocadownload/regime%20de%20incompatibilidade%20dos%20aposentados.pdf.

[10] The Cote D'Ivoire Law is available, in French, at http://www.mofo.com/files/PrivacyLibrary/3979/Cote-d-voire-loi_2013_450.pdf.

[11] The website of the Cote D'Ivoire DPA is at http://www.artci.ci/index.php/protection-des-donnees/Protections-des-donnees.

nization 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.

In Cote D'Ivoire, an organization must put in place appropriate mechanisms to ensure the respect of the "right to be forgotten" in a digital context.

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.[12] 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.

[12] The Gabon Law is available, in French, at http://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-%C3%A0-la-protection-des-donn%C3%A9es-personnelles-du-4-mai-20112.pdf.

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, un-

  PVLR ISSN 1538-3423

less 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 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.

The Ghana Law is one of the few data protection laws around the world that contains a carve-out for outsourcing.

GHANA

The Data Protection Act (Act 843) (Ghana Law), enacted in May 2012 (11 PVLR 1276, 8/13/12), regulates the processing of all personal information of natural persons by both the public and private sector organizations.[13] 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 (13 PVLR 1744, 10/6/14), is responsible for enforcement of the Ghana Law.[14] 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.

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.[15] 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 (10 PVLR 179, 2/7/11).

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.[16]

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.

[13] The Ghana Law is available at http://www.mofo.com/files/PrivacyLibrary/3981/GHANAbill.pdf.

[14] The website of the Ghana DPA is at http://www.dataprotection.org.gh.

[15] The Israeli Law is available at http://www.justice.gov.il/NR/rdonlyres/B11D19EE-7FC0-42ED-B2F5-2B4FDEE66BD4/18334/ProtectionofPrivacyLaw57411981unofficialtranslation.pdf.

[16] The website of the Israeli DPA is at http://old.justice.gov.il/MOJHeb/ILITA.

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.[17]

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.

[17] The Madagascar Law is available, in French, at http://www.afapdp.org/wp-content/uploads/2015/01/Madagascar-L-2014-038-du-09-01-15-sur-la-protection-des-donn%C3%A9es-%C3%A0-caract%C3%A8re-personnel.pdf.

MALI

Law no. 2013/015 on the Protection of Personal Data (Mali Law) was adopted in May 2013.[18] 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 Mali Law provides for the establishment of an independent regulator, the Authority for the Protection of Personal Data (DPA), which will be responsible for enforcement of the Mali Law; however, the DPA is not yet established. As of May 2015, the DPA has not yet been established.

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.[19]

In Brief. *The Mauritius Law restricts cross-border transfers to countries that do not provide adequate protection and requires registration. However, there is no*

[18] The Mali Law is available, in French, at http://www.afapdp.org/wp-content/uploads/2012/01/Mali-Loi-sur-la-protection-des-donn%C3%A9es-personnelles-du-21-mai-2013.pdf .

[19] The Mauritius Law is available at http://www.mofo.com/docs/mofoprivacy/DP%20Law.pdf.

  PVLR ISSN 1538-3423

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.[20] 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.[21]

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.[22]

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 (8 PVLR 563, 4/13/09), regulates the processing of all personal information of natural persons by both the public and private sectors.[23]

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.*

[20] The website of the Mauritius DPA is at http://dataprotection.govmu.org/English/Pages/default.aspx.

[21] The Guidelines on Privacy Impact Assessments are available at http://op.bna.com/pl.nsf/r?Open=kjon-9xep8s.

[22] The Guidelines for Handling Privacy Breaches are available at http://op.bna.com/pl.nsf/r?Open=kjon-9xep9m.

[23] The Moroccan Law is available, in French, at http://www.mofo.com/docs/mofoprivacy/Morocco_DP_Law_French.pdf.

Special Characteristics

Data Protection Authority. The National Supervisory Authority (DPA) is responsible for supervising compliance with the Moroccan Law.[24]

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, including the U.S.-EU Safe Harbor Program, 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.

The government of Qatar is currently working on comprehensive data privacy legislation.

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.[25] 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 government of Qatar is currently working on comprehensive data privacy legislation. A public con-

[24] The website of the Morocco DPA is at http://www.cndp.ma.

[25] The QFC Regulations are available at http://www.complinet.com/file_store/pdf/rulebooks/QFCRA_1559.pdf.

sultation was held in 2011, but a law has not yet been enacted.

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.[26]

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.[27]

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.[28]

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.[29]

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 (12 PVLR 2053, 12/9/13); however, it will only commence on a date to be proclaimed by the president.[30] It is unknown when that will happen, but the expectation is that it will be in about six months. 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.

[26] The website of the QFC Authority is at http://www.qfc.com.qa/en-US/Home.aspx.

[27] The Senegal Law is available, in French, at http://www.centif.sn/loi_caractere_personnel.pdf.

[28] The website of the Senegal DPA is at http://www.cdp.sn/index.html.

[29] The Seychelles Law is not available online.

[30] The South African Law is available at http://www.mofo.com/files/PrivacyLibrary/3789/Protection-of-Personal-Information-Act-4-of-2013.pdf.

  PVLR ISSN 1538-3423

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 (3 PVLR 1030, 9/6/04), regulates the processing of all personal information of natural persons by both the public and private sectors.[31]

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.[32]

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 (6 PVLR 171, 1/29/07) and amended in 2012.[33] 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 restricts cross-border transfers to countries that do not provide adequate protection, requires registration and imposes data security breach notification obligations.

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.[34]

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.

[31] The Tunisian Law is available, in French, at http://www.inpdp.nat.tn/version-francaise/textes/L_2004_63-1.pdf.

[32] The website of the Tunisian DPA is at http://www.inpdp.nat.tn.

[33] The DIFC Law is available at http://difc.complinet.com/net_file_store/new_rulebooks/d/i/DIFC_9227.pdf.

[34] The website address for the DIFC DPA is http://dp.difc.ae.

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.

COUNTRIES WITH PRIVACY LAWS	REGISTRATION REQUIREMENT	DPO REQUIRED [1]	CROSS-BORDER LIMITATIONS	DATA 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.

  PVLR ISSN 1538-3423