Bloomberg BNA

Privacy and Security Law Report®



**Data Protection**

In this third article of a three-part series on the status of data privacy laws in Latin America, the Caribbean, Asia, Africa and the Middle East, the author explores developments in Africa and the Middle East, where 17 countries in the region now have comprehensive privacy laws.

# Privacy Laws in Africa and the Middle East

BY CYNTHIA RICH

Once considered a privacy free-for-all, Africa and the Middle East have radically transformed their privacy regimes over the past few years. A critical mass of 17 countries in the region now have comprehensive privacy laws that regulate the collection and use of personal information by the private sector. Almost half these laws are either new or recently amended in the past three years.

While these laws impose many privacy obligations similar to those found in Europe, Latin America and Asia, the reality is that there are 17 different registration and 16 different cross-border rules and procedures. Moreover, only half of these countries permit personal information to be processed on the basis of a balance of interest exception. Two countries require breach notification, and one has voluntary procedures. Many of these regimes 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.

*Cynthia Rich is a senior policy analyst 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.*

## Implications for Business

Sorting through this wide array of laws raises questions about what these requirements mean for organizations in practical terms. The slow pace at which several of these countries are proceeding to establish data protection authorities (DPAs) and issue implementing regulations makes the process all the more challenging. Organizations doing business in Africa and the Middle East should pay attention to these laws because, while many of the substantive obligations are similar to those found in laws in other regions, the legal bases for collection and use and the practices and procedures for cross-border authorizations and database registrations vary. Moreover, in almost all of these countries, there are criminal and civil penalties for privacy law violations. Companies should examine their existing practices and begin to modify their privacy practices in these jurisdictions.

## Overview

The following provides an overview of the 17 countries in the region that have enacted data privacy laws. Because the laws in these countries impose the traditional data privacy obligations such as notice, choice, access and correction, security and data integrity, this discussion focuses solely on the key requirements that

 ISSN 1538-3423

are likely to impact an organization's global and regional compliance efforts. With the exception of Ghana and South Africa as noted below, there is no obligation elsewhere in the region to give notice to individuals or regulators in the event of a data breach.

## 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.[1] The Angolan Law imposes the full range of data privacy obligations. Consent or another legal basis is required to collect and use personal information; exceptions include when the processing is necessary to complete the contract, comply with a legal requirement or pursue the legitimate interests of the organization or the third parties to whom the information is disclosed (in European Union parlance this is referred to as ''a balance of interest'' exception). In addition, database registration and prior authorization of cross-border transfers to countries outside Angola that do not provide adequate protection are required; however, the DPA has not yet been established so these two obligations are not yet in effect.

## 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.[2] There are no specific legal bases for processing set forth in the Benin Law other than a general requirement that personal information be collected and used for specific, legitimate and nonfraudulent purposes as described in the notice. Individuals have the right to object to the processing of their personal information. Explicit consent or an exception is required to process sensitive information.

Registration of databases with the DPA is required unless the organization appoints a person to maintain a registry of the processing activities. Prior authorization is also required to process biometric data and transfer personal information to countries outside Benin, including those that guarantee a sufficient level of privacy protection. Transfers based on contractual clauses or internal rules also require authorization.

## 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.[3] Consent or another legal basis is required to collect and use personal information; there are exceptions for processing necessary to complete the contract or comply with a legal requirement, but there is no balance of interest exception.

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. Specific DPA authorization is not required for cross-border transfers, but such transfers must be included in the prior registration with the DPA.

## CAPE VERDE

The Law on Protection of Personal Data (Cape Verde Law), enacted in 2001 and amended in 2013, regulates the processing of all personal information of natural persons by both the public and private sectors.[4] Organizations must comply immediately with the amended law, particularly the access, correction, deletion and blocking requirements. Consent or another legal basis is required to collect and use personal information; exceptions include when the processing is necessary to pursue the legitimate interests, complete the contract or comply with a legal requirement.

**Organizations must comply immediately with the amended Cape Verde Law, particularly the access, correction, deletion and blocking requirements.**

Registration of data processing and prior authorization of cross-border transfers to countries that do not provide adequate protection are required. The deadline to register was Dec. 17, 2013, and the deadline for full compliance with the Cape Verde Law was March 17, 2014; however, as of the beginning of this year, the DPA had not yet been established.

## COTE D'IVOIRE

Law No. 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.[5] Consent or another legal basis is required to collect and use personal information; there are exceptions for processing necessary to complete the contract or comply with a legal requirement, but there is no balance of interest exception.

The Cote D'Ivoire Law provides for the establishment of a DPA and requires database registration and authorizations for cross-border transfers. Organizations must register all processing of personal information with the DPA prior to the commencement of processing, unless a data protection officer (DPO) has been appointed or another exception applies. However, even if a DPO is appointed, prior authorization is still required to transfer personal information to third countries. The Cote D'Ivoire Law provides for a six-month transition period to comply with these requirements.

## GABON

Law No. 001/2011 on the Protection of Personal Data (Gabon Law), enacted in 2011, regulates the processing

[1] The Angolan Law is available at http://www.mwe.com/info/pubs/Law_22_11_Data_Privacy_Law.pdf.

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

[3] The Burkina Faso Law is available 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.

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

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

  PVLR ISSN 1538-3423

of all personal information of natural persons by both the public and private sectors.[6] The DPA was established in November 2012. Consent or another legal basis is required to collect and use personal information; exceptions include when the processing is necessary to pursue the legitimate interests, complete the contract or comply with a legal requirement.

Organizations must register processing with the DPA for all data and all purposes unless a DPO has been appointed or another exception applies; however, the DPO exemption does not apply where cross-border transfers of personal information are planned. Organizations may only transfer personal information to a foreign country with prior DPA authorization or provided an exception applies. Prior DPA authorization is also required to process sensitive and genetic information.

## GHANA

The Data Protection Act, 2012 (Act 843) (Ghana Law) was enacted in May 2012, and a Data Protection Commission was established in November 2012.[7] Consent or another legal basis is required to collect and use personal information; exceptions include when the processing is necessary to pursue the legitimate interests, complete the contract or comply with a legal requirement. All processing must be registered with the DPA, but there are no limitations on or prior DPA authorization requirements for cross-border transfers. The recipients and countries to which personal information is intended to be transferred must be listed in the organization's database registration, and individuals must be informed about any recipients to whom their personal information may be transferred in the privacy notice provided at the time of data collection. In addition, there is an obligation to inform individuals and the regulator in the event of a data breach. Ghana was the first African country to include a breach notification obligation in its law.

**Ghana was the first African country to include a breach notification obligation in its 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.[8] The Israeli Law does not expressly require that there be a legal basis for processing personal information. Consent is generally not required to collect, use and disclose personal information within Israel provided it is for the purpose for which it was provided by the individual. To transfer to third parties outside Israel, however, consent or another legal basis is required unless the transfer is to affiliates that are under the corporate control of the Israeli company. There are also comprehensive security rules that include specific requirements for outsourcing activities.

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. Prior authorization of cross-border transfers is not required. 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 data transferred from the EU/European Economic Area (10 PVLR 179, 2/7/11). The DPA has increased its level of supervision and enforcement in recent years, particularly following the EU's adequacy determination.

## MALI

Law No. 2013/015 on the Protection of Personal Data (Mali Law) was adopted in May 2013.[9] It regulates the processing of all personal information of natural persons by both the public and private sectors. The Mali Law does not contain any explicit consent requirements for processing nonsensitive personal information except when it is for direct marketing purposes. Individuals do have the right to oppose processing of their personal information for legitimate reasons. There is also a general prohibition on processing sensitive information unless the individual provides his or her consent.

The Mali Law provides for the establishment of a DPA (which has not yet been established) and requires database registration and prior authorization for transfers of personal information to countries that do not provide an adequate level of protection.

## 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.[10] Express consent or another legal basis is required to collect and use personal information; there are exceptions for processing necessary to complete the contract or comply with a legal requirement, but there is no balance of interest exception. However, the DPA has issued guidance that warns organizations to be cautious about relying on consent as a basis for data transfers or contract necessity as a legal basis for the transfer of employee data within a multinational company.

While there are no mandatory breach notification obligations, the DPA has issued guidelines which include a voluntary notification procedure in the event of a security breach. In addition, the DPA has published detailed guidelines on security practices and privacy impact assessments.[11] Databases must be registered, and written DPA authorization is required to transfer personal information to countries outside Mauritius.

---

[6] The Gabon Law is available at http://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-?-la-protection-des-donn?es-personnelles-du-4-mai-20112.pdf.

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

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

[9] The Mali Law is available at http://www.mofo.com/files/PrivacyLibrary/3959/Mali-Loi-sur-la-protection-des-donnees-personnelles-du-21-mai-2013.pdf.

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

[11] The ''Guidelines for Handling Privacy Breaches'' are available at http://dataprotection.gov.mu/English/Documents/Publications/Guidelines/Guidvol4v3.pdf. The ''Guidelines on Privacy Impact Assessments'' are available at http://dataprotection.gov.mu/English/Documents/Publications/Guidelines/DPO_Vol6_PrivacyImpactAssessment.pdf.

## 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.[12] Consent or another legal basis is required to collect and use personal information; exceptions include when the processing is necessary to pursue the legitimate interests, complete the contract or comply with a legal requirement. Unless an exception applies or processing is otherwise provided for by law, organizations must register all partially or wholly automatic processing of personal information with the DPA and obtain the necessary prior authorizations where required (e.g., to process sensitive, genetic or health information or transfer information across borders). 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 Law. Transfers to inadequate countries are prohibited unless an exception applies.

According to the DPA, organizations also have the obligation to ensure through contractual means and compliance audits that their data processors comply with security requirements. The DPA has issued template language that organizations may use in their contracts with data processors.

In January 2014, the DPA announced its intention to expand its enforcement efforts by auditing websites, particularly those that buy, sell and advertise online.

## QATAR/QATAR FINANCIAL CENTRE AUTHORITY

Financial services organizations licensed by the Qatar Financial Centre Authority (QFC Authority) in Doha, Qatar, are subject to the Data Protection Regulations 2005 (QFC Regulations) that regulate their processing of the personal information of natural persons.[13] Consent or another legal basis is required to collect and use personal information; exceptions include when the processing is necessary to pursue the legitimate interests, complete the contract or comply with a legal requirement. Organizations must register with the QFC Authority prior to or immediately upon processing any personal information. A permit is also required to process sensitive information. 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 consented to the transfer or another exception applies. Alternatively, organizations may apply to the QFC Authority for a permit for the transfer. The government of Qatar is currently working on comprehensive data privacy legislation. A public consultation was held in 2011, but a law has not yet been enacted.

## 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.[14] Consent or another legal basis is required to collect and use personal information; there are exceptions for processing necessary to complete the contract or comply with a legal requirement, but there is no balance of interest exception.

Organizations must register all automatic processing of personal information with the DPA unless an exception applies. In addition to registration, certain processing requires DPA authorization, such as where data are transferred to countries that do not provide adequate protection or where certain types of data such as sensitive or genetic data are 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.[15] The Seychelles Law does not prescribe legal bases for the processing of personal information but simply requires that personal information be processed fairly, lawfully and only for specified purposes. Processing must be registered with the DPA, and the DPA has the power to prohibit cross-border transfers if it believes such transfers will violate the data protection principles under the Seychelles Law. Directors are liable for offenses committed by their organizations.

## SOUTH AFRICA

South Africa is the most recent country in the region to approve a comprehensive data privacy law. The 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.[16] 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.

**South Africa is now the second country in Africa that has adopted a breach notification requirement.**

The South African Law regulates the processing of all personal information of natural and legal persons by both the public and private sectors. Consent or another legal basis is required to collect and use personal information; exceptions include when the processing is necessary to pursue the legitimate interests, complete the contract or comply with a legal requirement. In the event of a security breach, the organization 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.

[12] The Moroccan Law is available at http://www.mofo.com/docs/mofoprivacy/Morocco_DP_Law_French.pdf.

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

[14] The Senegal Law is available at http://www.cdp.sn/images/doc/protection.pdf.

[15] The Seychelles Law is not available online.

[16] 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

South Africa is now the second country in Africa that has adopted a breach notification requirement.

The South African Law provides for the establishment of a DPA and 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 or 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

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.[17] Consent or another legal basis is required to collect and use personal information; there are exceptions for processing necessary to complete the contract or comply with a legal requirement, but there is no balance of interest exception.

The Tunisian Law provides for two kinds of registrations: notifications that are applicable to all kind of data and authorizations that are applicable to sensitive data. 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 that do not provide an adequate level of protection.

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

## UNITED ARAB EMIRATES/DUBAI INTERNATIONAL FINANCIAL CENTER

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.[18] The DIFC is a federal financial free zone established in 2004 for the conduct of financial services. It has its own civil and commercial laws, court system, judges and financial regulator, separate from the United Arab Emirates.

The DIFC Law, enforced by a DPA, regulates the processing of all personal information of natural persons. Consent or another legal basis is required to collect and use personal information; exceptions include when the processing is necessary to pursue the legitimate interests, complete the contract or comply with a legal requirement. Database registration is required, and personal information may not be transferred to countries outside the DIFC unless an adequate level of protection is ensured by laws and regulations applicable to the recipients or an exception applies. 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 DIFC. DPA authorization or the individual's consent to the transfer to an inadequate transfers are two of the exceptions provided under the DIFC Law.

[18] The DIFC Law is available at http://difc.ae/sites/default/files/dp-reg.pdf.