AN A.S. PRATT PUBLICATION
APRIL 2021
VOL. 7 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 3** **April 2021**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [69] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2021–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Out of Africa (and the Near East): Privacy Rules Come at Rapid Pace

By Cynthia J. Rich*

This article discusses some of the commonalities and differences among the privacy regimes in Africa and the Near East and identifies the jurisdictions that are likely to enact new or amended laws in the next few years.

Countries in Africa and the Near East have been enacting data privacy laws at a dizzying pace over the past several years, far exceeding the pace in other regions of the world such as Asia and the Americas. In the past decade, 24 laws were enacted in this region; 14 of these were just in the past five years. In comparison, 13 new laws in Asia and 21 in the Americas were enacted in this same 10-year period. All indications are that the region's privacy rules will continue to grow at a rapid pace into 2021 and beyond. Enforcement is also likely to increase in the region as more countries establish their data protection authorities and these privacy regimes begin to mature.

This region has some very distinct characteristics that set it apart from other regions of the world, particularly with respect to cross-border transfer and registration requirements. Contrary to the trend around the world to minimize registration requirements, most of the laws in this region require organizations to register processing activities with a data protection authority ("DPA)." Moreover, with its diverse array of the cross-border rules, this region's data privacy landscape is akin to the Wild West.

The explosion of new and disparate laws in this region in such a relatively short period of time, coupled with the fact that almost one-third of these jurisdictions have not yet established their DPAs, makes it challenging for companies to develop their regional privacy compliance approaches, let alone integrate them into their global compliance programs. Nonetheless, it is important to take these differences into account when developing privacy compliance programs.

This article discusses some of the commonalities and differences among the privacy regimes in the region and identifies the jurisdictions that are likely to enact new or amended laws in the next few years.

* Cynthia J. Rich is a senior privacy advisor in the Washington, D.C., office of Morrison & Foerster LLP. As a member of the firm's international Privacy and Data Security Practice, Ms. Rich works with clients on legal issues relating to privacy and transborder data transfers around the world. She may be contacted at crich@mofo.com.

CHARACTERISTICS OF THE CURRENT REGIONAL LANDSCAPE: COMMONALITIES AND DIFFERENCES

Thirty-four jurisdictions in the region now have comprehensive privacy laws.[1] More than two-thirds of these laws (24) were enacted within the past decade and, of these, 14 were enacted in the past five years. The newest laws are in the Republic of the Congo, Egypt, Kenya, Nigeria, Togo, and Uganda. In addition, the existing laws in Benin, Mauritius, and the UAE (DIFC and ADGM) were amended within the past three years.

While they share the same core data protection elements, all of these laws have specific rules that are very different from each other and from those in other regions. However, implementing data privacy programs to comply with these rules can be challenging, particularly in those jurisdictions that have yet to establish their DPAs.[2]

Scope

Most of the laws in this region apply to processing in-country only. However, three have extraterritorial provisions: Benin, Qatar, and Uganda. Benin's law applies to processing by controllers or processors in Benin, whether or not the processing takes place in or outside Benin. It also applies to controllers and processors not established in Benin that process personal information of people in Benin where these processing activities relate to:

- The offering of goods or services to people in Benin, whether or not whether or not they are required to pay;
- The monitoring of behavior of individuals, insofar as this behavior takes place in Benin; or
- Processing that takes place in a member state of the Economic Community of West African States ("ECOWAS").

Qatar's law applies to processing by controllers, processors, and website operators and Uganda's law applies to organizations within Uganda that process personal information or organizations outside Uganda that process personal information relating to Ugandan citizens.

---

[1] These jurisdictions are Algeria, Angola, Bahrain, Benin, Botswana, Burkina Faso, Cape Verde, Chad, Republic of the Congo, Côte d'Ivoire, Egypt, Equatorial Guinea, Gabon, Ghana, Guinea, Israel, Kenya, Lesotho, Madagascar, Mali, Mauritania, Mauritius, Morocco, Niger, Nigeria, Qatar, São Tomé & Principe, Senegal, Seychelles, South Africa, Togo, Tunisia, Uganda, and the United Arab Emirates (in two free trade zones – the Dubai International Financial Centre ("DIFC") and the Abu Dhabi Global Market ("ADGM")). The Mauritanian law has not yet entered into force. An implementing decree must be issued in order to bring the law into force. In addition, the law in Seychelles is not in force.

[2] The jurisdictions are Algeria, Bahrain, Botswana, Republic of the Congo, Egypt, Equatorial Guinea, Lesotho, Madagascar, Mauritania, and Togo.

Cross-Border Transfers

While most of the jurisdictions (31) impose restrictions on cross-border transfers for personal data, there is such a diverse array of rules that it is practically impossible to characterize them in meaningful ways.[3]

Adequacy

Twenty-nine of these 31 countries permit transfers to countries that provide adequate protection; however, most (24) have not issued their lists of adequate countries. Of the five that have, their lists vary widely. For example:

- The Côte d'Ivoire recognizes the member states of ECOWAS;[4]
- Chad recognizes the member states of the Central African Economic and Monetary Community ("CEMAC") and the Economic Community of Central African States ("CEEAC");[5]
- Lesotho recognizes member states that have transposed the Southern African Development Community ("SADC") data protection requirements;[6]
- Morocco recognizes the EEA Member States and Canada; and
- The UAE/DIFC and ADGM recognize the EEA Member States as well as other jurisdictions recognized by the EU as providing adequate protection.

In order to transfer to an adequate country, eight of these 29 countries additionally require DPA authorization, notification, or a DPA license: Benin, Republic of the Congo, Egypt, Guinea, Morocco, Senegal, Togo, and Tunisia. Two of these countries, the Republic of the Congo and Togo, have not yet established DPAs.

Adequate Protection Measures

Twenty-two of the 29 countries permit transfers where adequate protection measures are in place, such as contractual clauses, but in many cases the DPAs must also approve the transfers and/or contractual clauses. Only a couple of DPAs (in the UAE/DIFC and

[3] The laws in Ghana, Qatar, and Seychelles do not restrict cross-border transfers of personal data.

[4] The ECOWAS member states are Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo.

[5] 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, Chad, Republic of the Congo, Democratic Republic of the Congo, Gabon, Equatorial Guinea, and São Tomé & Principe.

[6] The SADC Member States are Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia, and Zimbabwe.

ADGM free trade zones) have issued their own clauses. Alternatively, Israel permits the use of EU Standard Contractual Clauses with minor modifications.

Legal Bases

All but a few laws permit transfers to inadequate countries provided one of the legal bases specified in the law applies. However, these legal bases vary widely. Some provide for one or more legal bases such as consent, contractual necessity, vital interests, and/or a legal claim; some only permit such transfers on the basis of consent while others limit the use of consent to transfers are that limited and specific. Many laws also require DPA authorization for such transfers. In contrast, laws in countries such Burkina Faso, Côte d'Ivoire, Guinea, Niger, and Tunisia do not provide any legal bases other than DPA authorization.

Breach Notification

More than one-third of the laws (14) require notification in the event of a data breach.[7] Five of the jurisdictions do not require notice to be given to individuals and/or the DPA where there is no risk of harm from the breach. The other nine jurisdictions require notification to the DPA in the event of any data security breach. While many of the laws only require that notice be provided to individuals and/or to the DPA "as soon as practicable" or "without delay," others (Republic of the Congo, Egypt, Mauritius, and the UAE/ADGM) require notification to the DPA within 72 hours. Most require that both individuals and the DPA must be notified about a breach.

Legal Bases for Processing

Almost half of the laws (16) do not permit processing on the basis of legitimate interests. Instead, the laws rely on other legal bases such as consent, contractual necessity, legal requirements, or vital interests. Only two countries, Israel and Mali, do not expressly require a legal basis for processing. Instead, they specify that processing for purposes other than those for which the information was provided constitutes a violation of privacy.

[7] Benin, Botswana, Chad, Republic of the Congo, Egypt, Ghana, Israel, Kenya, Lesotho, Mauritius, Qatar, South Africa, Uganda, and the United Arab Emirates (DIFC and ADGM).

Individual Rights

Access and correction rights must be provided in all countries. More than two-thirds of the laws (24) provide erasure rights and one-quarter (eight) provide data portability rights. The timeframes for responding to individual rights requests also vary widely: 12 countries require responses to rights requests within 30 days or more; two within 21 days; eight within 10-15 days; and one within six days. Ten do not specify a specific time period.

Data Protection Officer ("DPO")

More than one-quarter of the jurisdictions (10) require the appointment of a DPO: Benin, Republic of the Congo, Egypt, Madagascar, Mauritius, Nigeria, South Africa, Tunisia, Uganda, and the UAE/DIFC.

Registration

While the trend around the world is to minimize registration requirements, most of the laws in the region (31) require organizations to register processing activities with a DPA. The countries that do not impose registration requirements are the Republic of the Congo, Nigeria, and Qatar.

Security

Slightly more than half of the countries (18) have either some specific or very detailed security provisions. The countries with detailed security obligations are Benin, Israel, Senegal, and the UAE/DIFC. Three countries, Benin, Côte d'Ivoire, and Nigeria require the submission of security compliance or audit reports annually to the DPA.

Data Protection Impact Assessments ("DPIAs")

Most laws in the region do not require organizations to carry out DPIAs. DPIAs are required only in Benin, Republic of the Congo, Israel, Kenya, Mauritius, South Africa, and the UAE/DIFC.

Enforcement

With the entry into force of several new laws in the past two years and the recent establishment of DPAs in Kenya and Uganda with more likely to follow in the coming year or so, enforcement activity in the region is likely to increase. The DPAs in Benin, Ghana, Israel, Mali, Mauritius, Morocco, Senegal, and Tunisia have been the most active; the DPAs in Nigeria and South Africa are also likely to join that list soon. In the past year, the Nigerian DPA began issuing non-compliance notices to organizations that failed to submit their required data protection audits. In South Africa, the DPA has been established for a couple of years but enforcement of the data privacy law does not begin until July 1, 2021.

RECENTLY ENACTED PRIVACY LAWS

The following provides a brief snapshot of recently enacted laws:

Bahrain

Bahrain's Personal Data Protection Law,[8] entered into effect on August 1, 2019. The DPA is not yet established; however, the Ministry of Justice has temporarily assumed its functions and powers until an independent authority is allocated a budget and a board of directors is established.

Republic of the Congo

Law No. 29-2019 on protection of personal data[9] went into effect in November 2019; compliance by private sector organizations was required by November 2020. The DPA is not yet established.

Egypt

The Personal Data Protection Law, No. 151 of 2020 entered into force on October 14, 2020; compliance is required one year after executive regulations are issued. Those regulations are expected to be issued by April 14, 2021. A DPA has not yet been established.

Kenya

The Data Protection Act, 2019,[10] went into effect in November 2019; however, the data protection commissioner was only recently appointed in November 2020.

Nigeria

The Data Protection Regulation 2019[11] ("Regulation") was issued by the National Information Technology Development Agency ("NITDA") in January 2019. NITDA subsequently issued a draft Data Protection Implementation Framework for the Regulation which it encouraged companies to use as a compliance guide until a final text is issued. The final text has yet to be issued in final form. In the meantime, as

---

[8] Law No. 30 of 2018, https://www.bahrain.bh/wps/wcm/connect/40f1a510-96fb-40ba-b65d-a795c91d10b6/%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%B1%D9%82%D9%85+%2830%29+%D9%84%D8%B3%D9%86%D8%A9+2018+%D8%A8%D8%A7%D9%95%D8%B5%D8%AF%D8%A7%D8%B1+%D9%82%D8%A7%D9%86%D9%88%D9%86+%D8%AD%D9%85%D8%A7%D9%8A%D8%A9+%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA+%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9.pdf?MOD=AJPERES.

[9] http://www.sgg.cg/JO/2019/congo-jo-2019-45.pdf.

[10] http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf.

[11] https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf.

discussed below, efforts are now underway to develop a new and more comprehensive data protection law.

South Africa

Although it was enacted in 2013, South Africa's Protection of Personal Information Act[12] only entered into force on July 1, 2020. Organizations have been given until July 1, 2021 to comply with the law. The DPA has been operational since 2016.

Togo

The Law on Protection of Personal Data[13] went into effect October 2019 with enforcement to began in October 2020; however, the DPA is not yet established.

Uganda

Uganda's Data Protection and Privacy Act, 2019[14] was enacted in February 2019 and entered into force in February 2020. However, the necessary implementing regulations have not yet been issued. The Ministry of ICT and National Guidance released for public comment Draft Data Protection and Privacy Regulations 2020[15] ("Draft Regulations") which address, among other things, the provisions pertaining to the registration, security breach notification, and DPO requirements. The law provides for the creation of a data protection office within the National Information Technology Authority; however, there is no indication at this time that this office has been established.

UAE

In the DIFC, a new data protection law, Law No. 5 of 2020,[16] took effect on July 1, 2020, replacing the 2007 DIFC data protection law. In response to the pandemic, the government announced that businesses subject to the law would be given a three-month grace period, until October 1, 2020, to come into compliance with the law. While the law generally follows the EU's General Data Protection Regulation ("GDPR"), there are some notable differences in provisions regarding, for example, consent, individual rights, registration, and security breach notification.

The ADGM also enacted new data protection regulations in February 2021. The ADGM Data Protection Regulations 2021 ("Regulations") repeals the ADGM's current Data Protection Regulations, issued in 2015. The new Regulations align the

[12] https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf.

[13] https://jo.gouv.tg/sites/default/files/JO/JOS_29_10_2019-64E%20ANNEE-N%C2%B026%20TER.pdf#page=1.

[14] https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf.

[15] https://www.nita.go.ug/publication/draft-data-protection-and-privacy-regulations-2019.

[16] https://www.difc.ae/files/6215/9056/5113/Data_Protection_Law_DIFC_Law_No._5_of_2020.pdf.

ADGM's data privacy requirements with those of the GDPR and are similar to the new DIFC data protection Law.

NEW LAWS EXPECTED IN 2021 AND BEYOND

Anticipated Amendments to Existing Laws

Israel

Almost 40 years after the enactment of Israel's Protection of Privacy Law, 5741-1981,[17] the Israeli Ministry of Justice announced in 2020 its plans to update the law to take into account new technological developments. It held a consultation in December 2020 to solicit input from the public on the ways in which the law should be amended. In addition, efforts to improve and update the DPA's supervisory and enforcement capabilities have been underway since 2018.

Developments in Countries with No Privacy Laws

In the next couple of years, we expect to see more new laws enacted, possibly in Jordan, Namibia, Nigeria, Saudi Arabia, Zambia, and Zimbabwe:

Jordan

The Ministry of Digital Economy and Entrepreneurship submitted its draft data protection bill to the Council of Ministers and, in January 2020, the bill was published on the Bureau of Legislation and Opinion website. If enacted, the bill would, among other things, establish general data protection principles, require legal bases for processing personal data, provide for individual rights, including the right to be forgotten and data portability, impose 72-hour breach notification requirements, and restrict cross-border transfers of personal data to countries that provide adequate protection rules. The DPA would be established within the Ministry of Digital Economy and Entrepreneurship.

Namibia

The Ministry of Information and Communication Technology ("MICT") is reportedly working on draft data protection legislation. In February 2020, the Ministry participated in a workshop on drafting data protection legislation co-sponsored by the Council of Europe.

Nigeria

The Nigerian government has drafted data protection legislation, the Data Protection Bill, 2020,[18] which is expected to be introduced in the National Assembly. Unlike virtually

[17] http://www.wipo.int/wipolex/en/text.jsp?file_id=347462.

[18] https://www.ncc.gov.ng/documents/911-data-protection-bill-draft-2020/file.

all other laws enacted around the world, this proposed law would regulate personal data of individuals and legal entities (both public and private). Moreover, it would apply to processing by controllers established in Nigeria, controllers not established in Nigeria that use equipment in Nigeria to process personal data, as well as controllers (without regard to their establishment) that carry out processing of information relating to individuals who reside within or outside Nigeria and personal data which originates partly or wholly from Nigeria.

Like other laws, this legislation establishes basic principles and legal bases (such as legitimate interests, contractual necessity, and consent) for processing of personal data, provides for individual rights, including erasure and data portability rights, and imposes security requirements including specific obligations on data processors. In addition, it imposes restrictions on cross-border transfers and requires the submission of annual audit reports and notification of data breaches within 48 hours. Lastly, it provides for the establishment of a Data Protection Commission and imposes criminal penalties for law violations.

Saudi Arabia

Saudi Arabia's National Data Management Office ("NDMO"), the entity responsible for data governance in the Kingdom, has recently issued National Data Governance Interim Regulations[19] ("Interim Regulations") but their legal status (whether they are mandatory regulations or voluntary guidance) remains unclear. The Interim Regulations address areas such as data classification, data sharing, and data privacy, in anticipation of further rules or legislation in this area.

The data privacy-related provisions, among other things, impose data localization requirements that require controllers to store and process personal data within the country unless the controllers obtain written prior approval from the regulatory authorities, and require consent to process personal data in most instances and notifications of data breaches within 72 hours.

Zambia

Zambia's National Assembly is considering the Data Protection Bill, 2020, which currently is undergoing a second reading. The Data Protection Bill includes general data protection principles and individuals' rights similar to the GDPR. In addition, the bill proposes:

- Data localization for cross-border transfers, by requiring a controller to process and store personal data on a server or data center located in Zambia;

[19] https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf.

- Data breach notification, requiring controllers to notify the Zambia Information Communications and Technology Authority within 24 hours of any security breach affecting personal data processed. The controller or processor would also be required to notify the affected individuals, as soon as practicable;
- Registration requirements for controllers and processors; and
- Appointment of a data protection officer ("DPO"), which must be done in accordance with guidelines issued by the DPA.

Zambia's National Assembly also is considering the Cyber Security and Cyber Crimes Bill, 2020, which is undergoing a first reading. This bill would, among other things, establish offenses pertaining to, for example, unauthorized access to a computer system and data. In cases where a person intentionally accesses or intercepts any data without authority or permission to do so or who exceeds the authorized access could be liable to a fine and/or to imprisonment.

Zimbabwe

The Cyber Security and Data Protection Bill[20] is currently pending in Parliament. There were public hearings and a consultation on the proposed legislation last year and the legislature is expected to proceed with legislation in 2021. The bill has been controversial, largely with respect to provisions that would criminalize certain forms of online speech and activity. Critics have charged that these provisions would undermine the freedom of expression and freedom of the media. With respect to the data protection-related provisions, the bill establishes general rules for the processing of personal data, including sensitive data such as genetic, biometric, and health data, and would impose notice, consent, and breach notification requirements.

[20] http://www.veritaszim.net/sites/veritas_d/files/Cyber%20Security%20and%20Data%20Protection%20Bill.pdf.