University of New South Wales Law Research Series

DATA PRIVACY LAWS AND BILLS: GROWTH IN AFRICA, GDPR INFLUENCE

GRAHAM GREENLEAF AND BERTIL COTTIER

(2018) 152 *Privacy Laws & Business International Report* 11
[2018] *UNSWLRS* 52

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Data privacy laws and bills: Growth in Africa, GDPR influence

Graham Greenleaf & Bertil Cottier*

(2018) 152 *Privacy Laws & Business International Report* , 11-13

By early 2017, the number of countries with data privacy laws had risen to 120.[1] A year later, this has increased to 124 countries (although some of the laws concerned were enacted in 2016). At least five more countries also introduced during 2017 new official data privacy bills into their legislative processes. Reforms of some existing data privacy laws ('2nd generation laws') are also underway. Engagement with international data privacy agreements has also increased. This article surveys those developments, with some observations concerning any effects that the EU's GDPR is having outside Europe in relation to this recent legislation.

Four new countries with data privacy laws

The laws additional to those in the 2017 survey are from the Cayman Islands, from three West African countries – Mauritania, Niger, and Guinea-Conakry.

Cayman Islands (Data Protection Law 2017, Law 33 of 2017)[2] The Caymans are an autonomous British Overseas Territory in the western Caribbean (south of Cuba), comprising three islands of 264 square kilometres with a population of about 63,000. 'The territory has never levied income tax, capital gains tax, or any wealth tax, making them a popular tax haven.'[3] Enacted in March 2017, the Act is expected to commence in January 2019, and will assist the financial services industry to continue access to the EU market. It is comprehensive in scope, applying to all sectors and all types of personal data. Among the Act's provisions which go beyond the minimum required for a data privacy law are the following: special protections for categories of sensitive data; data exports restricted to where there is an adequate level of protection; 'opt-out' from direct marketing; right to reconsideration of significant decisions made solely by automatic means; right to stop processing (with some exceptions); and data breach notification (DBN) obligations to both the Commissioner and data subjects. Breach of any provision of the Act by a data controller gives a person affected a right of action for compensation before the courts. The Information Commissioner (IC) has legislated independence, powers to make orders in relation to processing operations, responsibilities for international cooperation and giving effect to international obligations, and powers to levy administrative fines where serious breaches cause substantial damage or

* Graham Greenleaf is Professor of Law & Information Systems, UNSW Australia and PL&B Asia Pacific Editor, and Bertil Cottier is Professor of Communication Law, Università della Svizzera Italiana, and Associate Professor of Law, University of Lausanne, Switzerland. Valuable information has been received from Dhiraphol Suwanprateep, David Duncan, Mohamad Lo, Smitha Prasad, Marie Georges, Sophie Kwasny and Dave Banisar, but all content remains solely the responsibility of the authors.

[1] Greenleaf, G 'Global data privacy laws 2017: 120 national data privacy laws now include Indonesia and Turkey' (2017) 145 *Privacy Laws & Business International Report,* 10-13.

[2] http://www.infocomm.ky/images/DataProtectionLaw2017.pdf

[3] Wikipedia: Cayman Islands: History.

distress to data subjects. Significant court-imposed criminal penalties can result from failure to comply with IC orders. The IC's Office states that it 'seeks compliance with' the EU GDPR.[4]

This is one of the strongest data privacy laws yet enacted in the Caribbean.

Draft Data Protection Regulations are currently open for consultation.[5]

Mauritania (Loi 2017-020 sur la protection des données à caractère personnel) and **Niger** (Loi 2017-28 relative à la protection des données à caractère personnel) are two West African countries, which are plagued by ailing economies and attacks by Islamic extremist militias. In 2017 they nevertheless enacted full-fledged data protection laws, applicable to the public and the private sectors. Both legal texts transpose into domestic law the Supplementary Act on Personal Data Protection of the Economic Community of West African States (ECOWAS) (Niger is a full member of ECOWAS, Mauritania an associated one). Thus, both laws are quite similar, particularly because both legislatures simply copied and pasted many relevant provisions of the Supplementary Act, such as the mandatory declaration of data processing; the authorization for sensitive data files; the right of access; and the principles guiding processing of personal data, as well as the list of exceptions thereto. As the Supplementary Act dates back to 2010, both legislatures introduced only a few novelties; most of them influenced by the European General Data Protection Regulation (GDPR), like the principle of minimization of data, more strict requisites regarding the consent of the data subject and the right to be forgotten. Still, rules on portability of data and data security breach notification are missing; the same goes for privacy by design and/or by default obligations; and, to a certain extent, for the institution of an in-house Data Protection Officer (indeed the law of Niger mentions this institution, but its role remains minimal compared to EU law). Worth noting, the Mauritanian act imposes relations between the data processor and the date controller to be governed by a written contract defining clearly each party's respective obligations and responsibilities. To ensure compliance with data protection rules, both Mauritania and Niger rely on independent National Data Protection Authorities vested with extensive and seemingly effective enforcing powers. However, neither the Mauritanian "Autorité de protection des données" nor its Nigeran counterpart have been established so far.

Guinea-Conakry (Republic of Guinea, formerly French Guinea) (Loi L/2016/037/AN relative à la cyber-sécurité et la protection des données à caractère personnel) is a Western African country still recovering from decades of tough dictatorship. It is also a member of ECOWAS. Accordingly its law on data protection (the final chapter of a law primarily dedicated to cybercrime and cybersecurity) fully implements the 2010 Supplementary Act in terms of processing of data, rights of the data subject or authorization for sensitive data files. Moreover, Guinea adopted the same innovations, modeled on the European GDPR, as Mauritania and Niger. In addition, private organizations and businesses must appoint an internal Data Protection Officer, whose profile and salary are to be defined by the National Data Protection Authority (so far no instructions on that matter have been issued, as the Guinean DPA has not yet been established). The most striking feature of the Guinean regime is the unprecedented severity of the penalties sanctioning violation of its provisions, quite often involving prison terms (up to twenty years in case of unlawful processing of sensitive data!).

---

[4] Information Commissioner's Office (Cayman Islands) *Data Protection Law, 2017 – Summary Sheet* <http://www.infocomm.ky/data-protection>

[5] The Data Protection Regulations, 2018 (Consultation Draft) <http://www.gov.ky/portal/pls/portal/docs/1/12634375.PDF>

All three laws adhere closely to the provisions of the ECOWAS Final Act (and the GDPR) in providing that their DPAs can issue 'pecuniary sanctions' (fines) against data controllers. However, as in most civil law countries, data subjects would have to proceed in the courts, under the Civil Code, to obtain compensation for harms.

In addition, the small African country the **Union of the Comoros**[6] may have enacted a data privacy law in 2016, but no copy has been obtainable. Comoros is already a signatory to the African Union Convention on cybercrime and data protection, and all other AU Conventions.

Revised laws outside Europe with GDPR influences

EU countries are busy aligning their laws with the GDPR, but some revisions of laws outside Europe within the last two years have included some elements similar to the GDPR. For example, **Mauritius** updated its 2004 law on 22 December 2017, and the new Data Protection Act 2017 (Act No. 20 of 2017) in one of Africa's dynamic but small economies has many elements going beyond minimum requirements. Those reflecting the EU Directive include legislated independence of the Data Protection Office (DPO); prior checking of proposals involving automated decisions or data linkage likely to adversely affect privacy; minimal collection; automatic destruction upon completion of purpose; special protections for sensitive data; restrictions on decisions made by automated processing; opt-out from direct marketing; and use of equipment in Mauritius, or carrying out processing through an establishment in Mauritius brings a business within the Act. Elements which reflect additional EU GDPR requirements include the need to demonstrate compliance (accountability); notification of data breaches (DBN) to the DPO and in high risk cases to the data subject; data protection impact assessments (DPIA); and the right to object to processing. Data exports are subject to prior proof to the DPO of 'appropriate safeguards', and other tests. Other elements detract from the Act's modernity. It still requires compulsory registration of processors, now a rather old-fashioned idea. An extremely weak aspect is that most of the Act's provisions are only enforceable by criminal fines of up to US$1,500, and the DPO has no power to issue administrative fines. There are no provisions for data subjects to seek compensation, either from the DPO or a court. There is also a significant carve-out from the Act of all transfers of data between government bodies.

New Bills globally reflect GDPR

Thailand has a new Personal Data Privacy Bill,[7] which will extend its law to the private sector, replacing a former 2015 draft. Public hearings were held in early 2018. New elements in the Bill are seen as reflecting the GDPR, and particularly its extra-territorial implications for Thai businesses.[8] It creates a DPA (the Personal Information Protection Committee – PIPC) but one with very weak independence from government. The PIPC is empowered to prescribe data protection practices generally, and to determine the criteria for allowed data exports. The Bill includes many standard elements of data privacy law, but is unusual in the degree of discretionary control the DPA has over basic privacy rules. Some elements of the Bill reflecting GDPR influence include direct obligations on processors; data breach notification (DBN) requirements (both to data subjects and to the PIPC); right to withdraw consent to

[6] Union of the Comoros is a group of islands north of Madagascar in east Africa with a population of a little over one million. France claims the island of Mayotte as its territory, but this is disputed by the African Union.

[7] The Bill in Thai is at < http://www.lawamendment.go.th/index.php/laws-independent-entity/item/1187-2018-01-22-04-05-29>.

[8] D. Suwanprateep 'Update: Public Hearing on the Thai Personal Data Protection Bill, Including New Provisions on Data Processing and Legitimate Interest' Baker & McKenzie Client Alert <https://www.bakermckenzie.com/en/insight/publications/2018/01/public-hearing-thai-pdp-bill/>.

processing; PIPC authority to determine fines and penalties; and civil liability of controllers to pay compensation for any damage.

The reform Bill in the process of passage in **Tunisia**, as yet only available in Arabic, is intended to fully implement the GDPR, and the government has expressed its intention that it will come into force on the same date in May as the GDPR. **Bhutan's** revised *Bhutan Information Communications and Media Act,*[9] which when enacted will include a data privacy law,[10] has as yet only passed the lower house.[11] At least four more countries – **Jamaica, Algeria, Zambia and Egypt** – also have new official data privacy bills for new laws under consideration, bringing the number of countries known to have such Bills to 33.

Engagement with international agreements

There has also been increased participation in international data privacy agreements. While there has been a good deal of recent attention to Asian countries (Singapore, Korea, Taiwan, Philippines, Australia, Taiwan) claiming they will participate in APEC's Cross-border Privacy Rules system (CBPRs), it is still the case that only US companies are currently accredited (the one accredited Japanese company failed to re-accredit), so the rest is 'wait and see'. Japan and Korea are seeking positive EU adequacy assessments. Meanwhile, Council of Europe Convention 108 now has 51 parties, four from outside Europe. Tunisia completed accession in the past year, joining Uruguay, Mauritius and Senegal. Requests to accede by Argentina, and Mexico have been accepted (joining those by Morocco, Burkina Faso, and Cape Verde), so Convention 108 is gaining strength in Latin America as well as in Africa. The African Union Cybercrime and Data Protection Convention also now has 11 signatories, although Senegal remains the only country to have deposited its instrument of ratification. And after 2017, ten countries have enacted laws to implement the 2010 ECOWAS Supplementary Act, quite a remarkable achievement for a sub-regional data privacy agreement.

Conclusions

Outside the EU, the area of most rapid current change in data privacy laws is Africa, but significant developments continue in Asia, the Caribbean and Latin America. Outside Europe, new laws, revised laws and Bills all demonstrate a significant level of adoption of standards that go beyond the '1st generation' OECD Guidelines, including not only the '2nd generation' 'European' standards associated with the 1995 EU Directive, but also to a surprising extent the '3rd generation' higher standards found in 2016 EU GDPR, even before it comes into force.

---

[9] Bhutan Information Communications and Media Bill, 2016 (Bhutan) <http://www.nab.gov.bt/assets/uploads/docs/bills/2016/FinalBICMAbill2016Eng.pdf>

[10] G. Greenleaf 'Privacy progress in South Asian (SAARC) States: Reasons for optimism' (2017) 149 *Privacy Laws & Business International Report*

[11] Sonam Yangdon 'Bhutan Information Communication and Media Bill passed in the NA' *The Bhutanese*, 10 June 2017 <http://thebhutanese.bt/bhutan-information-communication-and-media-bill-passed-in-the-na/>.