2020 ENDS A DECADE OF 62 NEW DATA PRIVACY LAWS

GRAHAM GREENLEAF AND BERTIL COTTIER

(2020) 163 *Privacy Laws & Business International Report,* 24-26
[2020] *UNSWLRS* 39

UNSW Law
UNSW Sydney NSW 2052 Australia

2020 ends a decade of 62 new data privacy laws

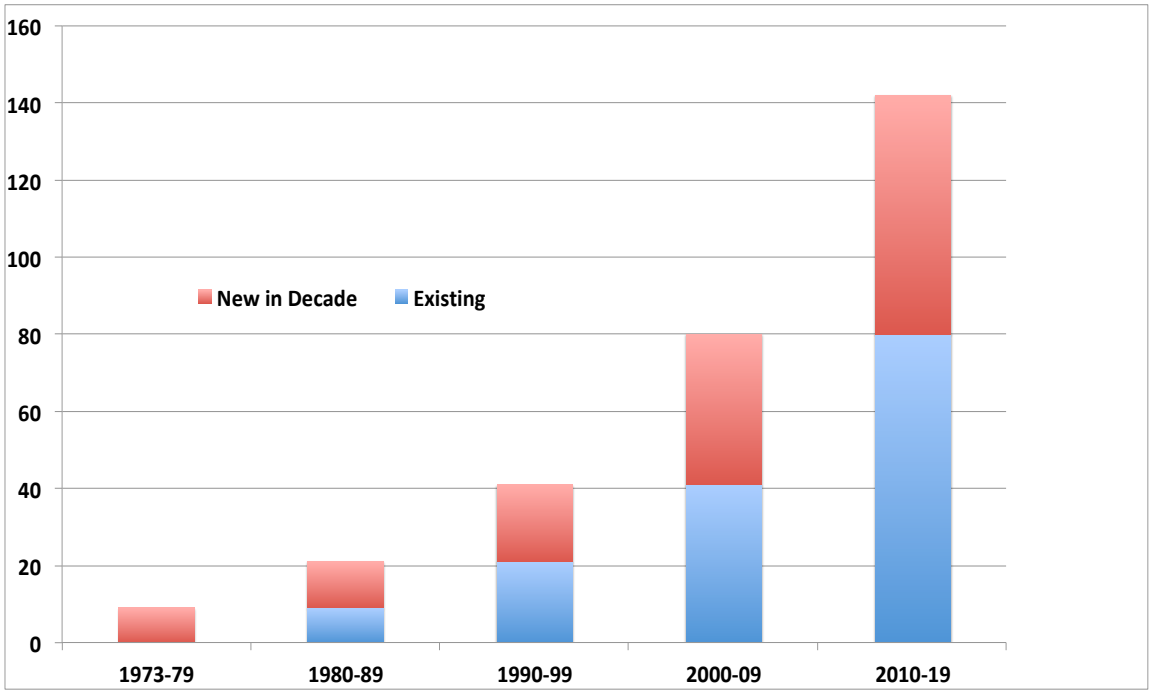
Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales &
Bertil Cottier, Professor of Law, Faculty of Communication Sciences, Università della Svizzera Italiana (Lugano) .

Published in (2020) 163 *Privacy Laws & Business International Report* 24-26

29 January 2020.

A record decade

The decade 2010-2019 has seen 62 new countries enacting data privacy laws, more than in any previous decade. The numbers of new countries with laws per decade are: 1970s – 10; 1980s – 10; 1990s – 20; 2000s – 40; 2010s – 62. This gives a total of 142 countries.



142 countries with data privacy laws by December 2019

By the end of the 2020s, if the current trajectory of enactment of new data privacy laws continues, there will be over 200 countries (including self-governing territories) with data privacy laws. What started as a novelty in one German State (Hesse) in 1970 will have covered the globe with its influence in sixty years.

Ten more countries with new laws, total 142

Since publication of the most recent *Global Tables of Data Privacy Laws* in January 2019,[1] which included 132 countries with such laws, a further ten laws have been enacted or located.

[1] Greenleaf, G. 'Global Tables of Data Privacy Laws and Bills (6th Ed January 2019)' (2019) Supplement to 157 *Privacy Laws & Business International Report* (PLBIR) 16 pgs <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380794>

They include six from Africa, three from Central Asia, and one from the Caribbean. Brief descriptions of each of these laws follow, now numbered #133 to #142.

#133. Barbados (Caribbean)

Barbados' *Data Protection Act, 2019*[2] is a complex Act, with comprehensive scope and some extra-territorial application. It establishes a Data Protection Commissioner, and Data Protection Tribunal. It is enforced by enforcement notices, administrative penalties (up to $50,000) and provisions for compensation. It includes many GDPR-influenced data protection principles, including rights to restrict or prevent processing, erasure (including the 'right to be forgotten', data portability, notification, and limits on automated decision-making. Lawful processing is defined, with more restrictive conditions for processing of sensitive data. Data controllers and processors must be registered, comply with data protection by design and default, notify data breaches to the Commissioner and the data subject, conduct data protection impact assessments, and appoint data privacy officers. Data exports are only allowed to jurisdictions where the is an adequate level of protection, or where defined forms of appropriate safeguards apply, or there is a 'public interest' order. Overall, this is one of the most GDPR-influenced data privacy laws outside the EU. However, there are numerous exemptions, including for data which is required to be made public, for manual data held by public authorities, and some unusual exemptions related to financial instruments.

#134. Botswana (Africa)

Botswana's *Data Protection Act, 2018*[3] is comprehensive but with limited exemptions for some State functions. It establishes an Information and Data Protection Commission, with a Commissioner and Deputy Commissioner. The Commission's independence is limited by the Minister's ability to give general or specific directions consistent with the Act. The Act sets out criteria for lawful processing, and prevents processing of sensitive data (including genetic and biometric data), with exceptions. Data subject rights are limited largely to access and correction. Data controller obligations include data breach notification to the Commission, notification to the Commission of automated processing operations, and appointment of a 'data protection representative' (DPO). Enforcement powers are limited to enforcement notices by the Commission, or fines upon prosecution for any processing contravening the Act, plus a right of data subjects to institute an action for damages in the courts for any such contravening processing. Transfers of personal data to other countries are prohibited, unless to a country on a white-list made by Ministerial Order, or to a country which the Commissioner has determined provides 'an adequate level of protection'. Other exceptions are provided from transfers made under adequate safeguards. The Act will come into force when gazetted.

#135. Congo-Brazzaville (Republic of Congo) (Africa)

Adopted the same month (October) as the Law of Togo, the Law of Congo-Brazzaville (*Loi 29-2019 portant protection des données à caractère personnel*)[4] is very similar to its Togolese neighbor (though the Republic of Congo is not a member of ECOWAS). The principles governing data processing (except for the finality principle, which, strangely, has been omitted), the rights of the data subject and the obligations of the data controller are all substantially the same; in addition, both laws are deprived of any extra-territorial scope. Nonetheless, there are two major differences. First, the Congolese law leans more towards the GDPR as it not only provides for data portability and data breach notification, but establishes

[2] *Data Protection Act, 2019* (Barbados) < https://www.barbadosparliament.com/bills/details/417>

[3] *Data Protection Act, 2018* (Botswana) <https://www.bocra.org.bw/data-protection-act>

[4] Congo-Brazzaville's law is at <http://www.worldlii.org/int/other/NDPrivLegis/toc-C.html>

a specific regime for the process of data concerning a minor (reinforced by an obligation for the data processor to provide him or her concise and easily understandable information. Secondly, the law of Congo Brazzaville does not institute any national Data Protection Authority, but anticipates it will be established by separate legislation in the near future.

#136. Kenya (Africa)

Kenya's *Data Protection Act, 2019*[5] emerged from lengthy debate and competing Bills as one of the most progressive English-language data privacy laws in Africa, with many GDPR influences. It creates a Data Commissioner who is required to act independently, and has other indicia of independence such as appointment approved by the legislature. Its scope is comprehensive of all sectors, but with few extra-territorial extensions. Exemptions are limited, but the Commissioner can prescribe new exemptions. There is Register of data controllers and processors (above prescribed thresholds of activity), an approach still common in Africa but not in most other regions. The obligations of controllers, similar to the GDPR, include the prohibition of processing except on specified lawful grounds; data protection impact assessments (DPIAs) prior to potentially high risk processing; restrictions on processing required on various grounds; limits on making decisions by automated processing; to implement data protection by design and default; and to notify the Commissioner and data subject of data breaches. Rights of data subjects include a variety of grounds on which to object to processing, or request deletion of data, and data portability. Data exports are only allowed where necessary for various reasons (including 'compelling legitimate interests'), or the Commissioner has been given proof of appropriate safeguards. Export of sensitive data also requires consent. 'Data localisation' may be achieved by the government prescribing that certain processing may only take place through servers or data centres located in Kenya. Enforcement provisions are relatively weak, including enforcement orders arising from complaints, and penalty notices to a maximum of US$50,000, or 1% or turnover, whichever is less. Data subjects are entitled to seek compensation in a court, for damage arising from processing in breach of the Act.

#137. Nigeria (Africa)

Made pursuant to the *Nigerian Information Technology Development Agency Act* of 2007, Nigeria's *Data Protection Regulation 2019* is a basic data privacy law which has previously been analysed here.[6] The Regulation may eventually be replaced by a stand-alone primary law. The President has refused to sign into law the Digital Rights and Freedom Bill, originally passed in 2018, and forwarded again to him by the legislature in November 2019.[7]

#138. Tajikistan (Central Asia)

Tajikistan's *Law on Protection of Personnel Data* of 3 August 2018 (No.1537)[8] is supported by a constitutional data protection provision. It is a comprehensive law (all sectors), designating the 'Communication Service' as the DPA with a minimal set of responsibilities, but 'state bodies' have parallel powers in their sectors. Data subject rights cover essential elements of a data privacy law only. Enforcement provisions include small administrative fines for security breaches, and some criminal offences but little else. Data exports are only to countries with

---

[5] *Data Protection Act, 2019* (Kenya) <http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019>

[6] G. Greenleaf, 'Nigeria Regulates Data Privacy: African and Global Significance' (2019) 158 *Privacy Laws & Business International Report*, 23-25.

[7] 'CSOs, Nigerians Urge President Buhari To Sign Digital Rights Bill' MSN Africa, 2 November 2019 <https://www.msn.com/en-xl/africa/top-stories/csos-nigerians-urge-president-buhari-to-sign-digital-rights-bill/ar-BBTqRoX>

[8] Tajikistan's law is available in Tajik <http://base.mmk.tj/view_sanadhoview.php?showdetail=&sanadID=609> and Russian < http://base.mmk.tj/view_sanadhoview.php?showdetail=&sanadID=609&language=ru>.

'adequate' protection, plus some common exceptions. There are no data localisation provisions.

#139. Togo (Africa)

Togo's law of nearly hundred articles (*Loi 2019-014 relative à la protection des données à caractère personnel*[9]), chiefly implements the 2010 *Supplementary Act on Personal Data Protection* of the Economic Community of West African States (ECOWAS). Togo is one of ECOWAS' founding members, and its legislators have very often just copied and pasted relevant provisions of the Supplementary Act, such as with the principles relating to processing of data (and the exceptions thereto), the mandatory declaration of data processing, the authorization for sensitive data files and the right of access. The legislator has introduced a few post-2010 novelties influenced by the GDPR, like stricter requirements regarding the consent of the data subject, the institution of an in-house Data Protection Officer (DPO) and, to a certain extent, the right to be forgotten. Still, rules on data minimization, on portability of data, on impact assessments and on data security breach notification are missing, as are privacy by design and/or by default obligations.

#140. Turkmenistan (Central Asia)

Turkmenistan's *Law on Information on Private Life and its Protection* No. 519-V of 2017[10] is comprehensive (all sectors), but does not create a separate DPA, instead appointing the Cabinet of Ministers as the administering authority. It includes a basic set of data subject rights, plus additional rights of blocking and withdrawal of consent, but few more advanced rights or obligations. Enforcement is through modest levels of fines, or imprisonment, plus compensation for data subjects. Data exports are only permitted to states that ensure protection of the information, but there are no data localisation provisions.

#141. Uganda (Africa)

At first glance, the *Data Protection and Privacy Act 2019*[11] of Uganda looks like full-fledged modern legislation. Indeed, many provisions are drawn from the EU GDPR: the minimization principle, a mandatory data protection officer, the obligation to notify security breaches, and rigorous rules governing automated decisions. Some requirements go even beyond the GDPR, particularly the prohibition of sale of personal data, and the extended extraterritorial scope of the law to any processing of data about Ugandan citizen taking place abroad. Nonetheless, some important features of modern DP laws are ignored: no data portability rules, no privacy by design/default obligations, and no right to be forgotten. In addition, restrictions to transfers of data to third countries only target outsourcing of data processing or storage. Finally, the national data protection authority must keep a register of all persons, institutions or public bodies processing personal data; the file is public and has to mention the purpose for which personal data has been collected. Such registers are still common in Africa, but not elsewhere.

#142. Uzbekistan (Central Asia)

Uzbekistan's *Law on Personal Data* of 2019[12] is the most advanced data privacy law in Central Asia. Its scope is comprehensive. Most personal data databases require registration in a State Register. Data processing requires one of seven lawful justifications. Processing of sensitive

---

[9] For Togo's law, see <http://www.worldlii.org/int/other/NDPrivLegis/toc-T.html>.

[10] *Law on Information on Private Life and its Protection* (Turkmenistan) – Was available in Russian from the Ministry of Justice site <http://www.minjust.gov.tm/ru/>.

[11] *Data Protection and Privacy Act 2019* (Uganda) < https://ulii.org/ug/legislation/act/2019/1>

[12] *Law on Personal Data* of 2019 (Uzbekistan) – in English at <https://kostalegal.com/publications/download/59_e6d3157fcaa6702e8f4bfa2ad640058c>

data is prohibited, except for a list of exceptional cases, with even more restrictions on processing biometric or genetic data. Data subject rights are essentially similar to those found in the EU Data Protection Directive (DPD, not the GDPR), including restrictions on automated processing. The obligations on those processing personal data are similarly complex, but contain few if any of the new obligations in the GDPR. Data exports are only allowed to countries providing 'adequate protection', with a few exceptions. The Law creates an 'authorised state body' to deal with data protection, the State Center for Personalization, but it is 'under the Cabinet of Ministers', and so is not an independent DPA. It has powers to 'issue instructions to address violations', but there are no other explicit enforcement measures. Overall, this law is a 'second generation' data privacy law, equivalent to the DPD, but with weak enforcement.

GDPR influences vary across the globe

With three new laws, all Central Asian countries except Mongolia now have data privacy laws, because Kazakhstan and Kyrzygstan already have such laws. While most are minimal in their rights and obligations, that of Uzbekistan is much closer to a second-generation law. But none of these laws show significant influences of the GDPR. In contrast, the new Barbados law is the high-water mark of GDPR influence among Caribbean countries.

Enactments in six more African countries brings the total number with data privacy laws to 31 of the 55 African Union members. All of these laws show some GDPR influences, strongest in Kenya and Congo-Brazzaville, and weakest in Botswana. However, each country adopts specific and differing GDPR-like elements, rather than their being any uniform influence.

Information: Thanks to David Banisar for identifying some laws otherwise omitted, included in his map at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416