THE STAGING OF THE HIDDEN:JAMAICA ADOPTS A POST-GDPR DATA PRIVACY LAW

GRAHAM GREENLEAF

(2020) (167) Privacy Laws & Business International Report, 5-8
[2021] *UNSWLRS* 3

UNSW Law
UNSW Sydney NSW 2052 Australia

Jamaica adopts a post-GDPR data privacy law

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia
(2020) 167 *Privacy Laws & Business International Report* 1, 5-8.

Jamaica's Data Protection Act 2020[1], enacted on 19 May but not yet in force, provides for a transitional period of two years. The Jamaican Information Commissioner, once appointed, should be influential in the region, at least within the anglophone Caribbean.

There are now fifteen Caribbean data privacy laws: the Bahamas (2003), St Vincent & Grenadines (2003), BES Islands (the Netherlands municipalities of Bonaire, Sint Eustatius and Saba) (2010), Curaçao (2010), St Maartens (2010), Aruba (2011), St Lucia (2011), Trinidad & Tobago (2011), Dominican Republic (2013), Antigua & Barbuda (2013), Bermuda (2016), the Cayman Islands (2017), Saint Kitts & Nevis (2018), Barbados (2019), and Jamaica (2020).[2] Five jurisdictions' laws (Aruba, Curaçao, St Maartens, Trinidad & Tobago, and St Vincent & Grenadines) are not yet in force, despite being enacted in 2013 or earlier.

Appointments to data protection authorities under recent laws should result in ten DPAs in the region. There is as yet a low level of engagement between them. It is the only region of the world with a significant number of DPAs which does not have a regional association.

Scope and definitions

The Act comes into effect on a day appointed by the Minister, and gazetted, or different days for different provisions (s. 1(1)) or different categories of data (s. 1(2)). Data controllers must comply fully with the Act within two years of the earliest of those dates, and proceedings against them cannot be taken within that period for actions 'done in good faith' (s. 76).

Extra-territorial effect

The Act normally applies only to a data controller established in Jamaica (irrespective of where the data is processed) (s. 3(1)(a)). 'Established in Jamaica' has a broad definition (s. 3(3)). Data processors not established in Jamaica will be bound by the Act if they use equipment in Jamaica for processing (not just for transit), or process data of a data subject who is in Jamaica in order to offer products or services to data subjects in Jamaica, whether or not payment is required, or monitor behaviour of data subjects taking place in Jamaica (s. 3(1)(b)). Such processors must appoint a representative established in Jamaica (s. 3(2)). This extra-territorial jurisdiction is very similar to that under the EU GDPR, and is rapidly becoming the norm in post-GDPR legislation around the world.

Definitions

Definitions in section 2 clarify the scope of the Act, with broad and conventional definitions of 'data controller' (public and private sectors).. 'data processors', processing, 'data subject' (identifiability) and 'personal data'. Unusually, the definition of 'personal data' applies to those deceased for less than thirty years.

---

[1] Data Protection Act 2020 (Jamaica) <https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf>.

[2] For details of these laws, see G. Greenleaf 'Global Tables of Data Privacy Laws and Bills (6th Ed January 2019)' (2019) Supplement to 157 *Privacy Laws & Business International Report* (PLBIR) 16 pags <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380794> ; Barbados' 2019 law is additional (see Conclusions).

'Sensitive personal data' is defined to include all the usual categories (as for example in the GDPR), including 'genetic data or biometric data' (both also defined). Regulations by the Minister may 'provide additional safeguards' in relation to such data (s. 74(2)(a)). Criminal conviction records also gain additional protection but are not 'sensitive personal data'.

The Information Commissioner

The Act establishes the office of the Information Commissioner, to carry out functions assigned under both the *Data Protection Act* and the *Access to Information Act* (s. 4).

The Commissioner is to 'act independently' and 'shall not be subject to the direction or control of any person or other entity' (s 4(4)), except that s/he 'shall be subject to the oversight of the Data Protection Oversight Committee' (s. 4(10)). This seven person Committee is appointed by the Governor-General after bipartisan consultation, with the function of holding the Commissioner 'accountable to the public' in performance of her/his functions. Its functions are essentially to monitor the Commissioner's performance of functions, and give reports to Parliament (Part II, First Schedule). This does not diminish the Commissioner's independence.

The Commissioner has the full range of functions expected of a DPA, including monitoring compliance, broad powers to advise the Minister on protection of personal data, advising the public, prepare or require preparation of good practice guidelines, and encourage trade associations to develop self-regulatory codes (s. 4(5)). He/she also has the unusual power to 'intervene as a party in any proceedings before a court, in respect of any matter concerning the processing of personal data or the enforcement of any provision of this Act' (except prosecution for offences) (s. 4(11)).

Appeals against the Commissioner's, decisions are to the Appeal Tribunal (s. 70), a committee of five privacy experts (Fifth Schedule). However, appeals concerning an enforcement notice, assessment notice or information notice, are enforced in a Parish Court, with appeals to the Supreme Court (s. 53).

Obligations of controllers, rights of data subjects

All data controllers must comply with eight numbered 'Standards', one of which includes compliance with the various 'Rights of the Data Subjects'. The Act also imposes four types of higher obligations, above the 'Standards', on some controllers in relation to some processing.

Higher obligations concerning some processing

Registration Data controllers must not process personal data unless they register with the Commissioner. The Minister may make exempt (by Gazette notice) controllers, or processing, 'unlikely to prejudice the rights and freedoms of data subjects' (s. 15). All controllers must register details of all proposed processing (s. 16), including recording data exempted (s. 16(1)(c)), otherwise it must be provided to a data subject on request (s. 16(5)). The register is open to public inspection (s. 17).

Specified processing The Minister can specify categories 'specified processing' 'particularly likely (a) to cause substantial damage or substantial distress; or (b) to otherwise significantly prejudice the rights and freedoms of data subjects' (s. 19(1); s. 74(3)(c)). The Commissioner must decide if proposed processing details for registration refer to 'specified processing', and inform the controller whether or not the processing is likely to comply with the Act, within 30 days (during which the controller must not commence processing: see penalties below).

Data Protection Officers (DPOs) A wide range of controllers must appoint a DPO: public authorities; if processing sensitive data (including criminal convictions); processing personal data 'on a large scale'; or in a class prescribed by the Commissioner (s. 20(1) and (6)). DPOs must be qualified and able to act independently, monitoring the controller's compliance with the Act, reporting breaches to the controller and, if they are not rectified, reporting them to the Commissioner (s. 20(2)-(5)).

Data protection impact assessments (DPIAs) The Commissioner can require that particular classes of personal data, or controllers, must submit a DPIA report annually in respect of all personal data they control in light of the risks involved (s. 45(4)-(5)). The DPIA must detail the 'legitimate interests pursued', 'the necessity and proportionality of the processing', 'the risks to rights and freedoms of data subjects', and 'measures envisaged to address the risks' (s. 45(3)). The Commissioner, after evaluating the DPIA, can issue such directions as necessary to ensure compliance with the Act (s. 45(2)).

'Standard' obligations of controllers

Part V of the Act sets out eight numbered 'standards' for processing personal data, with which data controllers have a duty to comply, as well as with other provisions of Part V (s.21(1)). These duties include requirements to notify the Commissioner within 72 hours of becoming aware, of (a) any contravention of the standards, and (b) any security breach which does or may affect personal data (in other laws, known as 'data breach notification' (DBN) requirements) (s. 21(3)). Each data subject whose personal data is affected by the contravention of breach must also be notified (s. 21(5)). All such contraventions, breaches and failure to notify are also offences (s. 21(2)). These are very strong requirements, particular the requirement to notify both the Commissioner and the data subject of any breach of standards.

The eight standards, in summary, are as follows:

1. ***Conditions for legitimate processing*** (s. 22) Personal data must not be processed except fairly and lawfully, and unless (a) for ordinary personal data, at least one condition in section 23 is met; or (b) for sensitive personal data, at least one condition in section 24 is met. These conditions are similar to the GDPR's conditions for legitimate processing. They may be expanded by regulations, or by Ministerial orders.

2. ***Specified purposes – use and disclosure*** (s. 25) Personal data may not be further processed in any manner incompatible with the purposes for which it was obtained.

3. ***Data quality*** (s. 26) It must be adequate, relevant, and necessary, relative to purposes.

4. ***Accurate and up to date*** (s. 27) It must be accurate and, where necessary, kept up to date.

5. ***Limited retention*** (s. 28) It shall not be kept for longer than necessary for its purpose, and disposed of in accordance with regulations.

6. ***Compliance with rights of data subject*** (s. 29) 'Personal data shall be processed in accordance with the rights of data subjects' (see below). Contraventions are defined.

7. ***Security*** (s. 30) Appropriate technical and organisational measures are required, and some are specified. The Commissioner must be notified of any breaches. Controllers have responsibilities for processors.

8. ***International transfers*** (s. 31) Transfers to a State or territory outside of Jamaica is prohibited unless it 'ensures an adequate level of protection'. 'Adequacy' has a definition similar to that under the GDPR, and exceptions to it are similar to those in the GDPR. Transfers can be made subject to both contractual terms and adequate safeguards approved by the Commissioner. The Minister may prescribe circumstances under which transfers may and may not be taken to be 'necessary for reasons of substantial public interest.' The Minister may also prescribe those states and territories 'which shall be taken to have an adequate level of protection'. However, the Commissioner may make additional determinations in relation to such countries, by a notice.

Part V (ss. 33-45) includes numerous exemptions from the standards, or from the 'disclosure to data subject requirements'. The result is that the range of conduct exempt from this law is extensive, and perhaps excessive if a law such as the GDPR is used as a benchmark.

Rights of data subjects

Part II (ss. 5-13) sets out 'Rights of Data Subjects and Others', as follows:

- ***Access*** Individuals are entitled to free access to 'a description' of their personal data held, the purposes of processing, and recipients (s. 6(2)(b)). A prescribed fee is required for a copy of what is held, including its sources (s. 6(2)(c)(i)), usually in permanent form (s. 7). Material exempt from disclosure must be severed (s. 6(1)). The Minister can order exemptions necessary for the safeguarding of the interests of the data subject or others (s. 43(1)).

- ***Portability*** For a prescribed fee, 'data portability' is provided to another data controller, of a machine-readable copy of data supplied by the data subject, (s. 6(2)(c)(ii)).

- ***Automated processing rights*** Data subjects, for a prescribed fee, are to be informed of 'the logic involved in … decision-taking' where automated processing is for the purpose of evaluating matters relating to them, and 'likely to constitute the sole basis for any decision significantly affecting the individual' (s. 6(2)(d)). Data subjects are entitled to require that no such significant decisions are made about them, to be informed if such a decision has been made, and to require the data controller to reconsider the decision (s. 12). Together, these are close to GDPR article 22 in spirit.

- ***'Consent'*** is defined narrowly to mean 'any informed, specific, unequivocal, freely given, expression of will by which the data subject agrees to the processing of that data subject's personal data' (s. 9). This affects various other rights and obligations.

- ***Rights to limit processing*** Data subjects may object to processing if it causes substantial damage or distress, is incomplete or irrelevant in relation to its purpose (which may include the 'right to be forgotten'), is illegal, or involves data retained for longer than is lawful (s. 11(2)). However if processing is based on any of the grounds of legitimate processing of (non-sensitive) personal data (the first standard), or in cases specified by Ministerial order,[3] then the rights to limit processing do not apply (s. 11(3)).

- **Limits on direct marketing** Data controllers must obtain consent, except for existing customers, and allow opting out (s. 10).

[3] Pursuant to s. 74(3)(b); however, that section mis-states its purpose.

- ***Rights to correction*** Data subjects have the right to 'rectify any inaccuracy' (s. 13).

Enforcement

The Act's enforcement is based on three types of notices, which can then lead to offences, administrative penalties, or compensation.

Enforcement, assessment, and information notices

All notices served on controllers refer to compliance with 'the data protection standards', but the Sixth Standard means that breaches of most protections in the Act are included.

The Commissioner may issue an ***enforcement notice*** when a controller 'has contravened or is contravening' (but not 'is likely to contravene') 'any of the data protection standards' (s. 44(2)). The Commissioner has wide latitude in what an enforcement notice may require and specify (s. 44). Compliance is not required until the appeal period has expired, except where a 'matter of urgency' is specified (s. 44(8)-(9)).

Most data protection laws refer to data subjects making a 'complaint' to the data protection authority, but in Jamaica a data subject makes a 'request for assessment' by the Commissioner, who then decides whether it is 'likely or unlikely' that processing affecting the data subject is in breach of the Act (s. 46). The Commissioner may serve an ***'assessment notice'*** on the controller requiring various forms of assistance to determine this (s. 47(1)), which is then set out in an 'assessment report', including any consequent recommendations (s. 47(7)).

An ***'information notice'*** by the Commissioner is used, for example where the Commissioner has made recommendations for compliance in an assessment report under section 47(7), but is not certain that they have been followed.

There are very technical provisions for each type of notice concerning service, requirements of the notice, urgency, appeals etc. The Commissioner is even required to issue a code of practice for how assessment notices will be administered (s. 47(7)).

Fines, administrative penalties and compensation

'Dissuasive sanction' under Jamaica's Act are various and extensive, including criminal offences (with possible imprisonment), and very large turnover-based fines for companies, and compensation payments.

Offences may occur under many sections, including failure to comply with an enforcement notice (or assessment notice, or information notice), processing of data without or contrary to registration (s. 18, s. 19(5)), illegal sale or purchase of personal data (s. 61), various types of 'forced disclosure' related to convictions (s. 63), or breaching pseudonymisation or encryption of personal data without a prescribed defence (s. 30).

However, the most important offence is that of processing personal data in contravention of any of the data protection standards, or other provisions of Part IV (including data breach notification requirements), or failure to report such breaches to the Commissioner (s. 21(2)). This makes breach of one of the 'standards' an offence in itself, whether or not the Commissioner has issued an enforcement or other notice.

Maximum fines for these offences range from one million dollars (US$6,900) to five million dollars (US$34,500), upon conviction for summary offences by a Parish Court, with the alternative of imprisonment for up to five years (or up to ten years for conviction on

indictment in the Circuit Court). These maximum fines are now low by international standards, but in effect they only apply to individuals, not companies.

A company (or other body corporate) committing an offence is liable to a maximum fine up to four percent of its annual gross worldwide turnover for the preceding tax year, notwithstanding any other penalties specified (as above) (s. 68(1)). The court must take into account five factors in assessing such a fine: estimated economic cost to consumers (and other data subjects) of the contravention; estimated economic benefit to the controller; period the contravention continued; number and severity of other offences by the controller; and other factors the court considers relevant (s. 68(2)). Responsible company officers 'shall be liable, as well as the body corporate to be proceeded against and punished accordingly' (s. 68(3)). These provisions have obvious similarity to GDPR administrative penalties, particularly in being based on worldwide turnover, and in the factors to be considered. However, they are fines imposed by a court, not administrative penalties imposed by a DPA. It remains to be seen how courts will apply them. The Minister can amend any penalties imposed by the Act (s. 75).

For certain offences, if the Commissioner considers that a controller has committed the offence, and other conditions are satisfied (concerning intention, likely substantial damage etc) then she/he can offer to let the controller pay a fixed penalty set by the Commissioner, in order to avoid the prosecution continuing (s. 62). There are many complex conditions.

In addition, compensation is available, by court proceedings, whenever the Act's provisions are breached. 'An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage' (s. 69(1)). A controller has a defence if they can establish that they 'took all such care in all the circumstances as was reasonably required to comply with the requirement concerned' (s. 69(3)). This provision is important because it gives data subjects the right to initiate enforcement actions in the courts, and not be reliant on prosecutions by the Commissioner.

Conclusions

Jamaica's *The Data Protection Act, 2020* is a remarkably strong post-GDPR data privacy law. Of the nearly 20 features of the EU's GDPR that are relevant to countries outside the EU, and are stronger than the 1995 Data Protection Directive, only a handful are missing from explicit inclusion in this law: data protection by design and default; demonstrable accountability of controllers; direct liability for processors; requirements to cooperate with other DPAs; and rights of public interest groups to take representative actions. The exemptions from the Act may prove to be unreasonably broad. It remains to be seen whether fines of up to 4% of corporate turnover will be genuinely dissuasive when administered by courts, and whether significant compensation awards will be made.

Jamaica's law joins the 2019 Barbados law,[4] with which it shares many features, as a strongly GDPR-influenced law in the Caribbean. However, the US$50,000 limit on fines in Barbados mean that Jamaica has a potentially much stronger law. If the data protection authorities of these two jurisdictions actively enforce their laws, data privacy may take on a different meaning in the Caribbean.

[4] Barbados' law is summarised in G. Greenleaf '2020 Ends a Decade of 62 New Data Privacy Laws' (2020) 163 *Privacy Laws & Business International Report* 24-26, at p. 24 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611>.