CARLTON FIELDS

Top Considerations for Businesses Under Jamaica's Data Protection Act, Effective 2022

CYBERSECURITY AND PRIVACY | INTERNATIONAL | OCTOBER 7, 2021


Christina M. Gagnier


Kristin A. Gore

Jamaica's Data Protection Act (DPA) was enacted in May 2020, modeled after the European Union's General Data Protection Regulation (GDPR). While many companies may not be aware of this critical piece of privacy legislation and the obligations it places on businesses, the 2022 compliance deadline is right around the corner. This means that businesses need to begin their compliance efforts now to ensure they are prepared for this deadline.

Here are the top considerations that every company that does business in Jamaica, or with individuals in Jamaica, needs to know about the DPA.

Which businesses must comply with the DPA?

The DPA applies to entities, both for-profit and nonprofit, that:

- Are located or incorporated in Jamaica; or
- If not located or incorporated in Jamaica:
    - Use equipment for processing the personal information of an identifiable person (or an individual who has been deceased for less than 30 years) in Jamaica; or
    - Process the personal information of an identifiable person (or an individual who has been deceased for less than 30 years) in Jamaica related to (1) the offering of products or services to data subjects in Jamaica or (2) the monitoring of the behavior of identifiable persons if their behavior takes place in Jamaica.

Businesses that must comply need to appoint a data protection officer for monitoring the business's compliance with the DPA.

Businesses also have to determine whether they are a "data controller" or "data processor" for the purposes of the DPA. A "data controller" is a business that directly collects, uses, and stores personal information. A "data processor" may act at the direction of a data controller to process that information (for example, if a data controller collects email addresses and uses a third-party email client to send emails to customers, that email client is a data processor).

How is "personal data" defined?

Personal data is defined as "information (however stored) relating to a living individual, or an individual who has been deceased for less than 30 years, who can be identified from that information alone or from that information and other information in the possession of, or likely to come into the possession of, the data controller, and which includes any expression of opinion about that individual and any indication of the intentions of the data controller or any other person in respect to that individual."

Plain and simple, this means any information that a business collects on an individual that would lead to the identification of that individual. This also means any personal data collected, whether on or offline.

Examples of personal information collected day-to-day by businesses that may be regulated under the DPA would include names, email addresses, addresses, phone numbers, transaction information, and any other data points that a business would collect from an individual that could identify that individual.

What rights do consumers have under the law?

Like the GDPR, and Brazil's privacy law (Lei Geral de Proteção de Dados - LGPD), consumers are given a distinct set of rights. The DPA gives consumers the following rights:

- **Right to Be Informed/Right to Access**: Consumers have the right to know what data is being collected and processed by a business.
- **Right to Rectification (Correct)**: Consumers have the right to correct information that may be inaccurate.
- **Right to Erasure (Data Deletion)**: Consumers have the right to request that the personal information a business collects and processes be deleted.
- **Right to Object/Opt Out of Processing**: Consumers have the right to opt out of the processing of personal data for targeted advertising, the sale of personal data, and profiling activities with personal data that may affect the consumer.
- **Right Not to Be Subject to Automated Decision-Making:** Consumers have the right not to have their personal information used in automated decision-making in the course of a business offering products or services.

What type of notice must be given to consumers?

One of the benchmarks of the various domestic and global privacy regulations is meaningful consumer notice. The DPA mirrors these requirements and makes it clear that businesses that do business in Jamaica must provide consumers with notice of the categories of personal data collected, the purpose of the data collection, the categories of personal information that may be shared with third parties (service providers and vendors), and how consumers can exercise their consumer rights under the DPA.

What is a data privacy impact assessment? Is this required?

Businesses must undertake data protection impact assessments (DPIA) regarding data processing activities. Businesses must submit these assessments annually to the Office of the Information Commissioner, within 90 days after the end of a calendar year.

Similar assessments are also required by the GDPR, as well as the Colorado Privacy Act (CPA), which goes into effect in 2022, and the California Privacy Rights Act (CPRA) and Virginia Consumer Data Protection Act (VCDPA), which go into effect on January 1, 2023.

What is data minimization, and how does it apply to a business?

The principle of data minimization appears in several data privacy regulations, which calls for businesses to limit the personal data that they are collecting. This principle essentially endorses a "use it or lose it" approach to data to reduce liabilities attached to this data. The DPA is no different and places this requirement on businesses. Businesses should have an articulated use case for the data that they collect and, when they no longer have use for it, have a data retention policy that outlines conditions for the data's deletion.

When is consumer consent required?

Much like the GDPR and the LGPD, consent must be express, informed, and clear. Consumers must be given information about what giving their express consent means, as well as the consequences of denying or revoking consent to the processing of their personal data.

What are the legal bases for processing data?

The DPA provides the following legal bases for processing data, which businesses may be familiar with due to GDPR or LGPD compliance:

- Explicit consent
- Contractual necessity
- Legitimate interests
- Legal obligations
- Interests of the data subject
- Public interest

What obligations does a business have related to its vendors or third parties?

Businesses must have data privacy addendums and other agreements in place as it relates to the responsibilities of the "data controller" and "data processor" in processing personal data. It is advised that businesses adopt vendor procurement policies and have a framework in place to assess vendors' data privacy practices.

What about data breaches?

Much like the LGPD and U.S. state level data breach notification laws — but unlike the GDPR — the DPA has a consumer notice requirement. The table below highlights the key differences.

Requirement	DPA	LGPD	GDPR
Time frame for notice to the regulator	Notify information commission within 72 hours	Reasonable amount of time	Notify European Data Protection Board within 72 hours
Notice to consumers/data subjects	Yes	Yes	Dependent on circumstances

Who will enforce the DPA?

The Office of the Information Commissioner is tasked with enforcing the DPA.

What are the consequences of failure to comply?

Like the GDPR, there are distinct enumerated penalties for violations of the DPA, including:

- *Fines*. Businesses can be fined up to 4% of their annual gross worldwide turnover for the preceding year.
- *Personal Liability*. Directors and officers of businesses can be held personally liable. Individuals can be fined up to 5 million JMD and can face imprisonment up to 10 years.
- *Civil Action*. Consumers can seek civil damages for violations of the DPA and may be entitled to compensation from a data controller for those damages.

Now is the time to comply

Consumer-focused privacy legislation is becoming an international trend, with countries from Canada to China adopting aggressive regulations to protect consumers and their data. With this growing trend, investment in compliance is necessary to adhere to these mounting regulations and avoid great financial and reputational liability.

Our seasoned cyber compliance team has been tracking and analyzing privacy legislation since the inception of the GDPR and looking ahead to the new era in privacy as we advise clients on digital strategy to help them navigate uncharted legal territory. If you have any questions about how the implementation of Jamaica's Data Protection Act affects your business, please contact the authors of this alert or any member of the Carlton Fields Cybersecurity and Privacy Practice. Additionally, to learn more about the DPA and what steps you can take today to comply, view our webinar.

©2022 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.