



BARBADOS

Data Protection Laws of the World



Introduction



Welcome to the 15th update of the Data Protection Laws of the World handbook. Data protection and privacy laws continue to evolve at pace, reflecting responses to technological change, increasing data-driven business models and heightened expectations around accountability and enforcement. Alongside jurisdiction-specific reform, a number of clear global trends are emerging, including increasing enforcement action, greater data localization and complexities with data transfers, and closer alignment between data protection, cybersecurity and wider digital regulation, all set within a backdrop of heightened geopolitical tensions. As a result, keeping track of developments across jurisdictions has become both more important and more challenging for organisations operating internationally.

Recent legislative and enforcement developments

This edition reflects another busy year for privacy and data protection, with new legislation taking effect in key markets such as India, while enforcement of established data protection laws, such as those in Europe, continues to be influenced by an increasingly complex geopolitical environment and escalating cyber threats.

Developments in the United States

In the United States, consumer privacy laws continue to rapidly develop at the state level, with the passage of more than 20 state comprehensive consumer privacy laws and increased state and multi-state enforcement. Recently, minor privacy laws have been passed and taken effect in a number of states, imposing privacy obligations and restrictions on websites and online services that provide services that are directed at minors under 18 years old or that collect personal information about known minors under 18 years old. In addition to increased regulator enforcement, privacy litigation is on the rise in the United States – key areas of focus for privacy litigation and class action risk include minor privacy and safety, online tracking, data breaches and cyber incidents, text marketing, and biometrics.

Responding to a rapidly evolving landscape

To support clients in navigating this fast-moving landscape, Data Protection Laws of the World will now be updated twice per year, reflecting the accelerating pace of reform within the data protection and privacy landscape and the growing need for up-to-date, practical insight.

Barbados

LAST MODIFIED 28 JANUARY 2024



Data protection laws

The Data Protection Act (the "Act") was passed on August 12, 2019, and came into force in March 2021. Some provisions of the Act are yet to be proclaimed. The purpose of the Act is to regulate the collection, keeping, processing, use and dissemination of personal data and to protect the privacy of individuals in relation to their personal data. Some provisions of the Act are yet to be proclaimed.

Definitions

Definition of Personal Data

"Personal data" means data which relates to an individual who can be identified:

- from that data; or
- from that data together with other information which is in the possession of or is likely to come into the possession of the data controller.

Definition of Sensitive Personal Data

"Sensitive personal data" means personal data consisting of information on a data subject's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- membership of a political body;
- membership of a trade union;
- genetic data;
- biometric data;
- sexual orientation or sexual life;

- financial record or position;
- criminal record; or
- proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court of competent jurisdiction in such proceedings.

National data protection authority

The Data Protection Commissioner (the "Commissioner") was appointed with effect from July 15, 2021 and is responsible for the general administration of the Act.

Registration

A data controller must be registered in the Register of Data Controllers.

A data processor must be registered in the Register of Data Processors.

Data protection officers

The data controller and the data processor must designate a data privacy officer where:

- the processing is carried out by a public authority or body, except for a court of competent jurisdiction acting in their judicial capacity;
- the core activities of the data controller or the data processor consist of processing operations which, by virtue of their nature, their scope and their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the data controller or the data processor consist of processing on a large scale of sensitive personal data.

The data privacy officer must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the duties and functions as set out under the Act.

Collection and processing

Where personal data relating to a data subject is collected from the data subject, the data controller must, at the time when personal data is obtained, provide the data subject with the following:

- the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- the contact details of the data privacy officer, where applicable;

Processing of personal data is only lawful where:

- the data subject has given consent to the processing of his personal data for one or more specific purposes; or
- the processing is necessary
 - for the performance of a contract to which the data subject is a party;
 - for the taking of steps at the request of the data subject with a view to entering into a contract;
 - for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
 - in order to protect the vital interests of the data subject;
 - for the administration of justice;
 - for the exercise of any functions of either House of Parliament;
 - for the exercise of any functions conferred on any person by or under any enactment;
 - for the exercise of any functions of a public authority;
 - for the purposes of legitimate interests pursued by the data controller or by the third party to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject; or
 - processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Transfer of personal data

Transfer of personal data is unlawful unless certain conditions are satisfied. Where the data subject has given their consent to the transfer of their personal data, the restrictions on the transfer of the data do not apply. The Act also sets out various other exemptions for the restrictions where transfer of the personal data is necessary e.g. for the performance of a contract between the data subject and the data controller, reasons of substantial public interest, for the purpose of obtaining legal advice, etc.

Personal data obtained must not be transferred to a country or territory outside Barbados unless that country or territory provides for (a) an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data and (b) appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects.

The circumstances for determining an adequate level of protection as well as methods for providing appropriate safeguards including the development of binding corporate rules must be submitted to the Commissioner for authorisation.

The "*binding corporate rules*" must specify (but not limited to) the following:

- the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- their legally binding nature, both in and outside of Barbados.

Security

The data controller and the data processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Breach notification

In certain circumstances, a data controller is required to report to the Commissioner data breaches which have affected a data subject.

Mandatory breach notification

Where there is a personal data breach the data controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller must communicate the personal data breach to the data subject without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Enforcement

Where the Commissioner is satisfied that a data controller or a data processor has contravened or is contravening this Act, the Commissioner may serve him an "enforcement notice".

In deciding whether to serve an enforcement notice, the Commissioner must consider whether the contravention has caused or is likely to cause any person damage or distress.

Electronic marketing

There are no specific laws in respect of these matters.

Online privacy

There are no specific laws in respect of these matters.

Data protection lawyers



Angela R Robinson
Partner
Chancery Chambers
arobinson@chancerychambers.com
[View bio](#)



Giles A M Carmichael
Managing Partner
Chancery Chambers
gcarmichael@chancerychambers.com
[View bio](#)

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg

Partner
Global Co-Chair Data, Privacy and
Cybersecurity Group
carolyn.bigg@dlapiper.com
[Full bio](#)



John Magee

Partner
Global Co-Chair Data, Privacy and
Cybersecurity Group
john.magee@dlapiper.com
[Full bio](#)



Andrew Serwin

Partner
Global Co-Chair Data, Privacy and
Cybersecurity Group
andrew.serwin@us.dlapiper.com
[Full bio](#)

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com