DATA PROTECTION LAWS OF THE WORLD

Bahamas

BAHAMAS

Last modified 26 January 2023

LAW

Data Protection (Privacy of Personal Information) Act **("DPA").**

DEFINITIONS

Definition of Personal Data

Section 2 DPA defines 'personal data' as data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller.

Definition of Sensitive Personal Data

'Sensitive personal data' is further defined in Section 2 DPA as personal data relating to: racial origin; political opinions or religious or other beliefs; physical or mental health (other than any such data reasonably kept by them in relation to the physical or mental health of their employees in the ordinary course of personnel administration and not used or disclosed for any other person); trade union involvement or activities; sexual life; or criminal convictions, the commission or alleged commission of any offence, or any proceedings for any offence committed, the disposal of such proceedings or the sentence of any court in such proceedings.

It should be noted that although sensitive personal data ('**SPD**') is distinguished from personal data under DPA in its specificity of certain categories of data, SPD does not otherwise receive any special treatment compared to general personal data. While DPA provides that the relevant Minister responsible for data protection may create regulations that would provide safeguards for such data under the Act, such a regulation has never materialized.

NATIONAL DATA PROTECTION AUTHORITY

Section 14 DPA establishes a Data Protection Commissioner ('**DPC**'), a corporation sole, that is tasked with the enforcement of the provisions of DPA. The DPC operates from the Office of the Data Protection Commissioner which would the Bahamian equivalent of a national data protection authority as seen in other jurisdictions.

REGISTRATION

There is no obligation under DPA to register with the Office of the Data Protection Commissioner as a data controller (or data processor).

DATA PROTECTION OFFICERS

There is no statutory duty to appoint a Data Protection Officer under DPA.

COLLECTION & PROCESSING

DPA in The Bahamas has only limited extraterritorial effect (as it concerns data controllers). Per Section 4(1) of DPA, the Act only applies to: data controllers established in The Bahamas (where the data is processed in the context of the local establishment); and data controllers established outside The Bahamas that use equipment in The Bahamas for processing data (other than for transit through The Bahamas).

In the above context, an 'established' data controller can be any of the following (in accordance with Section 4(3) of DPA): an individual ordinarily resident in The Bahamas; a body incorporated or registered under Bahamian law; a partnership or other unincorporated association formed under Bahamian law; and any person that does not fall into any of the foregoing categories but maintains an office, branch or agency in The Bahamas through which they carry on a business activity or regular practice. It can be seen, therefore, that a nexus to The Bahamas of the kind described above must be established for DPA to apply outside the jurisdiction.

Data controllers are defined in Section 2 DPA as a person who, alone or with others, determines the purposes for which and the manner in which any personal data are, or are to be processed. Data controllers owe a statutory duty of care to data subjects pursuant to Section 12(1) as it regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data. Further, Section 12(2) provides that data controllers must use contractual or other legal means to provide a 'comparable' level of protection from any third party to whom he discloses information for the purpose of data processing.

Data controllers, under Sections 6(1), must abide by several core duties as it relates that the collection, processing, keeping, use and disclosure of data of data subjects, namely, to ensure:

- The data or information constituting the data has been collected by means which are lawful and fair in the circumstances of the case (e.g., data subjects should not be deceived or misled as to the purpose(s) for which the data is being processed or collected – and the use of such data should not cause damage or distress to the data subject);
- The data is accurate and kept up to date where necessary (except in the case of data back-up);
- The data is only kept only for one or more specified or lawful purpose(s);
- The data is not used or disclosed in a manner which is incompatible with that/those purpose(s);
- The data collected is adequate, relevant and not excessive in relation to that purpose or purposes;
- The data is not kept for a period longer than necessary for the purpose(s) for which it was collected (except in cases where personal data needs to be kept for historical, statistical or research purposes);
- There are appropriate security measures in place to prevent unauthorised access to, or alteration, disclosure or destruction of data and against its accidental loss or destruction.

TRANSFER

Section 17 DPA speaks to the international transfer of data. Under Section 17(1) the DPC may prohibit the transfer of personal data from The Bahamas to a place outside The Bahamas in cases where there is a failure to provide protection either by contract or otherwise equivalent to that provided under DPA, subject to certain exceptions. In arriving at a determination to prohibit the international transfer of data, the DPC must consider whether such a transfer would cause damage or distress to any person and consider the desirability of the transfer. Pursuant to Section 17(8) however, data constituting data required or authorized to be transferred under another enactment; or data that is required by any convention or other instrument imposing an international obligation on The Bahamas; or otherwise, data that a data subject has consented to having transferred, will not apply under Section 17.

SECURITY

As mentioned previously, Section 6(1)(d) provides that data controllers must ensure that appropriate security measures are taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. In practice, appropriate security measures typically mean 'industry-standard' (particularly for institutions that store SPD, e.g. law firms, hospitals, banks, insurance companies, etc).

BREACH NOTIFICATION

There is no breach notification obligation under the provisions of DPA.

ENFORCEMENT

The DPC of The Bahamas is largely responsible for the enforcement of data protection in the jurisdiction. Section 15(1) states that the DPC may investigate or cause to be investigated whether any of the provisions of DPA have been contravened by a data controller or a data processor in relation to an individual when an individual has complained of a contravention of any DPA provisions or where he may otherwise be of the opinion that a contravention make have occurred. Enforcement measures the DPC can utilize include enforcement notices (Section 16 DPA), prohibition notices (Section 17 DPA), information notices (Section 18 DPA), and in rare instances bringing and prosecuting summary offences under DPA (Section 28 DPA).

Aside from its statutory functions, the DPC is also tasked with educating the public of data protection issues and trends and providing assistance in data breach remediation.

In accordance with Section 29(1) DPA, penalties for a person guilty of an offence under DPA are liable on summary conviction to a fine not exceeding $2,000.00 Bahamian Dollars; or on conviction on information, to a fine not exceeding $100,000.00 Bahamian Dollars. Further, Section 29(2) provides that where a person is convicted of a DPA offence, the court may also order that any data material which appears to the court to be connected with the commission of the offence to be forfeited or destroyed and any (relevant) data to be erased.

ELECTRONIC MARKETING

Data subjects have the right to prohibit processing for the purposes of direct marketing by way of Section 11 DPA. Though DPA provides that 'direct marketing' includes direct mailing, it also applies by extension to electronic marketing and newsletters. In order to prohibit such processing a data subject may make a written request to the data controller to cease using any data that has been kept for the purpose of direct marketing. The data controller then has no more than forty days to either erase or cease using the said data and notify the data subject in writing accordingly.

ONLINE PRIVACY

Outside of the current provisions of DPA and legislation governing law enforcement access to one's computing devices and encrypted data (e.g. the Interception of Communications Act, Computer Misuse Act, National Crime Intelligence Agency Act etc.), online privacy is largely unregulated and there are no specific laws aimed at the use of cookies or the collection of location data.

Under the Electronic Communications and Transactions Act ('**ECTA**'), however, Section 20 provides for online intermediary a procedure for 'dealing with unlawful, defamatory, etc. information'. An intermediary is defined under Section 2 ECTA as, in the context of an electronic communication, a person including a host on behalf of another person who sends, receives or stores either temporary or permanently that electronic communication or provides related services with respect to that electronic communication. Section 20(1) states that where an intermediary has actual knowledge that information in an electronic communication gives rise to civil or criminal liability, then as soon as possible the intermediary should remove the information from any information processing system within the intermediary's control and cease to provide or offer services in respect of that information and notify the police of the any relevant facts and of the identity of the person from whom the intermediary was supplying services in respect of the information, if the identity of that person is known to the intermediary. Similarly, Section 20(2) states that if an intermediary is aware of facts or circumstances from which the *likelihood* of civil or criminal liability in respect of the information in an electronic communication ought reasonably to have been known should, as soon as practicable, follow any relevant procedure set out in any code of conduct that may be applicable to the intermediary under the Act or notify the police and relevant Minister responsible for electronic communications. The Minister may then direct the intermediary to remove the electronic communication from any information processing system within the control of the intermediary and cease to provide services to the person to whom the intermediary was supplying services in respect of that electronic communication. It can be argued that these provisions give intermediaries (e.g. telecommunications providers) facilitating communications between end users' communications broad powers to potentially cease services or effectively censor electronic communications they deem objectionable on the grounds that civil or criminal liability could likely arise without any liability arising provided the action is made in good faith.

KEY CONTACTS

GrahamThompson
grahamthompson.com/

Sean G. McWeeney Jr.
Associate
GrahamThompson
T +1 (242) 322-4130
sgm@gtclaw.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.