DATA PRIVACY DAY

Office of the Information Commissioner

IT HAS often been said that if certain countries sneeze, the world catches a cold. At a time when the entire world is experiencing the COVID-19 pandemic, this seems only too true. Not all contagion is bad, however. In 2018, the European Union introduced its General Data Protection Regulation (GDPR) and countries across the globe caught the metaphoric data protection 'bug'. Whether for the purpose of international trade and investment or to protect their own citizens' rights to data privacy, numerous countries have passed, are in the process of passing, or are contemplating passing laws for the protection of people's personal information being processed by third parties.

Why is this good news? Because we are living in the digital age. In today's world, every business process, transaction and electronic platform, including websites and social media, requires some personal information and cyber-attacks occur with ever-increasing frequency. Individuals, therefore, need to know the risks to their personal data and be put in a position to guard against them or seek a remedy where they become victims of them. Data protection laws aim to give back individuals control over their personal data by recognising their information privacy right and imposing obligations on others to respect those rights.

Jamaica passed its Data Protection Act (DPA) in June 2020 and, on December 1, 2021, appointed Celia Barclay as the first Information Commissioner. With that, the process to implement a system to ensure compliance of data controllers with data protection standards commenced. The legislation also provides redress for data subjects whose right to privacy of their personal data (information from which a person can be identified) has been breached. Every identifiable Jamaican is a data subject for whose protection and other benefit the act was passed.

Consequent on the passing of the DPA, Jamaicans and other data subjects have certain rights, including but not limited to:

The right to know which, if any, of their personal data is being processed, the purpose for which it is being processed, and to whom such data will be disclosed;

The right to receive a copy of any personal data being processed and to be advised of its source if not provided by the data subject; and

The right to be compensated for damage or distress resulting from a data controller contravening the act.

Generally speaking, data controllers are persons or entities, including public authorities, who make decisions regarding the processing of the personal data of data subjects. The processing of data includes any method of collection, recording, storage, use, alteration or manipulation, retrieval or disclosure and even the disposal of the data when it is no longer required. A data controller does not have to control every type of processing to be subject to the act. Controlling any one or any combination of the activities mentioned in relation to personal data requires compliance with the relevant data protection standards imposed by the act.

In order to help protect against data controllers trespassing on the rights of data subjects, the DPA requires, among other things, that data controllers:

a) Register with the Information Commissioner

b) Appoint a Data Protection Officer (DPO)

c) Conduct and submit to the Commissioner an annual Data Protection Impact Assessment

d) Comply with the 8 data protection standards prescribed by the act.

The 8 data protection standards with which data controllers are required by law to comply are:

1. Personal data should be processed fairly and lawfully, i.e., certain conditions including as to consent and necessity must be met.

2. Processing of personal data must be for specific and lawful purposes only.

3. Any personal data to be processed or being processed must be adequate, relevant and limited to what is necessary for the purpose.

4. Data controllers must ensure the personal data processed are accurate and up to date.

Information Commissioner Celia Barclay

5. As soon as the personal data is no longer necessary, it must be properly disposed of.

6. Processing of personal data must also be in accordance with data subjects' rights.

7. Each data controller must ensure the appropriate technical and organisational measures are in place to properly process any personal data.

8. Personal data in the possession of a data controller should not be transferred outside Jamaica without the receiving territory also having adequate protection relating to the processing of personal data.

It is the responsibility of every organisation, whether a business or other entity, to demonstrate its compliance with the data protection standards. They can do this by, among other things, appointing a Data Protection Officer if required by the act, conducting a Privacy Impact Assessment, applying good practices, complying with codes of conducts relevant to data protection in their field or industry, and obtaining appropriate certifications from accredited bodies.

The Information Commissioner is responsible for promoting and ensuring compliance with the Data Protection Act and, particularly, with the data protection standards. The Commissioner will register and regulate data controllers. This includes promoting good practices by them, providing guidelines for different sectors and industries, and also for their regulatory bodies. In addition, the Office of the Information Commissioner (OIC) has as its mandate:

• Educating the public on the implications of the DPA and their data protection rights or obligations;

• Advising the Government of Jamaica on policies, procedures and other matters relating to data protection; and

• Cooperating and collaborating with international partners regarding data protection matters to ensure the country is compliant with its obligations under relevant international laws and that local data protection standards are consistent with international ones.

DATA PROTECTION Q & A

1. WHAT DETERMINES WHETHER INFORMATION IS PROTECTED BY THE ACT?

The act protects 'personal data' which is any information which can be used to identify a person. Common examples are names, addresses, TRNs, etc., but it also includes sensitive information such as genetic or biological data, biological relationship, race, ethnicity, sexual orientation, religion, political opinion, philosophical belief and health information.

2. DOES HAVING A DATA PROTECTION ACT MEAN THAT DATA SUBJECTS' PERSONAL INFORMATION IS NOW SAFE?

The act cannot guarantee personal data will be protected; it can only require it and impose penalties for when protection is inadequate or fails. Also, since data privacy is not data security, data subjects should still take steps to protect themselves. Get familiar with their data privacy rights and try as far as possible to prevent those rights being violated. Start reading privacy policies. Pay attention to the information required on forms, including electronic forms used online or by mobile applications. Ask questions: why is this personal information required? What will it be used for? Who will it be disclosed to? Do not give out personal data unnecessarily. Secure their information with appropriate devices and software applications. Most importantly, get professional help or advice if necessary.

3. CAN ORGANISATIONS REGISTER AS DATA CONTROLLERS NOW?

The process of building out the Office of the Information Commissioner, which includes developing the systems that will be required to formally register data controllers, has only just commenced so it is not yet possible for data controllers to apply to be registered. However, as there are several criteria that they will need to meet when registration commences, they are encouraged to take the necessary steps to get themselves ready.

4. DOES EVERY DATA CONTROLLER HAVE TO APPOINT A DATA PROTECTION OFFICER (DPO)?

No. While it is beneficial and therefore encouraged, the DPA only requires data controllers to appoint a DPO if they are a public authority, if they process personal data on a large scale, if they process certain types of personal data, or if they fall within a prescribed class of controllers. There is no express prohibition against an employee being appointed as the DPO; however, data controllers must be mindful that their duties as DPO do not conflict with their duties as an employee.

5. HOW CAN DATA CONTROLLERS KNOW IF THEY ARE COMPLIANT OR NOT?

There are several professionals, including lawyers and IT Service Providers, who specialise in Data Privacy and Information System Security. Data Controllers can consult these professional for detailed advice on their obligations under the act or request a Data Privacy Assessment to determine whether their systems and procedures for dealing with personal data provide adequate protection against breaches.

6. WHAT IF A DATA CONTROLLER IS NOT YET COMPLIANT WITH THE ACT?

The act provides for a 2-year transitional period within which data controllers are required to take all necessary measures to ensure their compliance with the data protection standards. During that transitional period which commenced on December 1, 2021, data controllers will not be prosecuted for any processing of personal data done in good faith.

7. WILL A DATA CONTROLLER WHO DOES NOT COMPLY WITH THE REQUIREMENTS OF THE ACT BE PENALISED?

Yes. The act provides various penalties for non-compliance with the data protection standards and other breaches of the act. These include both fines and imprisonment which vary, depending on the severity of the offence or impact of the breach. The penalties are imposed on the data controller who is given the obligation of protecting data subjects' personal data, not on the Data Protection Officer who is tasked with monitoring the controller's compliance with the DPA.

8. CAN A DATA SUBJECT GET COMPENSATION IF HIS/HER RIGHTS HAVE BEEN BREACHED?

Yes. A data subject whose rights have been breached MAY be able to get compensation from the relevant data controller. However, whether compensation is awarded and the amount of compensation will depend on several factors, including the nature and impact of the breach.

9. WHAT DOES THE DPA MEAN FOR NIDS?

The National Identification and Registration Authority (NIRA) through the National Identification System (NIDS) will seek to ensure the identifiability of every Jamaican. As an entity which collects and processes a large volume of personal data from the public, it is set to become Jamaica's largest data controller. The authority will be bound by the Data Protection Act and must also comply with all the data protection standards.

10. HOW CAN PERSONS GET MORE INFORMATION?

Persons can contact the Office of the Information Commissioner at 1st Floor, PCJ Resource Building, 36 Trafalgar Road, Kingston 10; Telephone: 876-929-8990-9; Email: **oic_info@mset.gov.jm**