Data Protection Act

ARE YOU READY FOR DATA PROTECTION ACT?

Chukwuemeka Cameron, Attorney and Founder, Design Privacy

HOW THE PRIVACY PARADOX AFFECTS BUSINESS GROWTH

Andrew Nooks, Director of Efficiency and Growth, Symptai

Please pass on this training memo to anyone who will benefit.

October 15, 2020

The Data Protection Act Is Here. Is Your Business Ready?

What is the Data Protection Act?

Jamaica's Data Protection Act was passed in June 2020.
It seeks to safeguard the privacy and personal information of Jamaicans by providing guidelines on how personal data should be collected, processed, stored, used and disclosed in physical or electronic form. The DPA states that:

- Data should only be obtained for specific lawful purposes, with the consent of the individual, and not to be further used or processed in any way incompatible with the original purpose;
- Data collected must be accurate and, where necessary, kept up to date; must not be held for longer than is necessary for the original purpose; must be protected using appropriate technical and organisational measures; and be disposed of in accordance with the regulations;
- Data must not be transferred to a State or territory outside of Jamaica, unless that State or territory ensures an adequate level of protection of the rights and freedoms of the individual from whom the data has been collected.

Consumer Rights Under the DPA

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to restrict processing;
- The right to object; and
- The right not to be subject to automated decision-making including profiling.

Steps to ensure compliance with the DPA

As long as you process personal data, you are subject to the Act. At the very minimum you should identify the lawful basis for your processing activity in the DPA, document it and update your privacy notice to explain it.

- Attend training sessions to become familiar with the Data Protection Act.
- Ensure management is aware of the DPA and what it entails.
- Appoint a qualified Data Protection Officer to oversee the implementation of your data protection compliance programme.
- Audit & document what personal data you hold, where it came from and who you share it with.
- Review your current privacy notices and put a plan in place for making any necessary changes after reviewing the DPA.
- Understand that you have an obligation to ensure your customers can exercise their privacy rights. Check your procedures to ensure they cover all the rights individuals have, including how you would provide data to a data subject.
- Review how you seek, record and manage customer consent and whether you need to make any changes. Refresh existing consents now if they don't meet the DPA standard.
- Ensure you have the right procedures in place to detect, report and investigate a personal data breach.

ARE YOU READY FOR DATA PROTECTION ACT?

Chukwuemeka Cameron, Attorney-at-law and Founder, Design Privacy

The Data Protection Bill was tabled in 2017. At that time industry stakeholders lobbied Parliament for a transition period between the passage of the act and its implementation. A minimum period of two years after the passage of the Act was requested to allow companies to do what is necessary to become compliant. It was argued that this was necessary given the fundamental changes and capital outlay that would have to be made by organizations. This request was consistent with the manner in which the General Data Protection Regulation (GDPR)(the equivalent to our Data Protection Act (DPA))was rolled out in Europe. The GDPR provided that it would not become effective until 2 years after its passage. It was passed in May 2016 and became effective in May 2018. The DPA in its current state only provides for a limited transition period for the government.

Two years having now elapsed since the introduction of the Bill and extensive consultations having been held, what steps if any have been taken by government agencies and private sector companies to become DPA ready in light of the transition period that was being requested? Appreciating the last minute propensity of our culture the better question may be what steps should one be taking to become DPA ready? Which companies should be more concerned about the DPA?

The reality is that all organizations, as long as they process personal data, are subject to the Act. However, some processing activities expose data subjects to more risks than other types of processing. Companies that process personal data as their core business, such as market research companies and telecommunications companies, for example, would pose a higher risk to data subjects. Additionally, companies that process large amounts of sensitive and/or personal data such as the medical, financial, tourism and BPO sectors also expose data subjects to high risks. Finally, companies that automate the processing of personal data, in addition to all companies listed on the junior and main stock exchange that are sensitive to external legal and regulatory risks should be in advanced stages of readiness for the DPA. Some industries like the hotel industry are already subject to the GDPR as they market directly to European data subjects.

ARE YOU READY FOR DATA PROTECTION ACT?

Chukwuemeka Cameron, Attorney-at-law and Founder, Design Privacy

Here are some practical tips to start your Data Protection Compliance journey. The first thing you need to do is become familiar with the new paradigm that the Data Protection Act is heralding in by attending some bespoke training that focuses on the Jamaican Data Protection Act and not the GDPR as they are significantly different, especially as it relates to the obligations and liabilities of organizations(data processors).

- You should make sure that decision makers and key people in your organisation are aware that the law is coming.
- Has this issue been discussed at any of your previous board meetings or has it been placed on your agenda for the next board meeting?
- For companies that do not have an active board, is it going to be discussed at your next business meeting?

The board or the business need to appreciate the impact the passage of the Data Protection Act is likely to have on the personal criminal liability of key personnel and the fundamental changes that have to take place on how one processes personal data. Updating one's privacy policy alone will not suffice.

ARE YOU READY FOR DATA PROTECTION ACT?

Chukwuemeka Cameron, Attorney-at-law and Founder, Design Privacy

The law as it now stands, requires all organizations to appoint an appropriately qualified Data Protection Officer who is to oversee the implementation of your data protection compliance programme. The Data Protection Officer(DPO) cannot be your CIO or head of HR or anyone that currently makes any decision in relation to how the data is processed in order to avoid a conflict of interest. Have you thought about what a duly qualified Data Protection Officer would look like for you? Have you thought about or started to short list persons to train as a DPO or hire as a DPO? The main functions of the DPO are to :

- Raise awareness of Data Protection issues and provide training;
- Monitor and oversee compliance with the DPA;
- Advice and help execute the mandatory Data Protection Impact Assessment;
- Provide advice on complying with the DPA;
- Cooperate with the supervisory authority, and
- Be the contact person for your customers in relation to personal data protection issues.

What might an appropriately qualified Data Protection Officer look like?

- Someone with an understanding of the legal and regulatory environment in which your business operates that extends beyond just the Data Protection Act;
- More than a basic understanding of ICT and information management systems;
- Experience in business operations and experience in a corporate or business environment, and of course;
- Some form of training and experience as a Data Protection Officer.

ARE YOU READY FOR DATA PROTECTION ACT?

Chukwuemeka Cameron, Attorney-at-law and Founder, Design Privacy

The next activity you can undertake is to document what personal data you hold, where it came from and who you share it with. You may need to organize an information audit across the organisation or within particular business areas. You should review your current privacy notices and put a plan in place for making any necessary changes.

Understanding that you have an obligation to ensure your customers can exercise their privacy rights, you should check your procedures to ensure they cover all the rights individuals have, including how you would provide data to a data subject.

The DPA includes the following rights for individuals:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to restrict processing;
- The right to object; and
- The right not to be subject to automated decision-making including profiling.

You should update your procedures and plan how you will handle requests to take account of the new rules. In general, if a customer were to exercise any of the above listed rights for example, request of you all the personal data you have on them, you will have 30 days to respond. If your organisation were to receive a large number of these access requests, have you thought through the logistical implications of having to deal with all of them at the same time?

ARE YOU READY FOR DATA PROTECTION ACT?

Chukwuemeka Cameron, Attorney-at-law and Founder, Design Privacy

At the very minimum you should identify the lawful basis for your processing activity in the DPA, document it and update your privacy notice to explain it. This will be something that will be totally new to your organization. Bear in mind, it may well be a breach of your customers privacy rights to process their personal data in the absence of a lawful basis. Organizations will be well advised to start considering this even in the absence of a Data Protection Act.

Obtain consent from your customers to process personal data and; you should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they do not meet the DPA standard.

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. The DPA introduces a duty on all organizations to report certain types of data breaches to the supervisory authority. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases. Failure to report a breach when required to do so in addition to the breach itself could result in criminal liability.

In addition to the Data Protection Officer you should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organization's structure and governance arrangements.

These are some of the issues your organization needs to start considering as you prepare for your data protection compliance journey.

HOW THE PRIVACY PARADOX AFFECTS BUSINESS GROWTH

Presented By: Andrew Nooks, Director of Efficiency and Growth, Symptai
Written by: DeAndre Harriot, Digital Marketing Strategist, Symptai.

According to the International Association of Privacy Professionals (IAPP), Privacy is defined as "the right to be left alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how personal information is collected and used."

- Imagine having all your customers and potential customers say 'they wish to be left alone'.
- As a marketer responsible for executing a customer growth strategy, that would be a nightmare.
- We are operating in a very interesting time in business where the rapid advancement in technology has led to large scale adoptions of aggressive digitization strategies. Artificial intelligence and predictive technologies are becoming commonplace in every industry, with this we are able to predict trends, changes in consumer behaviours and the effects emerging technologies will have on our Business Development strategies.
- At the centre of this customer growth strategy is data - customer data, the new oil. Being able to communicate one on one with your customers in a personalized manner, sharing with them only the things that are of interest to them, always being able to answer their questions even before they ask, providing real value long before the first sales conversation begins are all the things that, every sales and marketing executive dream of doing.
- Imagine meeting with your CEO to explain your customer growth strategy and showing how you have created value and connected with each customer as though they were a childhood friend.
- ***Can you say promotion? Huge end of year bonus?***
- Both customers and executives expect a value-adding growth strategy to include only relevant and timely information communicated in the precise way your customers would most prefer to receive it.
- **However, to make this a reality, customers are required to offer a company access to a lot of personal information, and this is where the Privacy Paradox is introduced.**

HOW THE PRIVACY PARADOX AFFECTS BUSINESS GROWTH

Presented By: Andrew Nooks, Director of Efficiency and Growth, Symptai
Written by: DeAndre Harriot, Digital Marketing Strategist, Symptai.

What is the Privacy Paradox?

The 'Privacy Paradox' is a term coined all the way back in 2001 by Barry Brown in a study done on the experience of internet users. In this study of early online shopping, Barry found that there was a paradox that existed between customers' concerns about their privacy and their desire to still use supermarket loyalty cards which had the ability to track their behaviour.

The Privacy Paradox simply says this 'Customers do not trust organizations with their data; however, they still expect to benefit from a personalized shopping experience'.

The biggest challenge your customers face is that while they know their information is valuable, they do not quite know how much it is valued. They receive value from doing business with your organization but there is no tangible or audible experience associated with parting with their personal data and as such, customers do not feel the impact of the transaction in the same way they do when there is a transfer of funds associated with a product or service. Organizations have been collecting and storing customer data and using it to predict behaviour for decades, sometimes for the benefit of the consumer but other times to their detriment.

In order to protect the human right to privacy, many governments and regulatory bodies around the world have been creating and implementing privacy laws and regulations around how organizations should collect, process, store, transmit and destroy personal data, returning the power of privacy to the hands of the consumer.

HOW THE PRIVACY PARADOX AFFECTS BUSINESS GROWTH

Presented By: Andrew Nooks, Director of Efficiency and Growth, Symptai
Written by: DeAndre Harriot, Digital Marketing Strategist, Symptai.

Privacy Regulations and Their Impact

By this point, we all would have heard of the General Data Protection Regulation (GDRP) coming out of the EU. Similar regulations have been enforced in different jurisdictions while many others are pending. Regulations such as the CCPA, CPA, PIPEDA, PDPA among others. All of which are extraterritorial regulations which simply means that they are valid across all jurisdictions. There is a common misconception that privacy is an IT or Security issue, which could not be further from the truth. Privacy is an organization-wide issue and Marketing, Sales and Customer Service are all warriors on the front-line. Almost all privacy regulations stipulate some basic rights, all of which affect how we engage with our customers. Some of these rights include:

Right to Consent – Access to process personally identifiable data must be clear and intentionally given.

Right to Data Protection – Personally identifiable data should be protected with adequate and effective security controls.

Right to Access and Rectification– Individuals should be able to, upon request, review all information collected and to correct where applicable.

Right to be Forgotten – All data that has been collected should be permanently deleted upon legal request including archived data.

All four concepts above in addition to others not named here, places the responsibility of data collection, protection and use squarely in the hands of the organization despite how it may have been obtained. With this responsibility comes very large fines for the misuse or inability to adequately protect this critical data.

For us Business Development Practitioners, this creates a bottle-neck of competing interests. No longer can we store or use customer information without clear legal interest that matches the use of data to the purpose for which it was collected.

HOW THE PRIVACY PARADOX AFFECTS BUSINESS GROWTH

Presented By: Andrew Nooks, Director of Efficiency and Growth, Symptai
Written by: DeAndre Harriot, Digital Marketing Strategist, Symptai.

So What's Next?

- Data privacy regulations should be viewed as a gift, not a curse.
- Following proper privacy regulations will lead to us collecting, storing and using less meaningless data as the less data we have, the lower the chances are of violations occurring. This creates a more competitive customer growth strategy as collecting less data means we need to collect more targeted data, and the more targeted the data, the more efficient our data use must become.
- Even without regulations customers are becoming smarter and more cautious about their data and expect a reasonable explanation for the use of their personal information.
- However, for most consumers, it's about how the data is collected and used not necessarily what data attribute is being collected. I
- don't necessarily mind the fact that you remind me that my yearly subscription is coming to an end a month or weeks in advance. What I do mind is you sending me an unsolicited email telling me that the shirt I wore to work today would look great with your new pair of designer slippers.
- Companies that combine data privacy with data use will, in the long-term, benefit from creating value through relevant communication all while increasing consumer trust over time.

Now, imagine meeting with your CEO to explain your customer growth strategy two days before she receives regulatory fines for privacy violations related to a recently concluded email campaign? Can you say no Promotion? Can you say let's start crafting our resignation letter because we might be out of a job?

Symptai Certified Information Privacy Manager Course Available for Registration Here: https://www.symptai.com/training-courses/cipm

REFERENCES

Chukwuemeka Cameron, Attorney-at-law and Founder, Design Privacy

- Number: 876-339-3673
- Email: chukwuemeka.cameron@gmail.com

Andrew Nooks, Director of Efficiency and Growth, Symptai

- Number: 876-527-5469
- Email: andrew_nooks@symptai.com