Data Privacy by Design: Legal meets Technology

Summary of webinar held on January 17, 2022

GDPR & Data Protection Acts in the Region

The enactment of the 2018 General Data Protection Regulation (GDPR) created a butterfly effect in the global data privacy landscape. The GDPR quickly became the data protection benchmark and harmonized the pre-existing patch set of rules which previously made it difficult for multinational companies to maintain regulatory data privacy compliance.

Fast forward to 2022, there are a number of data protection regulations across the region which are at various stages of enactment. It can be expected that in the near future we will see continued development of these various Acts, especially since a few islands have earmarked their Data Commissioner.

Legal & Regulatory Requirements – What you need to know

Each jurisdiction's Act will have their own local nuances. However, there are a few key principles upon which they are founded:

- Lawfulness and fairness
- Transparency
- Data minimization
- Accuracy
- Storage limitation
- Information Security (Confidentiality & Integrity)
- Accountability

If you are a company operating in different countries, you cannot pick and choose which countries implement data protection rules. All customers should be able to achieve similar service regardless of which branch they conduct business.

Data privacy management should be about giving the customer the best experience whilst managing regulatory requirements. In addition, regulators will be expecting that best practices are followed.

It is therefore advisable for a company to use the highest watermark as it relates to ensuring compliance with data protection best practices. We will highlight some requirements from a legal and regulatory standpoint, that you need to consider.

Do the relevant persons in your organization understand the requirements of the Act? Do all employees understand the purpose behind your various data protection policies? If your policies are too "legalese", then it is unlikely that they would adjust their behavior and help build a culture of privacy.

Notably, there is now a requirement of consent for the gathering of data. Thereby requiring that you have appropriate retention of data as well as the relevant controls to protect that data in place.

Webinar Highlights

As is often said, it is not a matter of if you will be breached, but when you are breached. It is your responsibility in the incident of a data privacy breach to report to the regulator (Data Commissioner) and all persons whose data privacy rights have been impacted.

In the case of an actual or suspected breach, or if for whatever reason your company is being investigated by the regulators, you need to be able to demonstrate that adequate safeguards were implemented, and that adequate professional consultation was obtained to assist with the development of data protection policies, frameworks, and infrastructure.

Your aim should be to achieve and maintain a defensible position. Finally, it is important to have these things in place prior to a breach occurring, as this will help save your company's profitability and reputation.

Achieving Compliance: Privacy by Design

So how do you create that defensible position? By using the highest watermark – data privacy best practices. Privacy by Design (PbD) is a framework that is structured around seven foundational principles and was developed by Dr. Ann Cavoukian, a former Canadian privacy regulator who collaborated with KPMG in Canada to roll out a globally acceptable privacy certification.

These seven principles are engrained in data protection legislations. The GDPR actually mandates Privacy by Design as a legal and enforceable obligation. This framework assists with implementing data privacy best practices before an incident occurs.

A company should avoid being in a position of considering their compliance status, only after they have to contact their legal representative to report a data privacy breach.

As was previously mentioned, being prepared saves your company's bottom line and reputation with customers.

Webinar Highlights (cont'd)

So from our experience, what happens if you have been breached? The law mandates that you disclose the breach to the regulators and all impacted persons within a set timeframe (72 hours in Barbados). After which there is the daily scrutinizing by the regulator, who will be tasked with assessing the breach and whether or not you followed the relevant guidelines. This puts additional pressure on companies as saving money is no longer the key objective and when the regulator says jump – you have to say how high.

> The Global Privacy by Design certification helps you to give your customers assurance that you respect their data. It also assists you with documenting evidence of having integrated data privacy best practices in areas such as your business operations, your retention of data policies, your consideration of consent and your secure storage of data. Thereby creating that defensible position for you and allowing you to achieve and demonstrate compliance – regardless of where your operations are located.

Embedding Technology: Protecting your data

In order to protect your data, you need to first understand the type of data you have, and know where it is located.

One pitfall is that persons are so focused on following the letter of the law, that they forget that data privacy is primarily about people and processes. So even though the legislation would not explicitly state that you must do data mapping or perform data lineage, in order to comply with the legal components of consent obligation, the secondary usage test and data minimization, these things should be incorporated into your daily procedures.

As it relates to embedding technology to achieve data protection, the fundamentals are important: zero trust principles, encryption and information rights management go a long way to allowing you and your data protection officer to sleep better at night.

Monitoring is an often overlooked area within IT operations, however, data privacy assessments are point in time and with the continually changing cyber threats and risk landscape, mechanisms should be implemented that allow for efficient continual logging, monitoring and raising of alerts in the event of an incident.

Webinar Highlights (cont'd)

Closing Remarks

Data privacy is coming, now is the time to get your house in order. Privacy is no longer just about policy and procedures, it is also about technology and people.

It is no longer sufficient to say that you are doing something, if it is not documented, then you are not doing it. It is good to have on hand the SOC reports and data privacy documentation, should it be requested by the regulator.

Regulators inspect what they expect, know what your risks are and take a prioritized look at what is high risk in order to have a defensible position in front of the regulator.

However, don't panic, your compliance journey is just that – a journey. Be aware of how much data you are carrying on your devices. Take small steps to help achieve the baseline.

Aim to right size your privacy program and embed data privacy champions. Remember to be privacy proactive, and have a culture of security by default.

Contributors

Sylvia Klasovec Kingsmill
Global Cyber Privacy Leader
Partner, Risk Consulting
KPMG in Canada

Ravi Sankar
KIG Head of Cyber
Principal, Advisory
KPMG in Jamaica

Kevin Boyce
Partner
Clarke Gittens Farmer
Attorneys-At-Law

Contact us

Ravi Sankar
KPMG Islands Group, Head of Cyber
Principal, Advisory
KPMG in Jamaica
T: +1 876 822 0708
E: rsankar@kpmg.com.jm

Allison James
Manager, IT Advisory
KPMG in Barbados & the Eastern Caribbean
T: +1 246 826 2247
E: allisonjames@kpmg.bb

kpmg.com/socialmedia