Data Protection

An interview with Stuart Jamieson, Chief Executive Officer of Obeden.

Stuart Jamieson, CEO, Obeden.

Can you briefly explain the term “Data Protection”?

Data protection is the process of safeguarding the personal information of your customers. It is the responsibility of each organization to ensure that you put in controls to protect personal data when you process them for your business transactions.

As an organization, you will be held accountable for those controls if, at any point, an issue occurs where personal data becomes exposed, either through an accidental, negligent or criminal act.

How did personal data protection regulations come into effect globally?

Any organization, regardless of its geographic location, either collect, process, or store personal data. In the early 70’s, the first modern data privacy law came into effect in Germany in reaction to growing concerns about computing advancements and privacy in processing personal data. In 1973, Sweden’s Government implemented the first national privacy law known as “Data Act”, and by the early 80’s, most of the EU/EEA member states had introduced data protection laws as fundamental rights into their legislation.

As computer technology grew and advanced in the early 1990’s allowing the free flow of information via the worldwide web, the European Union enacted in 1995 the Directive on Data Protection; this adopted the minimum standards among member states on how personal data is managed and moved or transferred between EU member states.

Most countries now understand the need to control the use of personal data, and on the 25th May 1998, ‘The General Data Protection Regulation’ (GDPR), which was implemented by the European Union was introduced. This has now become the standard for most global privacy laws, and many governments worldwide have adopted a version of it.

The Data Protection Act of Sri Lanka, which was certified by the Speaker of the Parliament on 19th March 2022, is modeled after the EU’s General Data Protection Regulation.

How do you see the Data Protection Act of Sri Lanka compared to the EU’

General Data Protection Regulations (GDPR)?

I see similarities in many ways. The definitions adopted by the Sri Lanka PDPA are fundamentally the same as the EU's GDPR. The key principles and protections for people, the definitions, controls, and responsibilities of a Controller of Personal Data and a Processor of Personal Data look very much the same. This gives Sri Lanka a strong basis for Data Protection.

What are the key principles or obligations under the Sri Lanka PDP (Personal Data Protection Act) Act?

The following at the key principles:
1. Legitimacy – To process personal data for an explicit or specific purpose

2. Proportionality – Processing of personal information must be adequate, relevant and must be in relation to the purpose of processing

3. Accuracy – Personal information processed must be accurate and up to date

4. Retention Limitation – Personal Information should not be kept longer than necessary

5. Integrity – Organisations must ensure the confidentiality of the personal data collected

6. Transparency – The obligation to process in a transparent manner and enable customers to receive the information they request regarding the processing of their own information

7. Accountability – To implement adequate controls and procedures in place in a more responsible manner

These are fundamentally the same as you would find in GDPR.

How should companies in Sri Lanka prepare themselves to ensure they comply locally and internationally?
As the Sri Lanka Personal Data Protection Act is applicable to any individual or an organization that collect, process or store personal information of individuals either

Sri Lankan or foreigners.

Thus it will be the responsibility of such individuals or organizations to ensure they put the right processes and controls in place to protect the personal data under their management. Therefore, all commercial entities will require to adopt or implement a sound ‘Data Protection Management Program’ (DPMP). They are also required to designate or appoint a Data Protection Officer, where necessary, to ensure the DPMP is implemented across the organization. As has been noted with the rollout of GDPR, staff training will be a key as they are the weakest link when it comes to safeguarding personal data.

Why is staff training a big part of privacy?

We have seen in the past that whether you are an SME or a large global entity if you have not provided adequate and continuous training to your staff on data privacy regulations, you will be vulnerable to data breaches. This can have a significant impact on your business operations.

For example, in 2020, British Airways were fined 22 million pounds for failing to protect the personal data of over 400,000 of their customers. Marriott International was fined 20 million pounds for 339 million guest accommodation records and in Singapore, the regulator fined S$1 million on SingHealth for failing to safeguard the health records of its patients.

All of these incidents would have been prevented if there had been proper staff training had been carried out.

Is it mandatory to appoint a Data Protection Officer (DPO)?

As per Sri Lanka Personal Data Protection Bill (Part 3, Chapter 20), it clearly states that any organization that acts as Controller or Processor of Personal Information shall designate a Data Protection Officer for the organization.

Is it possible to outsource the services of a DPO?

Yes. It is possible to outsource the function. But not the responsibility. The responsibility lies within the organization.

What are the considerations for companies when managing personal data?

Organizations need to understand what types of personal data they collect within their organization and how they use it. Once you have a clarity on types of data you have in your systems, then it is becomes easier to put processes and controls in place to manage that data. These processes and controls, along with assessing your suppliers, and training your staff combine to provide the fundamental basis for a Data Protection Management Program. It should be noted that any organization with one employee will be holding personal data and, therefore, will be required to have a Data Protection Management Program in place and a Data protection Officer to enforce it.

What are your thoughts on how Sri Lanka has fared with privacy regulations in the South Asian region?

Sri Lanka has always been an exciting destination in the South Asian region. It became the first nation in the region to enact comprehensive privacy legislation. It is crucial when doing business globally that you understand your responsibilities in global data protection.

Can you explain about fines and penalties imposed?

Sri Lanka PDP Act states a maximum fine of Ten Million rupees for non-compliance. Non-Compliance will be reviewed by the Sri Lankan data protection organization, and the fines will be assessed depending on the compliance level of the organization. Such as how the organization responded to a data breach and how effective the processes and controls the organization has to protect personal data.

In comparison, the European privacy regulator imposes a maximum fine of €10 million or 2% of a firm’s annual revenue, and in Singapore you would see financial penalty of up to SG$ 1 million or 5% of the organization’s annual turnover, where the organization’s annual turnover exceeds SG$ 20 million.

For the moment, the fines and penalties that can be imposed by the Sri Lankan Privacy regulator can be described as reasonable but can be expected to be increased over time.

Having said that, even if the fine is relatively low in comparison to GDPR, and organization that fell foul of the regulations would have a significant impact to its

reputation both publicly and privately.

What is usually expected from the regulator in the first year once the data protection authority has been established?

In the first year of operation generally a regulator will be building its organization as well as providing education and information to the organizations. It can however be expected that the regulator may want to make an example of organizations who are deliberately not following the regulations.

What are the restrictions of processing data outside of Sri Lanka?

Processing of personal data outside the territory of Sri Lanka is restricted to public authorities except if it is made under an adequacy analysis.

So for commercial organizations, processing data outside Sri Lanka will be possible if it is cleared through the regulator and analysis of the adequacy of the privacy regime of the country where the data will be processed is shown to be sufficient.

There are also a few exceptions to this for commercial organizations, one of which includes consent to process overseas through a written agreement with the owners of the data.

As a global player in privacy compliance, what opportunities do you see for Obeden and how do you wish to assist companies in Sri Lanka?

Obeden has been focused on providing support for organizations as they create or review their data protection standards. With significant experience in GDPR, UK GDPR, PDPA and other data protection legalization, we see being able to provide our expertise to Sri Lankan organizations as they adapt to the new Data Privacy laws being introduced.

Both through educational opportunities and direct support and software as a service platforms, we are looking forward to providing the first Sri Lankan PDP Act solutions to the Sri Lanka market space. Protecting organizations from potential fines and helping organizations protect the Sri Lankan people’s personal information that they hold and process.

support@obeden.sg