FEATURE STORY 2 : RECENT DEVELOPMENTS IN DATA PROTECTION LAWS IN THE WORLD AND PERSONAL DATA PROTECTION LAW IN SRI LANKA

Janith Wijekoon

Attorney-at-Law,

LL.B (Hons)(London)

RECENT DEVELOPMENTS IN DATA PROTECTION LAWS IN THE WORLD

Physical compartmentalizing of legal documents and case records has become a cumbersome task especially due to Courthouses being flooded with cases and vital information being piled up in public authorities. Law evolves constantly and with each passing day, a new area of Law is developed and legal documents and records are being rapidly archived in order to keep track of these developments which make physical access to legal documents and records ever so difficult. Just as much the field of Law needs growth, compartmentalizing of legal documents and records that comes as part and parcel of this growth needs advertence.

Compared to the other countries in the World, more often than not, Sri Lanka has been a follower rather than a leader in the area of legal evolvement. Sri Lankan Legislature's lackluster approach towards addressing this issue of compartmentalizing legal documents and records have resulted in Courthouses and public authorities being jammed with age old files and briefs which has created an environment for spiders to thrive on. It is long past time for the Sri Lankan Legislature to realize this issue and to come up with an expedient solution to address the same whereas other Countries have already implemented or have sought to implement methods to overcome this challenge.

Storing data electronically has become the method to which most countries in the world have appealed and thus far, it seems to be that it is the safest and the most expedient method too.

However, all the countries that have chosen to store legal documents and records electronically have introduced and placed Laws that enable them to protect the data that is being stored. This is so because storing data without having Laws to protect such data is similar to standing in the middle of a battleground unarmed. You know you are bound to get shot sooner than later. Ironically, the development of Data Protection Law and the legal suits that may follow in relation to same is in itself a legal evolvement, the records of which need protection.

Data Protection in Europe

The European Union, which is the overarching governing body for 28 European Countries has already initiated and placed a major Law on Data Protection replacing the "*Data Protection Directive 95/46/ec*". The General Data Protection Regulation (GDPR) took effect on May 2018 and almost all the member Countries have implemented domestic Laws to supplement the GDPR. Germany and Spain have opted not to incorporate GDPR into their jurisdiction but have enacted their own laws which underscore the fact that, while there is uniformity among the member countries in recognizing the issue of data protection, there is no complete uniformity when it comes to implementing Laws to remedy the same.

Primarily, GDPR mandates a threshold set of standards for the companies that manage EU citizens' data for better protection of the processing and movement of citizens' personal data. The following are some of the key privacy and data protection requirements of the GDPR;

- Requiring the consent of subjects for data processing.
- Anonymizing collected data.
- Providing data breach notifications.

Merely months after its implementation among the member countries of the EU, the GDPR is responsible for the world's largest data protection fine. CNIL, the French watchdog for data

protection, imposed a fine of 44 million pounds on Google LLC for failing to provide users with transparent and understandable information on its data use policies. It was alleged and proved that Google made it difficult for its users to find essential information "such as the data-processing purposes, the data storage periods or the categories of personal data used for the ads personalization" by splitting them among multiple help pages and settings screens. [1]

Although the introduction of GDPR is most certainly a step in the right direction, it does have its flaws which have resulted in over 59,000 reported data breaches across Europe since its advent. The Netherlands top the list and Germany and the UK are among the top rankings for reported data breaches.[2]

Despite these challenges, the initiative taken by the EU to protect one's data is commendable and the GDPR can be regarded as a stepping stone towards achieving a more comprehensive authority to govern data protection.

Data Protection in the USA

The USA, arguably the quintessential information technology hub in the world, lacks a central data protection authority which may come as a surprise to most of us. However, federal enforcements have taken place in certain States to protect data of the persons living in such States. The California Consumer Privacy Act (CCPA) is one such enforcement.

The CCPA provides certain privacy rights to individuals and among them the right to access and deletion, the right to know how a business has collected one's personal information in the previous 12 months and the right to opt-out of the sale of your personal information are worth mentioning. CCPA also enables an individual to bring a private action in relation to any violation

[1] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google llc
[2] https://www.dlapiper.com/en/germany/news/2019/02/dla-piper-gdpr-data-breach-survey/

of certain unencrypted personal information and given the liberal judicial approach in the US, this private right of action is expected to give rise to a significant number of class actions.

The CCPA, being the first of its kind in the USA, has most certainly laid the foundation for the implementation of a more comprehensive Data Protection Law in the other States of the USA.

Data Protection in other jurisdictions

- **Brazil** has proposed to implement its own data protection Law, which is called the General Data Protection Law, in February 2020. Similar to the GDPR, this Law applies extraterritorially and similar to the CCPA this Law grants an individual the right of access, rectification, deletion and data portability.

- **Bahrain** is the first Middle East country to implement a comprehensive Law solely dedicated to data protection by Law No. 30 of 2018 (Personal Data Protection (Data Protection Law) which has come into force on August 1st 2019. Prior to this enactment, Bahrain had implemented various Laws that dealt with number of issues pertaining to data protection such as the Constitution of Bahrain (Right to privacy), Legislative Decree No. 54 of 2018 with respect to Electronic Letters and Transactions and Decree No. 16 of 2014 with respect to the Protection of Information and National Documents to name a few.

- **India** – the most anticipated Law on data protection in 2019 is currently in the process of being drafted by the Committee of Experts chaired by Justice B.N. Srikrishna. The Committee has already tabled a draft bill to the Central Government titled Personal Data Protection Bill on 27th July 2018. In **Justice K.S. Puttaswamy Vs. Union of India 2019** the Supreme Court of India while holding that "*the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of*

the Constitution" also reiterated the need for a comprehensive data protection regime to achieve the same.

Most of the Laws cited above deal with data protection of individuals and Sri Lanka is in dire need of Laws that protect personal information that is being stored electronically as well as Laws which provide for the protection of legal documents if and when the Legislature decides that they be stored electronically. If in the future, the Legislature or the Judiciary for that matter decides to store legal documents and records electronically in an electronic device, Laws must be put in place to prevent such documents being tampered with externally. Hence, the implementation of an all-embracing Data Protection Law in Sri Lanka is long overdue in order to facilitate and safeguard the critical information that is stored electronically.

Proposed Personal Data Protection in Sri Lanka

Personal data protection in Sri Lanka has been a non-existent concept until the ministry of digital infrastructure proposed a framework for the protection of personal data act in May 2019. However, this proposed act still hasn't reached the parliamentary bill stage as at November 2019.

Personal data protection in Sri Lanka therefore is currently dictated by ad hoc rules that may be found in other statues or licences and regulations that are directed at relevant organisations. Sri Lanka entities that process data of European residents are however faced with the stringent obligations imposed but the General Data Protection Regulation of the European Commission.

GDPR

The General data protection Regulation (GDPR) has been hailed as the toughest personal data protection legislation enacted. This is primarily for two reasons; the harsh penalties imposed as well as the territorial breadth of the law. As per S. 3 of the GDPR not only are organisation that process data of European residents based in Europe bound to comply but organisations that are not based in Europe are also bound by obligations if they offer goods and services to European residents or they monitor the behaviours of European residents. Furthermore, the individuals that are offered protection of the regulation are not defined by citizenship, but it extends to anyone who is present in a European country.

The GDPR's sharp teeth have been seen by the heavy penalties that have been faced by top corporations such as Facebook, Google, YouTube, Marriot Hotels and British Airways for failure to comply with obligations of the GDPR or for data breaches that have occurred.

Therefore, if a Sri Lankan company offers goods or services to EU residents or if it monitors the behaviour of EU residents it is bound to comply with the obligations imposed.

Proposed SL Data Protection Act

The proposed SL act is more or less a replication of the GDPR save some minor changes.

The Framework was introduced by the Ministry of Digital Infrastructure early in 2019 and has gone through several drafts and public consultations thus far. The framework sets out two sets of entities covered to be covered under the obligations imposed: controllers and processors. Controllers are parties that have control over and decide as to the processing activities that should take place on the personal data. Processors are parties that process data only o the instructions of controllers. If a processor deviates from these contractual instructions, not only will he be in breach of contract, but he will also be considered to be a controller and will have to comply with all the obligations at a controller has. The Final version has several changes from the original draft, key being a provision which dealt with registration and a registration fee associated with controllers.

A key feature seen in both the SL framework and the GDPR is the extremely wide definition for processing activities. Under the SL framework 'processing' means any operation performed on personal data including but not limited to collection, storage, preservation, alteration, retrieval, disclosure, transmission, making available, erasure, destruction of, consultation, alignment, combination, or the carrying out of logical and/or arithmetical operations on personal data. There are however two exceptions where the act will not apply, namely where the data is anonymised, or the processing is for household activities.

There are 6 primary legal ways to process data; if the data subject has given consent; processing is necessary for the performance of a contractual obligation; processing is necessary to comply with a legal obligation; processing is necessary to respond to an emergency; and processing is necessary for a legitimate interest of the controller.

An aspect of the SL framework which is not seen in its exact form in the GDPR is schedule 5 which deals with a notice that has to be provided to the data subject before his or her data is processed. It is however similar to the privacy notice that has been required under the GDPR.

Both the GDPR and the SL Framework mandates the institution of a new office' namely the Data Protection Officer. This individual will be tasked with being in charge of ensuring the controller or processor complies with the obligations imposed.

Under the GDPR, data subjects have 8 rights. The right to be informed; the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object and rights in relation to automated decision making and profiling. Under the SL Framework data subjects are afforded the right of access, the right to withdraw consent, the right to object to processing, right to rectification, right of erasure, and rights in relation to automated decision making.

Finally, in relation to the penalties although the SL framework initially was identical to the heavy fine structure of the GDPR (€20 million, or up to 4% of the annual worldwide turnover of

the preceding financial year, whichever is greater) it now has in place the issuance of a warning in the first instance. Notwithstanding this provision the controller or processor is liable for a penalty not exceeding a sum of rupees ten million in any given case.

As has been seen with the GDPR the difficulty of data protection legislation comes with responding to data subject's rights and requests as rights such as the right to erasure entails a heavy technical investment by the controllers or processors.

Conclusion

With the development of digitalisation of one's information, the need to protect such information also arose and Laws on data protection gradually gained prominence as the frontrunner that could address this need. Most of the EU Countries and presently the Middle Eastern and Asian Countries have realised and understood the value of implementing Laws on data protection and have placed mechanisms to achieve a comprehensive Law on data protection. Sri Lanka on the other hand did not give much consideration towards developing Laws on data protection until 2019 and with the proposed Act, Sri Lanka is making an attempt to come into the fold albeit other Countries have already begun the journey. Nevertheless, a much needed legislation has now been tabled, subject to the approval from the Cabinet to fill in the void and this attempt by the Legislature should be appreciated and it must be taken as a stepping stone to achieve a better piece of legislation, if needed, in the future.