# Data Protection Laws and Compliance Requirements - Analysis of Laws from Europe, Singapore and India

**Adv. Prashant Mali, Founder & President – Cyber Law Consulting(Advocates & Attorneys)**

**Abstract**

The modern era has become severely riddled with cyber-crimes, and other offenses related to identity theft and data protection have gained impetus in the passing years. Where at one hand, the data-related tasks have become indispensable for our day-to-day transactions, the integration of communications and transfer of data and online transactions has increased the risk of these incidents of crimes happening manifold as compared to the erstwhile offline work. Reacting to the need, several countries have enacted their own versions of their respective data protection regulations, with the aim of enforcing stringent compliance requirements upon the individuals and corporate entities alike. However, some of the regulations enacted have had a worldwide impact, such as the General Data Protection Regulation passed by the European Union. The author has conducted a review of the regulations, with reference to few other regulations, such as the Personal Data Protection Act, 2012 of Singapore, so as to assess how effective and similar the General Data Protection Regulations are. The author has also taken into account the provisions of compliance requirements that are similar, as well as different in both these regulations. The compliance requirements have been assessed from the perspective of the corporate entities. The author has also included a short introduction of the data protection regulations existing in India and the prospective developments that may be seen in the regime since it is still in a nascent stage at present. The aim of the author is to assess if any similarity exists in the three regulations when it comes to compliance requirements, and the author has concluded the assessment by presenting an opinion regarding the same.

**Keywords** – Data protection, regulations, compliance, privacy, law, GDPR, PDPA.

## INTRODUCTION

Communications and all data-related tasks have become an integral part of our lives, and no digital transaction of the contemporary world is untouched by this influence. Where the electronic transfers are becoming easier and quicker, as they are becoming extremely facilitated by the advent of internet services, this facility does come at its own costs, since the risk of hacking, fraud, data theft and other related

cybercrimes has also increased along with it. As opposed to the other paper works, which are done offline in the usual course of events, the risk is magnified manifold with the advent of technological transactions and transfer of data between the users. There have been several estimates that the cross-border flow of data has become 45 times more in 2014, as compared to what it was in 2005, and as much as 12 per cent of the international trade that takes place, especially of goods, is carried over e-commerce platforms, which are the likes of Alibaba and Amazon (Manyika, 2016). The US International Trade Commission estimates that in 2014, global digital trade, including data processing and other data-based services, led to a more than 3.4 percent increase in US Gross Domestic Product (GDP), by increasing productivity and lowering the costs of trade.2 These estimates underscore the importance of cross-border data flows for the diffusion of knowledge and technology and for enabling the fragmentation of production of goods and services across countries (US International Trade Commission, 2018).

The issues related to Data protection have already gained limelight in plenty of countries around the world, and several of them have already acted on the issue by developing their own regulatory frameworks to tackle the problem of data protection. The most recent change that the world of data protection witnessed was the GDP Regulations passed by the European Union, which tended to send ripples of impact down to almost every country, causing them to adapt to the changes as mandated by their new compliance requirements. The EU Regulations on Data Protection have been in development for quite a long time now, and thus, are a well-researched and advanced set of regulations. In contrast to the Personal Data Protection Regulations of Singapore passed in the year 2012, the GDPR can be termed to be a significant upgrade of the principles enshrined in the PDPA. The companies around the world have been thrown into a hassle to ensure compliance with the new upgrade regulations in order to function in a proper manner. However, a change such as where the global regulatory bodies adapt their regulations in accordance to the ideology of the European GDPR is a rather high hoped move, since the EU's conception of privacy is more centric around the ideology of it being a fundamental human right (Kuner, 2017). This conception is rooted in the deep history and culture of the European Union, and it is not exactly a perspective that the other countries in the world will necessarily share (Whitman, 2017).

In comparison to these countries, India is more in the sense of a nascent bird, with little going on with it in relevance to the concern for data protection. The Indian regulations for the same are still under

deliberation, and have been modelled more or less in the same manner as the GDP Regulations, but are still a long way from being implemented. This article explores the compliance requirements of the three distinct regulations from the perspective of corporate entities, and thereafter, refer to them in order to find if all the regulations, i.e. the GDP Regulations, the Personal Data Protection Act and the Personal Data Protection Bill (India), have any element common in them with relevance to the corporate entities.

The article has been divided into three main parts, where the first three parts tend to elaborate upon the various aspects of the regulations discussed here. The fourth part deals with the elements that can be seen as common to all the three regulations, while the last part forms the conclusion of the opinion of the author in regards to the same.

## PART I – The General Data Protection Regulations

The European Union's General Data Protection Regulation (GDPR, 2016) lays great impetus on the fact that the personal data of any individual is important and thus, from every perspective, the GDP Regulations have been structured in a manner as if dealings with data required a great deal of planning. The GDPR, adopted by the EU in May 2018 to replace the earlier Data Protection Directive, reflects the importance of privacy as a human right and its significance in the EU (Schwartz & Peifer, 2017). It expands the scope of the EU Data Protection Directive, with tighter privacy standards and greater extraterritorial application (Directive 95/46/EC, 1995).

The GDP Regulations became a law in 2016, but the same did not become enforceable until the year 2018 (GDPR, 2016). Before the GDPR, the Data Protection Directive of the European Union prevailed, which also laid the foundation for the GDPR as it is right now. However, the previous act had significantly poor enforcement and equally bad compliance. One of the major reasons why the GDPR in current has attracted the attention of the corporate entities is the fact that the regulations contain heavy fines for the lack or failure in compliance with the requirements as have been laid down, as well as also the incorporation of several external mechanisms so as to encourage compliance at the earliest possible by the corporate entities and other individuals as included within the provisions of the regulations. This has caused quite a spur on an international level, leading to the GDPR becoming one of the most sensational regulations, impacting almost all of the world. The expanse of the GDPR has been devised in a manner such that the electronic domain

becomes inviolable from unauthorized intrusion. In doing so, the regulations thus cover a wide variety of information-related problems (Foulsham, Hitchen & Denley, 2019).

The strategic design of the GDPR is such that it plants into the minds of the companies the importance of data, and the variety of possible use of this data in their activities. The design also puts these regulations almost equal to the regulations that tend to be taken seriously by the companies – such as the antitrust laws and other laws related to corrupt practices. There have been instances in the past where the companies indulged in wrongdoings related to data have been fined less than what they would pay to one of their employees, which is not that big of a motivating factor for the companies to comply with the laws itself. Contrary to those times, the current GDPR has a renovated penalty allotment and enforcement mechanism, as well as stringent compliance requirements which need to be followed by those which have been included within the ambit of GDPR (Jay Hoofnagle, Van Der Sloot, & Zuiderveen Borgesius, 2019)

GDPR applies to any organizations, which has been operating within the EU as well as any organizations outside the EU that offers good or services to customers or businesses in the EU. There are two different types of data-handlers the legislation applies to: 'processors' and 'controllers'. A controller is a "person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data", while the processor is a "person, public authority, agency or other body which processes personal data on behalf of the controller". If you were subject to the UK's Data Protection Act, for example, you'll likely need to be GDPR compliant, too. "You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR," says the UK's Information Commissioners Office, the authority responsible for registering data controllers, taking action on data protection and handling concerns and mishandling data. GDPR ultimately places legal obligations on a processor to maintain records of personal data and how it is processed, providing a much higher level of legal liability should the organization be breached. Controllers are also forced to ensure that all contracts with processors are in compliance with GDPR (Palmer, 2019). There are several other definitions that can be noted as important, such as what does the regulation include within the ambit of *'personal data'*, which has been defined as, *" the personal information means information about an identified or identifiable natural person (" the data subject"'); an identifiable person is a person that can be directly or indirectly identified, in particular on the basis of the*

*ID such as first and last name, , identification number, location data, online ID or one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of the natural person" (GDPR, 2016).*

Personal data is collected online in multiple ways, including through ecommerce activities, use of social networks and twitter, through data observed from internet browsing, and location data from smart phones. Personal data can also be inferred from non-personal data when collected and analysed to produce a personal profile (World Economic Forum, 2014). As this taxonomy of personal data reveals, distinguishing between personal data and non-personal data is not straightforward. For instance, collecting data on habits, locations, and physical conditions may be used to create a personal profile of a person, even if each individual bit of data collected is not personal (US Federal Trade Commission Staff Report, 2015).

In regards to the impact the regulations will have on the companies, the authorities had given the specific companies a certain time period, within which the companies had to ensure that they were in complete compliance with the provision that had been included in the regulations.

Any company that stores or processes personal information about EU citizens within EU states must comply with the GDPR, even if they do not have a business presence within the EU. Specific criteria for companies required to comply are:

- A presence in an EU country.
- No presence in the EU, but it processes personal data of European residents.
- More than 250 employees.
- Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data. That effectively means almost all companies (Nadeau, 2019).

In addition to the companies that satisfy each of the above criteria, the GDP Regulations also tend to impact several other third party and customer contracts, placing equal liability on the data controllers, and the data processors as well. In Europe, data protection is increasingly seen as separate from the right to privacy. Data protection focuses on whether data is used fairly and with due process (G. Fuster, 2014), while privacy preserves the Athenian ideal of private life.

The GDPR extends territorial application beyond that under the Data Privacy Directive. One commentator described this as a 'dramatic shift in extraterritorial application' (Wolf, 2013). Another has described the application of GDPR globally as an 'illusion that EU data protection law can provide seamless effective protection of EU personal data transferred around the world' (Kuner, 2017).

The Directive preceding the GDPR was proving to be a troublesome directive for the European Union, since the harmony between the national privacy laws could not be maintained, and thus, several tech-giants began to abuse the existing loopholes, which urged a revamp of the directive. The GDPR took shape of the attempts made at revamping the older directive, and thereby in doing so, bridge in the gap which had been created in the meanwhile.

The GDPR now applies, first of all, to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing take places in the EU or not (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014). It also applies to the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the EU, where the processing of activities is related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union (GDPR Article 3). However, where the controller is not based in the EU, then the Regulation requires that the controller designate a representative in the Union (GDPR, 2016).

Recitals 23 and 24 of the GDPR provide additional context. According to recital 23, offers of goods or services online combined with use of an EU member's language and with opportunities to purchase are likely to constitute an offering for sale under the GDPR. Recital 24 of the Regulation elaborates on the meaning of 'monitoring' as occurring when 'individuals are tracked on the internet with data processing techniques which consist of 'profiling' a person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his preference, behaviors, or attitudes'. Taken together, this would appear to capture a large amount of what happens when people use the internet.

Since privacy regulations affect international data transfers upon which digital trade depends, developing countries could, in principle challenge the consistency of the GDPR with EU trade commitments in the WTO. However, WTO litigation is unlikely to address the underlying challenge raised by the GDPR—how

to preserve digital trade opportunities while maintaining nationally desired privacy standards. Nevertheless, WTO litigation could induce the EU to be more flexible in its application of the GDPR and offer other countries the opportunity to negotiate arrangements like the one with the USA (Department of Commerce, 2016).

## Part II – Personal Data Protection Act, 2012 (Singapore)

The Personal Data Protection bill was a result of the endless striving in the country, so that the country of Singapore may have a law related to Data Protection, and the string of efforts was endless. The state of the data privacy law before this act came into existence was worse off than it is now (Chik, 2005), it having considerably improved since the act having come into force. However, even though the law was for discussion in the Parliament in 2012, the law itself did not come into force until the middle of the year 2014.

The Personal Data Protection Act 2012 (PDPA) governs the collection, use and disclosure of personal data. The PDPA was passed by Parliament in October 2012 and came into force in 4 stages between January 2013 and July 2014. The PDPA recognises both:

- The right of individuals (natural persons, whether living or dead) to protect their personal data; and
- The need of organisations (all corporate bodies – e.g. companies – and unincorporated bodies, including those formed or resident outside of Singapore) to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

The objective behind Personal Data Protection Act, 2012 is so as to ensure that some base standards are put into place which would lead to curbing of the excessive, and at the same time, unnecessary collection of the personal data of the individuals, which happen to be collected by the businesses. The other objective of the Personal Data Protection Act is to ensure that certain requirements are also included as mandatory to be fulfilled, so as to obtaining the consent of the individuals becomes necessary for the business which do consensually record data, before such data is being disclosed by them (Iqbal, 2011).

The Act covers a relative inclusive definition of what is covered within the ambit of personal data, as well lays down any compliance that an organization operating within the border of Singapore will need to comply with. The following sections of this part shall discuss in brief the provisions of the Act itself. The PDPA establishes a data protection law that comprises various rules governing the collection, use, disclosure

and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. Personal data in Singapore is protected under the Personal Data Protection Act 2012 (PDPA).

*Business obligations under PDPA* - The 9 main obligations under the PDPA are (Singapore Legal Advice, 2018):

- **Consent Obligation**: your business can only collect, use and/or disclose the personal data of individuals who have consented to such collection, use and/or disclosure. Read more about the PDPA consent obligation in our other article.
- **Purpose Limitation Obligation**: your business can only collect, use and/or disclose personal data of individuals for the purpose(s) for which consent have been given by these individuals.
- 3. **Notification Obligation**: your business must inform individuals of the purpose(s) for which their personal data is being collected, used and/or disclosed.
- 4. **Access and Correction Obligation**: your business is obliged to provide information to individuals, upon request and as soon as reasonably possible, on:
    - What personal data of theirs is in your business's possession or under its control; and
    - How such personal data has been used or disclosed within 1 year before the date of the request?

  Your business must also correct errors or omissions in the personal data that is in its possession upon request, unless it is reasonable to not make the correction.

- **Accuracy Obligation**: your business must make a reasonable effort to ensure that the personal data collected by the business is accurate and complete, if the personal data is likely to be:
    - Used by your business to make a decision that affects the individual to whom the personal data relates; or
    - Disclosed by your business to another organisation

- **Protection Obligation**: your business must put in place reasonable security measures to protect the personal data in its possession or control. This is to prevent risks such as the unauthorised access, collection, use and/or disclosure of such data.
- **Retention Limitation Obligation**: your business should retain the personal data for only as long as is necessary for business or legal purposes.
- **Transfer Limitation Obligation**: if your business is transferring the personal data overseas, such as storing the data in the cloud, ensure that the transfer meets the PDPA's data protection requirements. This is to ensure that the data being transferred is offered a comparable level of data protection as is provided by the PDPA.
- **Openness Obligation**: your business must implement the necessary policies and procedures to fulfil its PDPA obligations. It must make information about such policies and procedures publicly available.

The PDPA does not prescribe the precise mechanisms by which organisations should obtain consent, although the PDPC notes that it is good practice to 'obtain consent that is in writing or recorded in a manner that is accessible for future reference' (Personal Data Protection Comission, N.D.)

## Part III – The Personal Data Protection Bill (India) & other Laws

In India, towards data protection, there indeed are provisions for the same. However, what is lacking is a unified and dedicated legislation and instead, the provisions are scattered across a multitude of legislations, as well as some constitutional decisions. Although India does not have a consolidated legislation such as the EU GDPR, or the PDPA in Singapore, or like the sectoral legislations that are found in several other countries for data protection, but this does not mean that India does not have any provisions in this regard at all (Singh, 2018).

1. *Information Technology Act, 2000 and SPDI Rules:*

The legal principles regarding data protection are contained in the Information Technology Act, 2000 ("IT Act") and the rules framed thereunder inter alia on matters relating to collection, storage, disclosure and transfer of electronic data (Information Technology Act, 2000).

The IT Act also prescribes punishment of imprisonment and/or fine for offences involving illegal downloading, destruction, alteration or deletion of data, introduction of viruses into computer systems, illegal access to computer systems, data theft, identity theft, cheating by personation, cyber terrorism, breach of confidentiality, privacy and disclosure of information in breach of lawful contract, to name a few (Pal Dalmia, 2017).

Specifically, with respect to personal data, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"), mandate adherence to specified procedures and measures by a body corporate, which processes, deals with, stores or handles sensitive personal information or data in a computer resource which it owns, controls or operates. Some of the key compliances under the SPDI Rules are as follows (Jheengan & Yadav, 2018):

- Obtaining prior written consent from the provider for collecting information, while providing an option to the provider to not provide such information sought from it and to also withdraw his/her consent given earlier in this regard.
- Taking of reasonable steps to ensure that the information provider has knowledge of the fact of collection, purpose of usage, intended recipients of the information and details of the agency that is collecting and that will retain the information.
- Personal information should not be retained for longer than is necessary for achieving the corresponding purpose or as is otherwise required under applicable law.
- Formulation and communication of a privacy policy for handling of or dealing in personal information.
- Non-disclosure of personal information to any third party without prior permission (unless such disclosure is required by law or has been contractually agreed with the information provider).
- Designation of a grievance officer for addressing discrepancies and grievances.
- Implementation and maintenance of reasonable security practices and procedures. The international standard IS/ISO/IEC 27001 on "Information Technology -Security Techniques - Information Security Management System - Requirements" is deemed to be reasonable security practice subject to certification by independent auditors.

- Information may be transferred to any other person that ensures the same level of data protection as provided under the SPDI Rules, provided that it is necessary for performance of lawful contract with the information provider or where such provider has consented to data transfer .

In addition to the IT Act and the SPDI Rules, depending on the entity collecting the data and type of data collected, several other India laws can also come into play when it comes to data protection. For instance, collection of financial information (such as credit card, debit card, other payment instrument details) is primarily regulated under the Credit Information Companies (Regulation) Act, 2005 and regulations framed thereunder along with the circulars issued by Reserve Bank of India, from time to time. In the telecom sector, certain data protection norms can be found in the Unified License Agreement issued to Telecom Service Providers by the Department of Telecommunications, and to deal with unsolicited commercial communications, the Telecom Commercial Communications Customer Preference Regulations, 2010 have been formulated. Data protection norms for personal information collected under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 are also found in the Aadhaar (Data Security) Regulations, 2016, which impose an obligation on the Unique Identification Authority of India (UIDAI) to have a security policy which sets out the technical and organizational measures which will be adopted by it to keep the information secure (Fossoul, de Villenfagne & de Terwangne, 2005).

*2. New Data Protection Law on the Horizon:*

With the gamut of laws regulating collection and usage of various types of data, the data protection regime in India is still not exhaustive enough, and several concerns are being raised to further secure and adequately deal with the complex issues including loss of data and consequent privacy.

The Indian Government is however, seeking to further strengthen and equip its regulatory framework for data protection and privacy. Accordingly, a Committee of Experts under the chairmanship of former Supreme Court Justice, Shri B. N. Srikrishna ("Committee"), has been formed to study various issues relating to data protection in India, make specific suggestions on principles to be considered for data protection and suggest a draft Data Protection Bill. The Committee has accordingly released a white paper on November 27, 2017, on a data protection framework for India, seeking public comments. In January earlier this year, the Committee in collaboration with the Indian Ministry of Electronics & Information

Technology has also conducted stakeholders' consultation meetings at various Indian cities, to obtain their opinions and concerns regarding the issues raised in the white paper (Datermann & Gupta, 2018).

Earlier, the Personal Data Protection Bill, 2006 had been presented in the Parliament on October 18th, 2010, and it lapsed before it could even be realized into a law (Ananthapur, 2011). However, the aforementioned bill was brought into consideration later once again, as was confirmed by the then Minister of Communications and Information Technology, Mr. Ravishankar Prasad (Subramaniam, 2016). The draft bill which is still in consideration to become a proposed law, has some definitions which are worth noting, such as the definition of data, which has been defined to be what relates to a living, natural person, such that the concerned person can be identified with the help of additional data that the controller has, or is likely to have (Subramaniam, 2017).

The Indian government is in the process of developing privacy legislation. In India, an emphasis on community norms and other postcolonial priorities meant that so far, individual rights to privacy have developed incrementally through common law and some legislation (Justice K. Puttaswamy, 2012). Yet to date, India does not have a privacy regime that would be deemed adequate by the EU. In fact, in 2010, the Commission concluded in a White Paper that India did not provide an adequate level of privacy protection. As a developing country, India's approach to privacy may strike a different balance between managing the risks that use of personal data could result in a breach of privacy with the economic and trade potential of such data use. Furthermore, in a developing country with one-fifth of the population below the poverty line, India's thriving IT industry and export-oriented businesses present an important opportunity to engage in sophisticated services trade and stimulate economic growth.

After many delays, the Srikrishna Committee finally submitted the draft regulation to the Ministry of Electronics and Information Technology (MeitY) last week. Analysis by leading law firm Nishith Desai & Associates explains that once the MeitY finalizes the draft, it should place such a law in the public domain and provide stakeholders an opportunity to provide further inputs, before the law is placed before parliament.

With major government-driven initiatives such as Make in India and Digital India, the ramifications of a data security law can be far-reaching for the Indian technology sector. Now it's up to the Indian government to provide India its first data security law, which can revolutionize the Indian technology industry (Balaji, 2018).

There are several provisions in the Bill that are worthy of interest, as well as the fact that the Bill also introduces several concepts to the Indian Data privacy regime, which were not recognized by the existing laws. *Data Fiduciary, Data Principal* and *Data Processors* are few such concepts, which are equivalent to what the *Data Controller and Data Subjects* mean as they have been included in the General Data Protection Regulations.

The Draft also includes the definitions of what is data, and also lays down the valid and legal procedure for the collection of the data, which has been laid down in the Section 8 of the Draft Bill. The Section also lays down the procedure for the intimation/the notice which needs to be provided to the Data Principal. The provision also lays down that such a notice or intimation needs to be given every time any and all kinds of data is being collected, of the natural person.

Section 8 is a storehouse to various mandatory compliance requirements for the companies, where the provisions are also given in regard to the disclosures that any Data Fiduciary needs to make to the Data Principal when collecting any sort of Data. These disclosures include the reason for which the Data is being collected, the identity and contact details of the Data fiduciary who is collecting the data, as well as the fact that the Data Principal reserves the right to withdraw the consent for the collection of the Data. The intimation to the Data Principal regarding the existence of the right to withdraw consent is a mandatory requirement which the Data Fiduciary has to inform the subject about. The disclosure also needs to be made regarding the time period for which such data is going to be collected, as well as the time for which period the collected data shall be retained by the data fiduciary.

Section 10 further elaborates on this right of the Data fiduciary to store the Data, which lays down that the data fiduciary may not store the data for a period longer than reasonable, so as to satisfy the reason for which the data was being collected by the Data fiduciary.

Above all, the legislation also sheds light on the mandatory requirement of consent, which has been laid down in the Section 12 of the Bill. This section also lays down in detail the ways in which the said consent may be obtained from the data principal, and provides that the consent must be obtained no later than prior to processing of the said data which is sought to be collected. The Bill also talks about the rights of the Data Principal, which have been laid down in the Chapter VI of the Bill. One such interesting right, which is also seen in the other more deliberate data protection legislations around the world, and one which

has also been included in the Indian Data Protection Bill is the *Right to be Forgotten*, which has been laid down in the Section 27 of the Act. However, as a part of the Indian Data Protection Bill, it has been restrained to a certain limit. Contrary to the provision in the GDPR, where the data principal is allowed to erase his/her personal data, no such right has been included in the Indian Legislation. Rather, under the Section 27 of the Personal Data Protection Bill, the data principal is only given the right to restrict of discontinue to the continuous disclosure of the personal data of the data principal, but no such right to erase such collected data has been provided in the hands of the data principal.

However, the bill has also a reserved chapter for including the exceptions to the provisions of the Bill i.e. the Chapter IX of the Draft Bill. These exceptions have been included with the purpose to sustain and maintain the national security of the state of India, and thus, provides certain exceptions for the State/government in regards to the otherwise mandatory obligations on their part for the data privacy.

Although, prima facie, the provisions of the Bill seem to be more or less a rip-off of the provisions of the General Data Protection Regulations, but the bill does, however, differ from the GDPR in some respects—the most significant being the provision of criminal penalties for harms arising from violations of the bill, and the proposal to treat the relationship between a data processor and its consumer as a "fiduciary" relationship.

Nevertheless, these provisions in the bill would increase data protection obligations significantly. The bill would enforce economy-wide changes to the data collection, storage, and management practices of Indian businesses, as well as foreign firms that provide services within India. While the EU had a pre-existing privacy framework (the 1995 Data Protection Directive), the bill would be a novel data protection framework for India. The cost of compliance and data protection obligations would, therefore, be much higher for India. In addition, no systematic economic analysis of the proposed bill has been conducted yet to provide an accurate analysis of its overall impact within India.

In view of the cursory overview of the provisions that all the three aforementioned regulations contain, following is a table that contains a comparative analysis of the provisions, in a tabulated form (KPMG, 2018). This is an assessment based on the limited number of criteria, which could be found to be similar to the provisions that were present in the regulations. However, in no manner are these criteria exhaustive.

| Criteria | GDPR, 2016 (EU) | PDPA, 2012 (Singapore) | PDPB, 2018 (India) |
|---|---|---|---|
| **Applicability** | Applies to almost all organizations established within, or outside EU upon satisfaction of certain criteria. | Covers only the businesses in Singapore | Covers only the data being processed in India, and outside India, upon satisfaction of some conditions. |
| **Consent** | Chapter 2, Article 7 – Enumerates the conditions for a valid consent for data processing. | Section 13 – requires consent to be obtained before data is collected, processed or released. | Section 12 – Provides for the processing of the personal data only on the basis of consent. |
| **Breach Notification** | Chapter 4, Section 2, Article 33 – provides for a breach notification. | Does not have any provision for a breach notification. | Section 32 – provides for a data breach notification. |
| **Right to be Forgotten** | Chapter 2, Article 17 – Allows the data subjects to access, correct, block and even erase their personal data. | The PDPA only allows the data subjects to access their data, and make corrections to it, in certain circumstances, which is also subject to several exceptions, under | Section 27 of the Act allows the data principal to restrict or prevent any continuing disclosure of the personal data, subject to certain conditions. |

| | | | |
|---|---|---|---|
| | | Section 21. | |

**Conclusion -**

On the cursory overview, there seems to be minimal level of similarity in regards to compliance within the regulations. The PDPA was enforced four years prior to the enforcement of the GDPR, which obviously makes GDPR a significantly more advanced regulation, with modern concerns included in it to further the protection of data privacy. Thus, it is obvious that there will be a minimal level of similarity in the compliance requirements of the two regulations. As for the Indian legislation, which is still under development, the legislation tends to still be in a nascent stage, and continues to develop while it mimics the provisions included in much more advances and effective legislations. The efficacy of the legislation in India cannot be judged until a later point of time. As for the compliance requirements being common from the perspective of the corporate entities, there is very little to be noted as to being common, except for the limitation of transfer, which imposed by GDPR and PDPA alike, in regards to the data being sent out of the countries.

Indeed, it is pointless to hope that a majority of the legislations will be similar to the path which has been followed by the European Union in the drafting of the GDPR, since it is focussed mostly on the stringent nature of the repercussions on the event of violation. GDPR is mostly focussed on the protection of the individual privacy, which as has been discussed, is a fundamental right to the EU ideology. However, it is also a notion which is not widely popular among nations, and thus, there are bound to be several differences in how these legislations treat the issue of data protection amongst themselves (Bier & Beyerer, 2016).

However, despite the discrepancies in how these regulations treat the procedure or data privacy in itself, there are still some aspects amongst the regulations which tend to remain the same. Thus, it is worth noting that the notion of data privacy tends to resonate between the legislations, although the ways these regulations deal with it tends to be largely different.

**References**

Aaditya Mattoo, Joshua P Meltzer, International Data Flows and Privacy: The Conflict and Its Resolution, *Journal of International Economic Law*, Volume 21, Issue 4, December 2018, Pages 769–789

Ananthapur, Raghunath. (2011). India's new Data Protection Legislation. *8 SCRIPTed* 192, 2013.

Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', German Law Journal 18 (04) (2017), at 881.

Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', German Law Journal 18 (04) (2017), at 864

Christopher Wolf, 'Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation', The Future of Privacy Forum White Paper, January 2013, at 2

Department of Commerce Fact Sheet: Overview of the EU–US Privacy Shield, https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shield-framework.

Determann, Lothar & Gupta, Chetan. (2018). Indian Personal Data Protection Act, 2018: Draft Bill and Its History. Compared to EU GDPR and California Privacy Law. *UC Berkeley Public Law Research Paper*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3244203

Digital Trade in the US and Global Economies, Part 2, 4485 (US International Trade Commission, 2014) https://www.usitc.gov/publications/332/pub4485.pdf.

Directive 95/46/EC, European Parliament and the Council of the EU, 1995.

Fossoul, Virginie; de Villenfagne, Florence & de Terwangne, Cecile. (2005). *First Analysis of the Personal Data Protection Law in India: Final Report to the European Commission*. Retrieved from http://www.crid.be/pdf/public/5946.pdf

Foulsham, Mark; Hitchen, Brian & Denley, Andrew. (2019). *GDPR: How to Achieve and Maintain Compliance.* Routledge, 2019.

G. Fuster, Gloria. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Switzerland: Springer International Publishing.

General Data Protection Regulation (GDPR), Regulation EU 2016/679, OJ 2016 L 119/1.

Google Spain SL and Google Inc. vs. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Judgment of the Court of Justice of the European Union (Grand Chamber), C-131/12, 13 May 2014.

James Manyika et al., Digital Globalization: The New Era of Global Flows (McKinsey & Company, 2016), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004). Faculty Scholarship Series, Paper 649

Jay Hoofnagle, Chris; Van Der Sloot, Bart & Zuiderveen Borgesius, Frederik. (2019). The European Union General Data Protection Regulation: What it Is and What It Means? *Information and Communications Technology Law, 28*(1), 65-98.

Jhingan, Seema & Yadav, Neha. (April 4, 2018). *Worldwide: An Overview of Data Protection Laws in India and European Union.* Retrieved from http://www.mondaq.com/india/x/687750/data+protection/An+Overview+Of+Data+Protection+Laws+In+India+And+European+Union

Justice K S Puttaswamy v Union of India and Ors, Supreme Court of India, Writ Petition (Civil) No. 494. https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf.

KPMG Assets. (2018). *Indian Data Protection Regime – Close to Reality?* Retrieved from https://assets.kpmg/content/dam/kpmg/in/pdf/2018/08/personal_data_protection_bill.pdf.

Nadeau, Michael. (May 29, 2019). *General Data Protection Regulation (GDPR): What you need to know to stay compliant?* Retrieved from https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

Pal Dalmia, Vijay. (December 12, 2017). *India: Data Protection Laws in India – Everything You Must Know.* Retrieved from http://www.mondaq.com/india/x/655034/data+protection/Data+Protection+Laws+in+India.

Palmer, Danny. (May 17, 2019). *What is GDPR? Everything you need to know about the new General Data Protection Regulations.* Retrieved from https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Paul M. Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law', The Georgetown Law Journal 106 (115) (2017), at 128

Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, 12.5. [Key Concepts Guidelines].

Rethinking Personal Data: A New Lens for Strengthening Trust (World Economic Forum, 2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf.

Rishab Bailey and Smriti Parsheera, "Questioning the Means and Ends," NIPFP Working Paper Series, no. 242, October 31, 2018, https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf

Shamma Iqbal, Singapore to Introduce Data Protection Law (Inside Privacy, 13 May 2011), http://www.insideprivacy.com/international/singapore-to-introduce-dataprotection-law/.

Sindhuja Balaji, India Finally has A Data Privacy Framework – What Does it Mean For Its Billion-Dollar Tech industry, (August 3rd, 2018), https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/#63a9f7e670fe

Singapore Legal Advice. (December 27, 2018). *Essential PDPA Compliance Guide for Singapore Businesses.* Retrieved from - https://singaporelegaladvice.com/law-articles/essential-pdpa-compliance-guide-singapore-businesses/

Singh, Shatakshi. (2018). Data Protection – Protection of What, Protection From Whom and Protection for Whom – An Analysis of the Legal and Judicial Provisions in India and Abroad. *NLIU Law Review*, 7, 79-117.

Subramaniam, Aditi. (2016). The Privacy, Data Protection and Cybersecurity Law Review. *The Law Review*. Retrieved from - https://thelawreviews.co.uk/edition/1001264/the-privacy-data-protection-and-cybersecurity-law-review-edition-5.

Subramaniam, Hari. (May 15, 2017). Data Protection 2017. *ICLG*. Retrieved from https://iclg.com/practice-areas/data-protection/data-protection-2017/india

The Information Technology Act, 2000, No. 2, Acts of Parliament, 2000 (India).

US Federal Trade Commission Staff Report (2015), 'Internet of Things, Privacy and Security in a Connected World', at 14.

Warren Chik, The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on the Internet: A Comparative Case Study of Hong Kong and Singapore - Two Differing Asian Approaches, 14 IJITL 47 (2005)

Christoph Bier, Kay Kühne, and Jürgen Beyerer. 2016. PrivacyInsight: The Next Generation Privacy Dashboard. In Annual Privacy Forum. Springer, 135–152.