A Comparative Analysis of EU's GDPR and Indian PDPB towards Data Privacy of Employees

Dr. Jijo James Indiparambil
Sanjo College of Management and Advanced Studies (SCMAS)
Rajakkad, Kerala, India.

Abstract

The progressive and enlightened landmark judgment of Supreme Court of India on August, 2017 declared the Right to Privacy as a fundamental right, i.e., an intrinsic part of the Right to Life under Article 21 of Indian Constitution. However, the existing legal framework in India provides only limited protection for employee data privacy. Thus, a poignant dilemma aroused at the stark contrast between the spirit of the judgment and the bounds of employee privacy. The increasing sophistication in Information and Communication Technologies (ICT) with its concurrent capacity to collect, analyze and disseminate numerous and various data along with its wide and open execution in the workplaces have introduced an urgent demand for privacy legislation in India. A consequent critical situation underlines the real threat called data protection that entire humanity encumbers to individually shoulder. This study, therefore, critically compares the General Data Protection Regulation (GDPR) 2018 of European Union with the Indian Personal Data Protection Bill 2019 to understand the ideological and operational nearness and remoteness of legal framework provided to create data protection, and analyze it within the context of monitoring employees in the workplace. This comparative and analytic investigation creates an urgency to generate various programmes to help individuals clean up and cosmeticize their data personas.

Keywords: Data protection, data privacy, employee monitoring, data minimization, data flows.

Introduction

Individuals identify privacy issues in the private and public spheres of their employment due to the implementation of several Information and Communication Technology (ICT) platforms in national and international levels. The increasing sophistication in ICT with its capacity to collect, analyze and disseminate numerous and various data simultaneously and its wide and open execution in the workplaces have introduced an urgent demand for privacy legislation in India. For, an amounted data flows occurs more recurrently in Indian organizational workplace with the extensive use of information technology in the normal occupational functioning and especially its use of employee monitoring purposes. Hence, the current impediments of data processing and data protection are two sides of same coin that facilitate data privacy debate. The leading ambiguity over who is allowed to collect data, what data can be collected, what are the rights of the individual, and how the right to privacy will be protected, and the extent of personal information being held by various service providers, etc. intensify an augmented dispute over the subject matter. Hence, it is extensively recognized the need and integration of legal systems to generate the protection of employee data privacy. This paper, therefore, compares EU's General Data Protection Regulation, 2018 (GDPR) and Indian Personal Data Protection Bill, 2019 (PDPB), and lays down key ideas relating to the protection of natural persons with regard to the collection, holding and processing of personal data (private, professional, public) and analyses the same in connection with data privacy of employees.

The General Data Protection Regulation (GDPR) and Data Privacy

The General Data Protection Regulation (GDPR) is a European Union (EU) regulation to protect the personal data of its individuals in EU and the European Economic Area (EEA). It is the new data protection regulation from the EU, released in May 2016 and implemented on May 25, 2018 and this regulation replaces the 20-year-old Directive

95/46/EC, stipulating a variety of requirements around how and why data can be processed. Though it is indented to protect individuals against abuse of personal data in EU and EEA, it addresses the transfer of personal data outside the above EU and EEA areas when EU institutes a legal relationship or bond with them. For instance, foreign organizations that are not established in the EU, but process personal data in relation to either (a) offering goods or services in the EU, or (b) monitoring the behavior of individuals in the EU, will come under this regulation. The GDPR prioritizes that the collectors, controllers and processors of personal data must put in place appropriate technical and organizational measures to implement the data protection principles among the individuals. This confirms that those who handle the data must clearly disclose any individual or collective data collection or processing with a prior declaration of its lawful basis and purpose, the extension of the data, the duration of the data retention, and the justifiable reasons if it is being shared with any third parties.

Personal data is any information relating to an individual and his or her private, professional or public life. As per the Article 4 (1) of GDPR, the term 'personal data' denotes any information that is related to an identified or identifiable natural person. This definition includes any information one must assume or assigned to a person in any form by which he or she can be directly or indirectly identified. These data can be a name, identification number, account data, telephone number, credit card number, customer card number, IP addresses, appearance, and special characteristics that denote physical, physiological, mental, genetic, and other economic, socio-cultural identities, etc. It also includes highly sensitive data of persons such as genetic, biometric and health data and those data denoting a person's race, ethnicity, political, religious or ideological convictions and adherences, etc. Along with definition (Art. 4) of personal data, Art. 9 of GDPR illustrate and analyses the procedures of processing of special categories of personal data. The specific parameters (1) through technology design (Privacy by Design), i.e., having privacy undertaking in every processing of personal data, and (2) through implementation (Privacy by Default), i.e., applying strict privacy setting once a product or service is released without the intervention of the user, ensure the technical and organizational measures to be taken to protect the personal data. Art. 25 of GDPR demonstrates this notion of data protection by design and by default.

The notion of Consent, a volunteer agreement or submission to the proposal or desires of another, becomes the basis for privacy protection around the globe. The data protection laws generally secure the personal or individual privacy by insisting the properly expressed consent to collect or use any personal data. GDPR explains in Recital 40 that "in order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis." That means consent justifies, if at all, the collection, handling, and/or storage of people's personal data by a third party. Art. 4 (11) of GDPR defines consent of data subject as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." However, it also has to be noted that the consent is only one of the six bases (other measures include: contract, legal obligations, vital interests of the data subject, public interest and legitimate interest) for processing personal data mentioned in Art. 6 (1) of GDPR. That means, after defining (Art. 4) the consent, GDPR further explains the lawfulness of processing (Art. 6), conditions for consent (Art. 7,8), details on processing of special categories of personal data (Art. 9), and the derogations for specific situations (Art. 49).

The Right of Access or Right to Access is the right to obtain from the controller confirmation as to whether or not personal data concerning a person are being processed, and, where that is the case, access to the personal data (Art. 15 of GDPR). Essentially, that means, for example, consumers can obtain access to the personally identifiable material that has been collected about them or being processed, if so. This is one of the data subject empowerment measures widely used and often operated as per the Subject Access Request (SAR) to the data collector. Whereas Art. 12 of GDPR deals with transparent information, communication and modalities for the exercise of the rights of the data subject, number other Articles demonstrates the right of access by the data subject (Art. 15 of GDPR) and the transferring of data subject to appropriate safeguards (Art. 46 of GDPR). It is to be noted that the right of access allows the data subject to exercise further rights such as rectification and erasure and thus it holds a central role in GDPR. In addition to the right to erasure, the 'right to be forgotten' personal data ensures that the data subjects have the rights to obtain from the data collector or the data controller the erasure of personal data concerning them without undue delay if the data are no longer needed for their original processing purpose or when the consent is withdrawn or when there is no other legal ground for processing or keeping them.

However, this right to be forgotten is not unreservedly guaranteed and its usage is limited especially when this right collides with the right of freedom of expression and information. Art. 17 of GDPR addresses the Right to erasure ('right to be forgotten'), whereas, Art. 19 of GDPR concentrates on the notification obligation regarding rectification or erasure of personal data or restriction of further processing procedures of data. In the same way GDPR provides individuals a right to be informed about the collection and use of their personal data. , This right leads to a variety of information obligations by the data controller to collect, hold and process the data and thus it becomes the key transparency requirements under GDPR. The privacy information, such as purposes of data collection, retention period, third party sharing, the sources of data collection, etc. has to be adequately provided. This information has to be concise, transparent, intelligible, easily accessible, and must use the clear language to avoid any type of confusion or misapprehension. Art. 13 and 14 of GDPR explains the kind of information to be or not to be provided, respectively, when personal data are collected from the data subject.

International trade, business and cooperation stipulate the data transmission to other countries (Third Countries). The legitimacy of data transfer, however, depends upon several factors. The legality or the legal position of data transfer stands the first position of its examination. Though the processing of personal data is prohibited, the possibility of authorization (consent), which is freely given, functions as a loophole here (Art. 6 of GDPR) and makes it more ambiguous when reasons of contract fulfillment (binding corporate rules) and protection of central interests (public interests) play a vital role (Art. 9 of GDPR provides further information on legal requirements). Even if the general requirements of data transfer are fulfilled, the GDPR then looks for the worthiness of the country (secure or unsecure) to which the data processing has to be sanctioned. Countries having a suitable level of data protection (adequacy decision) or countries with personal data protection regulation comparable to that of GDPR will only be considered to permit the data transfer. In this way, a data processing control by both the provider and the recipient is ensured. Towards this, GDPR provides further suitable recommendations, such as provisions of codes of conduct (Art. 40), general principles for transfers (Art. 44), adequacy decision on transfers (Art. 45), transferring with appropriate safeguards (Art. 46), and derogations for specific situations (Art. 49).

The GDPR and Employee Data Privacy

How might the GDPR inform our perspective on the processing of personal data and data protection in an employment context? As researchers observe the GDPR does not protect employees from any particular data subject. However, it does affirm the importance of individual rights in the workplace and prohibit processing sensitive data in the labour field. The GDPR offers an example of how acceptable legal structures could be developed to achieve a more acceptable balance between the use of electronic surveillance systems and technologies in the workplace and employee privacy and data protection. Its aim is to protect citizens from privacy invasions and data breaches. The GDPR incorporates several fundamental principles, including transparency and fairness, guarantees specific rights to individuals, and warrants the exercise of those rights by organizations. It legally entitles employers to monitor employees, but on condition that employee's grant consent through advance communication.

The GDPR thus ensures the legitimate collection and processing of personal data as well as its limitation and protection. It is designed to protect the personal data of individuals, though it also applies to data control and processing and related activities. In order for the interests of employers to process employee data to qualify as legitimate and legal, the employer must balance the interests, rights and freedoms of employees. Likewise, the GDPR enables employers to establish compelling legitimate grounds to process data. It is argued, however, that the imbalance of power in organizations and in the employer-employee relationship makes it difficult to rely on employee consent to collect and process the data. For under such conditions, the legitimate interests of the employer or the data controller emerge as the deciding factor in an organizational context. In the same way, consent may be given unwillingly when employees face a potential negative effect from withholding consent.

Chapter II of the GDPR in Article 1 (a) guarantees that personal data shall be processed lawfully, fairly and in a transparent manner (fulfilling specific requirements by securing the data subject's consent or by another legitimate means prescribed by law or the legitimate interests pursued by the controller). This makes clear that the GDPR regards the lawfulness, fairness and transparency of data processing as of vital importance. Article 1 (b) states that personal data shall be collected only for specified, explicit and legitimate purposes and that the data collected should not be further processed if not compatible with those purposes (purpose limitation). It also seeks "data minimisation" in

Article 1 (c), where data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." This principle of data minimisation is significant in the DGPR, given that frequent data collection for multiple reasons and treatments is alarmingly on the rise in the domain of digital transformation and data exchange. Moreover, according to Articles 6 and 7, data controllers must perform an analysis and risk assessment (physical, logical and organizational) to ensure that the data to be collected is adequate, relevant, limited, accurate (inaccurate data must be rectified), and not stored beyond a reasonable date. The values of confidentiality (against accidental loss, destruction or damage) and accountability (controller responsibility) are similarly ensured by the GDPR. The GDPR also provides tools to guarantee that data subjects are free to decide upon which of their personal data can be collected and processed to define their "personal identity," and thus secures the rights of data subjects to receive transparent information and communication (Articles 12-15).

Article 16 provides data subjects the right to rectify inaccurate personal data. It also guarantees the right to erasure when the collected data is no longer necessary in relation to the purpose for which it was collected or processed. If data is collected unlawfully, the data subject may withdraw consent on how that data is processed. It also includes a right to restriction of data processing (Article 18), a right to data portability (Article 20), and a right to automated individual decision-making (Article 21). This automated individual decision-making includes profiling. The GDPR strengthens and confirms the freedom and rights of data subjects, the right to live without arbitrary and unwarranted interference, intrusion or limitation, and thus the right to individual profiling. As a continuation of this, Article 35 treats any excessive use of electronic monitoring (such as CCTV monitoring) to profile employees as "high risk" profiling. According to this article, excessive electronic surveillance results in a high risk to the rights and freedoms of natural persons. Such profiling further requires a Data Protection Impact Assessment (DPIA) to demonstrate the need for and proportionality of the employer's interests in seeking employee data. For instance, Article 35 (1) states that "where a type of [data] processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data." Given this requirement of a systematic and extensive evaluation of personal aspects, it is clear that the rights and freedom of natural persons are highly valued by the GDPR.

Articles 45-50 outline legal measures for transferring personal data to a third-party, whether to countries or to national or international organizations. Article 45 (1) speaks about data transfers on the basis of an adequacy decision, ensuring that the third-party will provide an adequate level of protection for the data. This adequacy level is determined by several factors, including the rule of law, respect for human rights and fundamental freedoms, relevant general and sectoral legislation, public security, etc. Articles 46 and 47 respectively state, that a data controller or processor may transfer the data subject to appropriate safeguards and that this should be done by means of binding corporate rules. However, according to Article 49, when the adequacy decision and binding corporate rules are absent, the explicit consent of the data subject must be obtained for any data transfer. Based on the preceding elaborations of the GDPR, employee monitoring has to be in compliance mainly with the principles of data protection, including, as already discussed, lawful and fair processing, transparency, purpose limitation and necessity (data minimization), proportionality, integrity and confidentiality. Providing adequate protection of personal data in a work context is among the safeguards meant to ensure the privacy of employees. Within the workplace context, the employer is classified as a data controller with regard to its employees' personal data. For this reason, applicable data protection rules are directly relevant to workplace privacy. However, we have already noted concerns over the legitimate interests and practice of data protection. The above mentioned GDPR enforcement priority areas are expressed in Exhibition 1.

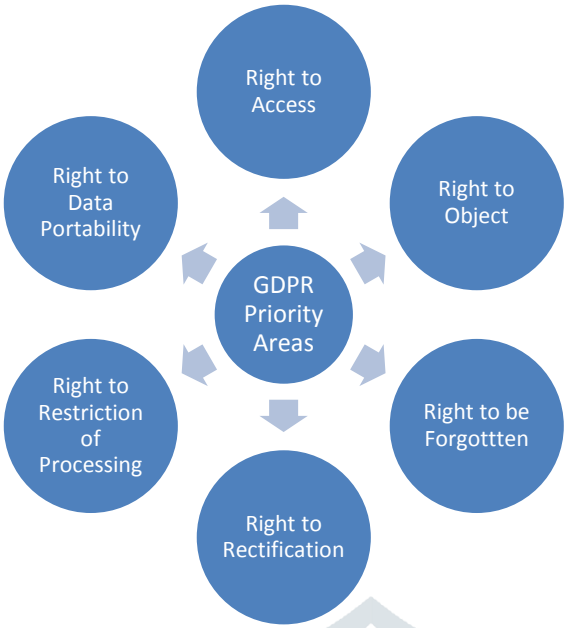

Exhibit 1 - GDPR Priority Areas

The indicated ambiguity of the data subject's consent – whether it is freely given, with full knowledge, with specificity, based on prior information, etc., along with the nature of the relationship between employer and employee – puts in question the legitimacy of employee monitoring and data processing. It is to be noted in this regard the notion of "notice and choice" stated by Daniel Solove. For him the important component of privacy management is the adequate information given to the individual (notice) about the data collected and used as well as allowing him or her to decide whether they accept (choice) this data collection and use (Solove 2013). The nature of the data to be processed also matters, having adverse effects on employees, when it comes to highly sensitive and confidential data about an individual employee. It is also needed to establish the impact of monitoring on employees, including individual risks and concerns (privacy related identity manipulation) as well as social ones (power distance, discrimination). The GDPR (Recital 75) in this regard provides a list of possible risks in data processing and managing: "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; or where processing involves a large amount of personal data and affects a large number of data subjects."

Therefore, any assessment of the impact of employees' data monitoring requires an assessment of these risks and their applicability to the proposed monitoring. A key contribution of the GDPR in employee monitoring is that "it marks a fundamental change in the balance of power between organisations and individuals in the collection, processing and storage of personal data elevating individuals' right to access and control use of their personal data" (Goddard 2017, 705). With the advent of the GDPR as law, rather than merely a recommendation, the notion of a right to privacy in the context of data is particularly well-defined. Now, the question is about the correlation between the data protection principles noted above and their relative weight in balancing employees' rights to privacy and freedom with employers' legitimate interests. This has to be further researched based on other potential and actual impacts of these practices on both employers and employees. The following section includes some concerns of data privacy based on a proposed privacy Protection Bill in India.

India's Legal Frameworks including PDPB 2019 Governing Employee Monitoring

The general surveillance systems in India function in various agencies and departments of the Indian central Government. These include: *National Intelligence Grid* (NIG), *Crime and Criminal Tracking Network System* (CCTNS), *Central Monitoring System* (CMS), *Unique Identification Authority of India* (UID Scheme), *Indian Computer Emergency Response Team* (CERT-In), and *National Counter Terrorism Center* (NCTC). Though these agencies administer and exercise their functions with specific rules and regulatory norms pertaining to each

department, the lack of central specific laws governing surveillance in India forms further hindrance to its general application. To contextualize this issue, the advent of globalization and its consequent liberalization and privatization marked the shift in labour laws and policies with a global framework, which prompted to adopt and adapt new measures to handle the current nuanced labour situations and challenges. The increased mass surveillance, which is made possible by the technological advancement, creates along with its benefits an extensive infringement of privacy and individual liberty. In this milieu of invasion into the human rights and interests, it is untoward and regrettable to be deficient in the specific laws governing surveillance in India, especially in the corporate and organizational workplace context.

Though there is no adequately establishment upon the specific laws concerning or permitting employee monitoring and the regulation of processing personal data of employee in India, Article 21of the Indian Constitution, entitled "Protection of Life and Personal Liberty," states that no person shall be deprived of his life or personal liberty except according to procedure established by law. It assures the right to live with human dignity, free from exploitation and intrusion by others. Hence, the right to privacy is implied in this right to life and liberty. However, Indian legislature has passed certain rules and acts that indirectly govern surveillance, such as the above mentioned Information Technology Act 2000 ("IT Act"), Information Technology Amendment Act 2008, Indian Telegraph Act 1885, information Technology (Procedure and Safeguard for interception, Monitoring and Decryption of Information) Rules 2009, and Right to Privacy bill 2011. These acts deal with the digital and telephonic surveillance in general. The Information and Technology Act 2000, which is amended in 2008 and named the Information and Technology (Amendment) Act 2008, reaffirms the fundamental right to life and liberty (including right to privacy) as guaranteed by the Indian Constitution. This requires the prior consent of employees before collecting and processing personal data. As primary law dealing with cybercrime and electronic commerce, IT Act 2008 provides legal frameworks for electronic governance and monitoring computer/network records and data. It defines cybercrimes and clusters them into three basic groups: those against the individual (email harassment, cyber stalking, dissemination of obscene material, hacking, indecent exposure, network trespassing, etc.), against organizations (hacking/tracking, possession and transmission of unauthorized information, cyber-terrorism, etc.), and against society at large (scandalizing the youth by indecent exposure, trafficking, pornography, etc.).

The IT Act 2000, for example, widely regulates the interception, monitoring, decryption and collection of information and data of digital communications in India. This IT Act 2000, especially its section 69, directs and empowers both central and state governments to issue directives for monitoring via computer and internet resources, and its succeeding collection, retention, and transmission of data. This act also ensures the civil and criminal liability in regard to hacking, electronic voyeurism, identity theft, redundant and unauthorized disclosure of obtained information, etc. Likewise, the amendment introduced to the IT Act in 2008 grants a mandatory data protection in the Indian law on individual rights. The Information Technology (Reasonable Security Practices and procedures and Sensitive personal information) Rules, 2011 further guarantees a reasonable security for sensitive personal information. The workplace surveillance still remains an unregulated area that has not been specifically addressed either by the Indian cyber laws or by labour laws. Labour laws widely focus on the safe working conditions assuring workers non-discriminatory wages in the organized sectors and look for fair and secured work environments.

Researchers observe that unlike countries like the United States, where privacy and individual rights are valued and legally guaranteed against its invasion of any kind, in India, the focus is given on employee surveillance to protect the company interest, not to the employees' interests or individual rights such as privacy (Fernando 2010). Having no proper and relevant legislation, the imposed technological monitoring exposes the individual worker to unprecedented and constant scrutiny, and there is nothing an employee can do as long as the absence of specific surveillance or privacy laws persists. Remarkably, the cyber laws to a minimum extent address the issue of data privacy and rights of both the employer and the employee, which we will explain in detail in the next chapter dealing with the nature and issues of privacy and the individual rights. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, nevertheless, provides detailed guidelines about the limit and extent of data collection, retention and transmission. It expresses also the necessity of the informed consent for the collection and disclosure of information. Likewise, even though there is no particular law governing the extent of allowed monitoring in the workplace, Indian Constitution provides and directs States to ensure and secure the just and humane work conditions. However, the problem continues as it does not provide the workers any remedy for unjust and inhumane work environments. Since these regulations and restrictions are not comprehensive enough and

particular to the practices of surveillance in the organizational workplace, the government should issue a legal framework specific to workplace surveillance.

In this regard, the Personal Data Protection Bill (PDPB) of 2019 concerns data protection and privacy across India. In 2017, the honorable Supreme Court held the privacy as a fundamental right, flowing from the right to life and personal liberty under Article 21 of the Constitution of India. The Court also observed that privacy of personal data is an essential aspect of this right to privacy. Imbibing the spirit of the Supreme Court, a Committee of Experts examined various issues related to data protection in India and introduced this Bill for personal data protection. This Bill was introduced in Parliament (Lok Sabha) by the Minister of Electronics and Information Technology on December 11, 2019, and seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. The Bill has been referred to a Joint Parliamentary Committee for detailed examination, and the report is expected by the Budget Session this year. The initial form of this *PDPB* could be found in the Privacy (Protection) Bill, 2013 proposed by the Centre for Internet and Society. Though this Bill of 2013 does not provide any definition on privacy, it focuses on the protection of sensitive personal data of persons. Personal data is perceived as data pertaining to characteristics, traits or attributes of identity, which can be used to identify an individual. Key areas of priorities in Indian PDPB 2019 is given in Exhibit 2.

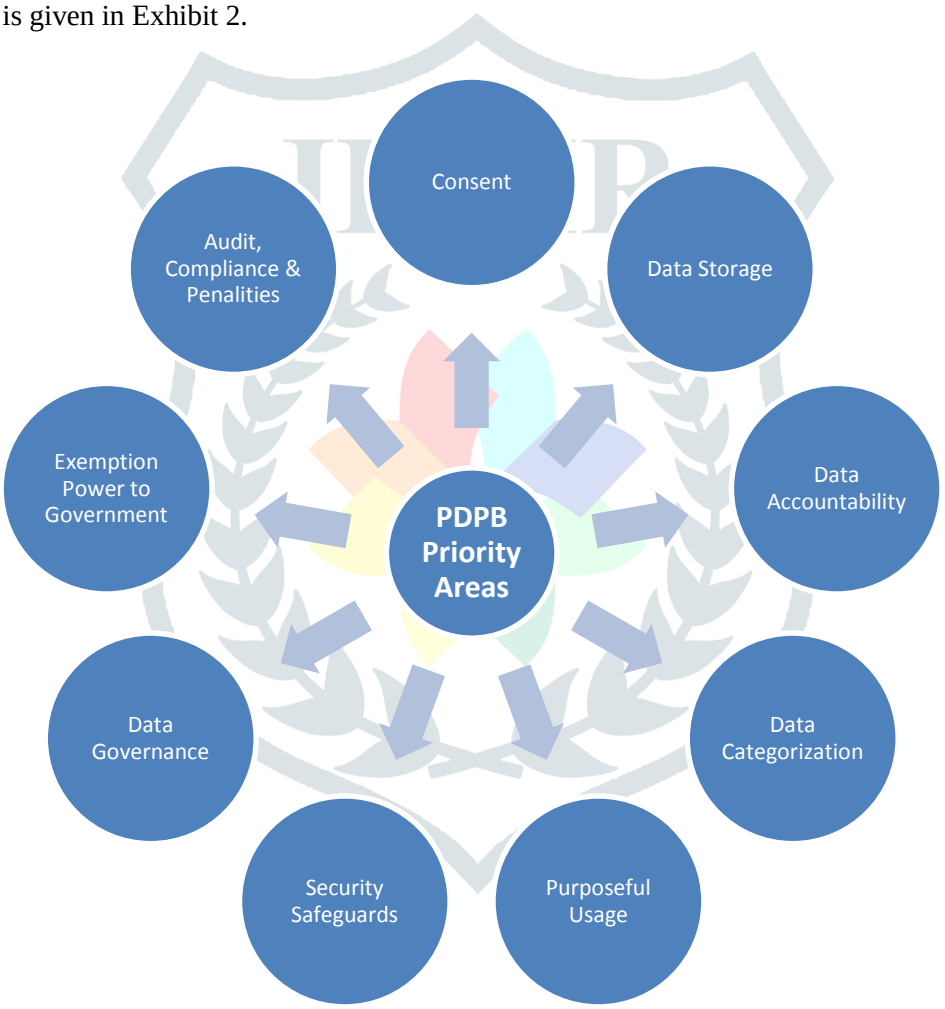

Exhibit 2 – Priority areas of PDPB

Data protection refers to policies and procedures seeking to minimize intrusion into the privacy of an individual (breach of privacy) caused by collection, processing and usage of their personal data. The PDPB, as it is given as the beginning of this Bill, aims "to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organizational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorized and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto." This PDPB governs the processing of personal data by government, companies

incorporated in India, and foreign companies dealing with personal data of Indian citizens. It recognizes the right to privacy as a fundamental right and the need to protect personal data as an essential facet of informational privacy.

The Bill establishes legal requirements for the collection and processing of personal data and limits the processing of sensitive personal data as well as the period of its retention. The sensitive personal data includes, as it is in PDPB Art. 3(36), personal data revealing or relating to password, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe. This broad definition of sensitive personal data that includes passwords and financial data is a landmark step taken in this Bill and thus marks its distinction from other international data protection laws. The PDPB ensures personal data to be processed only for specific, clear and lawful purpose, and must undertake certain transparency and accountability measures in processing data, such as implementing security safeguards (such as data encryption and preventing misuse of data) and instituting grievance redressal mechanisms to address complaints of individuals. In a situation like that of a workplace, employee surveillance and monitoring cause to trace more data of individual and that the present ubiquitous nature of global data transferring through computer mediated internet networking exposes individuals to more privacy risks. It challenges businesses which are collecting the data directly entered by users, or through actions without the knowledge of employees. For instance, via web surfing, e-banking or e-commerce the data can be correlated and by using more advanced analytic tools the data holder can generate economic value out of it.

The category of sensitive personal data includes, as it is in GDPR, the financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government. For instance, Article 4 guarantees a fair and reasonable processing of data, respecting the privacy of the data subject, or data principal. For data collection and processing, the Bill includes a purpose limitation (clear, specific and lawful - Article 5) and a collection limitation (limited and necessary – Article 6). In the same way, the data fiduciary is obliged to provide the data principal with adequate notice prior to the collection of personal data (Article 8). The entity or individual who decides the means and purposes of data processing is known as data fiduciary, while an individual whose personal data is being processed is a data principal under the Bill. It provides the data principal with certain rights with respect to their personal data including the quest of permission or seeking confirmation on whether their personal data has been processed, searching of correction, completion or erasure of data, allowing transfer of data to other fiduciaries, and restricting continuing disclosure of their personal data, once the processing of a particular data no longer necessary or if consent is withdrawn with valid reasons. The processing of data is always subject to certain purpose, collection and storage limitations. It guarantees that the personal data can be processed only for specific and lawful purposes undertaking the measures of transparency, accountability, and security safeguarding, along with further data protection impact assessment.

The Bill also requires that data processing be of a certain quality (complete, accurate, not misleading – Article 9), that data storage be limited (Article 10), and accountability on the part of those conducting this data processing (Article 11). The Bill guarantees that organizations designate a Data Protection Officer and conduct a third-party audit of the processing of personal data (Article 36). It assures that security safeguards will be implemented, including (where appropriate) de-identification and encryption, as well as safeguards to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data. The Bill would also require regulator notification of any data breach (Article 32 (1-7)). Article 3 (30) defines personal data breach as "any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal." Along with the wide definition of sensitive personal data, the Bill guarantees data localization (Article 40). Every data fiduciary is required to store a copy of personal data on a server or data centre located within the territory of India. This will restrict the global transfer of the data. Certain exemptions of these data processing restrictions are reported in the Bill, such as central government agencies can exempt this in matters of state security, public order, sovereignty and integrity of India. The definitive purposes of prevention, investigation or prosecution of any offence or as required by the State to provide benefits to the individual, legal proceedings, and responds to medical emergency, etc. mark further exemptions.

Familiarity (Common factors) with GDPR and Uniqueness of Indian PDPB

This PDPB 2019 considers the laissez-faire approach of the US legal framework, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and the EU's focus on individual privacy and data

protection (GDPR) and in view of all these adopts a comprehensive data protection law. Yet the Bill takes a specifically Indian approach by establishing, on the one hand, the role of the State to protect the common good, while on the other guaranteeing an enforceable framework for the individual right to privacy. The core concepts of the EU are GDPR, discussed above, is reflected in this proposed *Personal Data Protection Bill of 2019* (PDPB). For instance, as it is shown in Exhibit-3, the core principles of data protection in the GDPR are all a part of the proposed PDPB as well. The basic principles behind the processing of personal data both in GDPR and PDPB are fairness, lawfulness, transparency, consistent purpose, time limitation, accountability, integrity, confidentiality, accuracy, and data minimization. However, it has to be noted that though the PDPB does not refer to the term 'principles' in its description, it provides number of provisions imposing these requirements. Hence, there is a significant degree of exchange between these two legal frameworks.

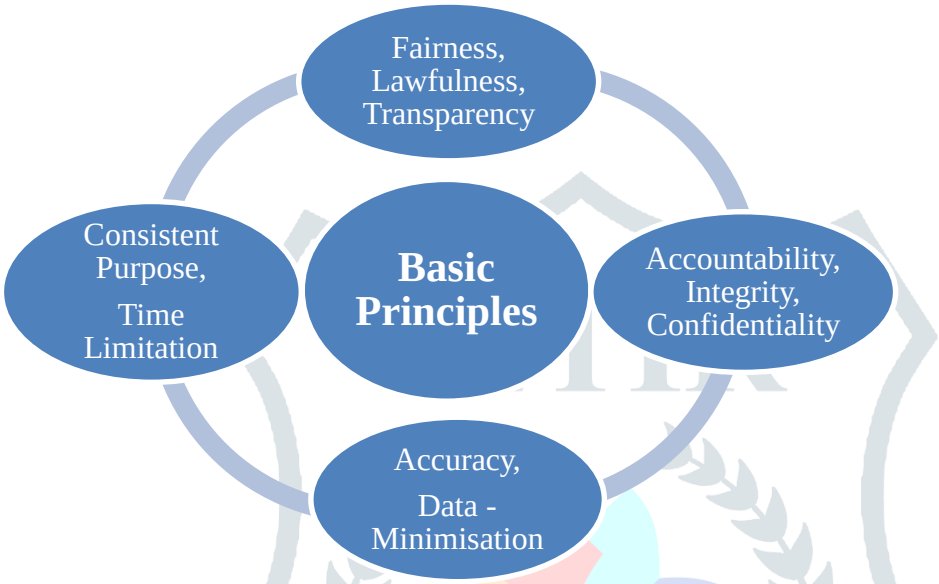

Exhibit – 3 Basic Principles of Both GDPR & PDPB

Along with all the fair procedures and purpose of data processing, the principles of integrity, transparency and accountability will strengthen the data controllers to provide detailed information about how data are processed what grounds are being used to justify it and what rights individuals have to access, delete and port data. In the same way, the principle of data minimization will hold on to the minimum necessary. Thus, both GDPR and PDPB policies ensure that they comply with these basic principles when deals with individual data. Within the sphere of lawfulness in data processing, the PDPB bestows towering emphasis on the role of consent, and is more strictly linked to transparency than that of GDPR, which emphasizes specific and meaningful control of the data. Similarly, one can compare the GDPR and PDPB in terms of the rights of data subjects, such as a right to correction, confirmation and access, a right to portability, and a right to be forgotten.

Within the category of personal data, the anonymous data is out of scope in GDPR. However, though anonymous data is generally out of scope in PDPB, it grants the government broad authority to compel the disclosure of information that does not constitute personal data. That shows its uniqueness as it allows central government to direct organizations to disclose anonymized personal data. The concept of personal data in GDPR takes into account the reasonable likelihood that an individual will be identifiable. At the same time, this flexibility does not appear in the PDPB, and hence, the definition and explanation of personal data under the PDPB is broader than the corresponding GDPR understanding. Though the notion of special categories of personal data in GDPR corresponds with the notion of sensitive personal data in PDPB, and one could find a significant overlap between these two frameworks, the understanding of this category of data is broader under the PDPB. For instance, the incorporation of financial data within the scope of sensitive data in PDPB and the provision of allowing government to define further types of data under this category make PDPB unique in this realm. Nevertheless, unlike the PDPB, the GDPR provides room for additional rules for processing criminal convictions and offenses data.

Along with the accuracy requirements, the storage limitation provision of PDPB is more specific than those of GDPR. For example, GDPR permits data controllers to retain the data, if necessary or not, in a form that no longer

identifies an individual, while PDPB requires deletion of data after the purpose completion and asks the fiduciaries or data controllers to conduct periodic reviews for personal data to be retained, in emergency, in its possession. That means, PDPB demands to take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed. Nonetheless, the PDPB does not have a provision analogous to the integrity and confidentiality principle governing GDPR. But the specific provisions governing information security in PDPB requires the same. In addition, for instance, performance of a contract is a legal basis for processing of personal data in GDPR. On the contrary, the PDPB does not provide for a basis for data processing that is necessary for the performance of a contract. Yet, the legal basis of consent seen in both GDPR and PDPB is defined less restrictively in both the frameworks and may permit processing that is necessary to enter into or perform contracts. There is also a strict development in PDPB that a clearer legal ground of personal data processing in relation to employment is guaranteed while this is left not very explicit in the GDPR.

For instance, the expedition of 'reasonable purposes' basis under the PDPB is similar to that of 'legitimate interests' basis under GDPR concerning a legal basis for processing of personal data. Yet, the basis of reasonable purposes in PDPB is strictly specified by more regulations, including for preventing or detecting unlawful activity, whistleblowing, mergers and acquisitions, network and information security, credit scoring, recovery of debt, the operation of search engines, or processing of publicly available personal data. Similarly, additional bases for health and safety and for employment purposes under the PDPB may have been justified under the GDPR's broader legitimate interests or public interests bases, which do not appear under these labels in PDPB. Likewise, the GDPR permits data processing under the legitimate interests, even without the consent of data subjects as these interests are not taken precedence over rights and interests of these data subjects. In this case, the legitimacy and proportionality of these interests are determined by the data controller. The PDPB, in this regard, permits the Data Protection Authority (DPA) to specify the reasonable purposes, rather than the data controller similar to legitimate interests, for data processing, and thus becomes more stringent than the GDPR.

The reasonable purposes in PDPB include certain specified activities, such as fraud prevention, information security, recovering debt and processing publicly available personal data (among others), and the DPA may enumerate others not provided in the bill. However, in employment context, organizations tend to rely on legitimate interests of GDPR for a wide range of activities that are not enumerated in the PDPB, like that of marketing and product development and improvement. In this manner, the processing of above mentioned sensitive data requires explicit consent. The standards for explicit consent to process sensitive data are closely aligned in both GDPR and PDPB. The GDPR may compromise with sensitive data only when it has to comply with obligations and exercising rights in the employment and social security context. However, according to PDPB, sensitive personal data may not be processed for the employment purposes legal basis and in the absence of this purpose, employers will likely rely more heavily on explicit consent for employee benefits programs. All these clauses show that the requirements for disclosing data or recipients under the PDPB may require more specific disclosures of data processors than is required under GDPR. The rights of access, the right to portability, the right of correction, and the right to be forgotten, are broadly similar and aligned in GDPR and in PDPB.

Finally, the record of processing requirements in PDPB appears to be more flexible than those under the GDPR and will likely apply to a small proportion of companies subject to the framework. Analyzing security and breach notification, it is clear that t here is little functional difference between these provisions both in GDPR and PDPB. For instance, GDPR guarantees that data controllers must notify individuals of a breach without undue delay only if it is likely to result in a "high risk" to individuals. Similar expression is found in PDPB that the data fiduciaries must notify the DPA of a breach "as soon as possible" if it is "likely to cause harm to any data principal." Being said that, it has to be specifically noted that the localization requirements represent a significant area of divergence between the PDPB and the GDPR. For example, localization is not required (unless international data transfer requirements are not met) under GDPR, while all the critical personal data or sensitive personal data must be processed in India, except under emergency circumstances or where the government has approved the transfer (taking into account India's security and strategic interests) under PDPB. That shows, only sensitive data is subject to data transfer restrictions under the PDPB. Hence, PDPB envisions transfer mechanisms similar to the safeguards given in GDPR. Yet, this would not remove the need to collect explicit consent for data transfer.

The most fundamental principle, within the legal framework of both GDPR and PDPB, governing data privacy and data protection in employment context is the authorized restriction for any organization to collect any data of an individual without his or her specific and unforced permission/agreement about the information being collected after being made aware of the purpose of its use and further possible processes, if any (Banaji 2018). That means, organizations need to have a clear *modus operandi* for explaining noticeably to employees what data is being collected, how it will be used, how long it will be held, what brings this particular data in the interest of employers, and why it is in the employees' interest, before asking for their consents. Once employee data is collected and stored, along with its legal possession, the organization is supposed to assume automatically the responsibility for protecting the data. This realm of high risk processing of data guarantees to gather little sensitive personal information as possible from employees. The highlights of these illustrations are expressed in a view that the individuals, or employees themselves in an employment context, are real owners of data concerning them, and not the organization or any corporate. Hence, researchers agree in asserting that "organizations must permit employees free access to it on-demand and with minimal hassle or red tape" (Banaji 2018). These legal matters of GDPR and PDPB restrict the collection, recording processing, and storing up of personal data of employees.

It is evidently experienced in India that most corporates here assume the legal right to monitor employees and collect data at the workplace. However, the parameters of GDPR and PDPB ensure that apart from general policy of permitting monitoring, every guidelines and procedures of this policy have to be explained in detail about how, where and why employees are monitored and how this gathered information will be used, stored, and transmitted, if situation demands. The principle of fair and reasonable processing determines the rightful and lawful processing of employee data in organizations. The notion of consent is identified as one of the primary grounds for employee data processing and hence this provides the data principal adequate control over the processing of his or her personal data. The agreement and assurance of treating sensitive personal data with extra care and protection mark employees' concern over the high risk possibility of their private information be made public. In the same way, amidst the ubiquitous surveillance and monitoring processes, the basic rights granted to employees to access, seek confirmation, rectify, and erase personal/private data promote transparency in the workplace. It has to be adequately realized that both GDPR and PDPB requires transnational or multinational corporations (MNC) to be cautious in data transmission across the local or national boundaries abiding all legal restrictions and security safeguards to prevent the free-flow of employee information and sensitive data.

Conclusion

This paper underlines a real threat called data protection that entire humanity encumbers to individually shoulder. Various programmes have been generated to help individuals clean up and cosmeticize their data personas. The Indian legal framework provided limited protection for employee data privacy and data protection. Most of the protection provided by the Information Technology Rules is related to individual's sensitive personal data. India's Personal Data Protection Bill 2019 (PDPB) as a long-awaited comprehensive Bill (to be passed as legislation) on the data protection (the 'right to privacy' in general terms) will make significant advances in data privacy for employees and thus for all people in India. The most progressive legislation on data privacy (of employees) available today is the European Union's General Data Protection Regulation 2018 (GDPR) that ensures data processing is done only with specific principles and processes of consent, legitimate purposes, necessity & proportionality, purpose limitation, accuracy and transparency, etc. In this context, a high-level comparison between the GDPR and PDPB is conducted to facilitate a comprehensive understanding about more restrained and controlled data processing that almost unthinkingly people authorize on the one hand and more demonstrative data protection to be actualized while being in an employment situation on the other hand.

The said PDPB Bill in India identifies the grounds for collecting, processing and storing personal data with a gamut of various reasonable and lawful purposes. It calls out a separate valid legal ground for organizations to process employee personal data in a restrictive way, which is necessary and indispensable with employment purposes. Legal and Justifiable provisions for implementing adequate security safeguards to manage the data processing are extended to all individuals, entities, and organizations including those which have been provided with exemptions under the Bill itself. Comparing the GDPR and PDPB, this paper analyzed several variables such as prohibition of processing personal data and restriction on its retention; grounds for data processing with or without consent and processing with reasonable purposes; right to access, correction, erasure, limited process, and to be forgotten; lawfulness, transparency

and prescribed prohibition on processing of sensitive or critical personal data, etc. All these areas are covered basing on the highly required and decidedly demanded initiatives towards implementing data privacy and data protection laws in India, especially within its employment context. These above mentioned stringent requirements of the Bill will make an impact on all the business processing in India without impeding the steady economic growth of India.

References

Banaji, Visty. (2018). "Employee Data Privacy is up to HR." *People Matters*. https://www.peoplematters.in/article/employee-relations/employees-data-protection-and-privacy-cant-be-ignored-17824 [accessed February 22, 2020].

Burri, Mira and Rahel Schär. (2016). "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy." *Journal of Information Policy* 6: 479-511.

European Parliament. (2018). "General Data Protection Regulation." *Official Journal of the European Union*. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [accessed February 22, 2020].

Fernando, A.C. (2010). *Business Ethics and Corporate Governance*. Delhi: Pearson.

Goddard, Michelle. (2017). "The EU General Data Protection (GDPR): European Regulation That Has a Global Impact." *International Journal of Market Research* 59 (6): 703-705.

Gürses, Seda and Jose M. del Alamo. (2016). "Privacy Engineering: Shaping an Emerging Field of Research and Practice." *IEEE Security & Privacy* 14 (2): 40-46.

Jindal, Rakhi, Gowree Gokhale and Vikram Shroff. (2012). "The Indian Legal Position on Employee Data Protection and Employee Privacy." *Employment & Industrial Relations Law*: 47-49.

John, Bernadette. (2018). "Are You Ready for General Data Protection Regulation?" *BMJ* 360:k941: 1-2.

Kak, Amba. (2018). "The Emergence of the Personal Data Protection Bill, 2018 - A Critique." *Economic & Political Weekly* 53 (38): 12-16.

Maheshwari, Vidhan. (2015). "Article 21 of the Constitution of India – The Expanding Horizons." http://www.legalserviceindia.com/articles/art222.htm [accessed February 16, 2020].

Nishith Desai Associates. (2018). "New Data Protection Law Proposed in India! Flavours of GDPR," July 30. http://www.nishithdesai.com/fileadmin/user_upload/pdfs/NDA_Summary.pdf [accessed January 16, 2020].

Ogriseg, Claudia. (2017). "GDPR and Personal Data Protection in the Employment Context." *Labour & Law Issues* 3 (2): 1-24.

Pati, Partha and Nishith Pandit. (2013). "Surveillance in India and Its Legalities." *Legally India*, June 2013, http://www.legallyindia.com/Blogs/surveillance-in-india-and-its-legalities [accessed January 20, 2020].

Singh, Vishalashi. (2017). "An Analysis of Personal Data Protection with Special Emphasis on Current Amendments and Privacy Bill." *International Journal of Law and Legal Jurisprudence Studies* 4 (1): 144-152.

Solove, Daniel J. and Danielle Keats Citron. (2018). "Risk and Anxiety: A Theory of Data-Breach Harms." *Texas Law Review* 96: 737-786.

The Centre for Internet & Society. (2013). "The Personal Data (Protection) Bill, 2013." https://cis-india.org/internet-governance/blog/the-personal-data-protection-bill-2013 [accessed February 16, 2020]

The Information Technology (Amendment) Act, 2008. *Ministry of Law and Justice, India*, 2009. http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf [accessed February 20, 2020].

The Information Technology Rules 2011. *Ministry Of Communications And Information Technology* http://deity.gov.in/sites/upload_files/dit/files/GSR3_10511(1).pdf [accessed February 20, 2020].

Xynou, Maria and Elonnai Hickok. (2015). "Security, Surveillance and Data Sharing Schemes and Bodies in India." 1-15. http://cis-india.org/internet-governance/blog/security-surveillance-and-data-sharing.pdf [accessed February 12, 2020].