VOLUME 18 ISSN 2456-9704

THE NEW BEHEMOTH DATA PROTECTION LAWS FOR THE 21st CENTURY: THE GENERAL DATA PROTECTION REGULATION

By V Adharsh
From Army Institute of Law

INTRODUCTION

"Facebook could tell that in Oklahoma the race between Republicans and Democrats is particularly close, identify the 32,417 voters who still haven't made up their minds, and determine what each candidate needs to say in order to tip the balance. How could Facebook obtain this priceless political data? We provide it for free. In the heyday of European imperialism, conquistadors and merchants bought entire islands and countries in exchange for coloured beads. In the twenty-first century our personal data is probably the most valuable resource most humans still have to offer, and we are giving it to the tech giants in exchange for email services and funny cat videos."

- **Yuval Noah Harari** (Israeli Historian)

In his book - *Homo Deus: A Brief History of Tomorrow*

The European Union has long been interested in the issue of the protection of personal data in the current world where every piece of information is digitized and is technologically driven. Initially the Data Protection Directive was issued by the European Union in 1995, regulating the processing of personal data within territory of the European Union.

Now, after duration of almost two decades, the European Union has enforced the behemoth **General Data Protection Directive (GDPR)**, superseding the Data Protection Directive since **25 May 2018**, taking data protection to whole new level and of importance. With a new legal framework requiring both organizational and technological changes along with accountability, the GDPR will necessitate an entire structural shake-up of organizations dealing with personal data of the citizens for its protection and prevention from its misuse.

The striking feature of the GDPR rests on the fact that it is applicable to **all** those organizations around the world, which deals with **collection and processing of data on residents domiciled with the EU, including expatriates and visitors along with the permanent residents.** Therefore, the compliance is on the basis of geographical location of the individuals whose personal data is collected by the organizations, and not by the registration domicile of the organization.

It has profound implications on as to how these organizations will comply with these rules in order to protect the personal data of anyone within the EU, and has the capacity to influence the data protection of even the non-EU residents as well owing to the fact that these organizations are likely to set up a uniform system for data protection for all individuals for ease of function. Hence the "General" may as well be called "Global" in GDPR as it imposes strict financial penalties with regards to non-compliance and therefore

mandates attention and function in accordance with the GDPR by all those organizations who conduct businesses across Europe, including both EU and the European Economic Area (EEA) along with United Kingdom post Brexit as they have assented to an equivalent Act namely Data Protection Act, 2018.

India, hence naturally, is also influenced by the GDPR with its organizations being required to be GDPR ready and compliant so as to avoid heavy financial penalties imposed in the GDPR.

DATA PROTECTION PRINCIPLES

There are six general privacy principles which form the basis of this legislation, whose bedrock lies in accountability, responsibility and compliance with these principles:

1. **Lawfulness, fairness and transparency** – Personal data is processed lawfully, fairly and in a transparent manner.
2. **Purpose limitation** – Personal data is obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing is allowed for archiving, scientific, statistical and historical research purposes.
3. **Data minimisation** – Personal data processed is adequate, relevant and limited to what is necessary.
4. **Accuracy** – Personal data is accurate and, where necessary, kept up to date.
5. **Storage limitation**– Personal data is not kept longer than is necessary (but data processed for archiving, scientific, statistical and historical research purposes can be kept longer subject to safeguards).
6. **Integrity and confidentiality** – Appropriate technical and organisational measures are put in place to guard against unauthorised or unlawful processing, loss, damage or destruction.[1]

REGULATORY IMPERATIVE OF THE GDPR

The GDPR is essentially a new regulation superseding the earlier 1995 EU Directive, on data protection for personal data across EU. It continues to follow the original Directive's foundational principles, while raising the level and complexity in some of the significant areas. The GDPR is important for two key reasons:

1. It is likely to apply to all organizations, even those not based in Europe, because it mandates certain protections and provisions for any organization that controls or processes personal data on EU residents where processing is related to offering goods or services ("irrespective of whether a payment of the data subject is required") or monitoring behaviour that takes places place within the EU (Article 3). Being located

[1]Efamro and ESOMAR, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR, Esomar Org (Jun. 7, 2020, 1:11 PM), https://www.esomar.org/uploads/public/government-affairs/position-papers/EFAMRO-ESOMAR_GDPR-Guidance-Note_Legal-Choice.pdf.

outside of the EU does not grant an exemption to a data controller.[2]

2. Cost of non-compliance with the regulation is significant, with financial penalty as high as that of **€20 million as fine or 4% of the total annual turnover of the preceding year, whichever is higher.**

WHAT IS PERSONAL DATA?

The scope of GDPR is "personal data". Personal data is defined in **Article 4** according to which it's as "any information relating to an identified or identifiable natural person ... who can be identified, directly or indirectly ... by reference to an identifier. "The identifiers which are listed in Article 4 include name, location data, identification number, and other identifying factors, such as mental, physical, and cultural among others.

But not all data which an organization possesses or collects falls under the scope of "personal data". For instance, previously collected data that have been fully anonymised and can't be re-identified to an individual is excluded from the ambit of GDPR requiring compliance, and hence can be used for data analytics, for example.

DRIVERS FOR INTRODUCING THE GDPR

The GDPR also acts as one of the essential elements of the **Digital Single Market priority** by the **European Commission**, aimed at bringing the 28 national markets to a **single market**, specially designed for the digital age. Two of the most significant ways in which the regulation makes a contribution towards it are:

1. It both harmonizes and modernizes the legal framework for protection of data across the EU. With a uniform single law across all the member States, organizations are relieved of the hassle of implementing different approaches per market.
2. Creation of a level playing field for organizations concerning data protection wherein principles regarding data protection apply irrespective of where the organization is based.

DATA CONTROLLERS AND DATA PROCESSORS

Article 4(7)[3] defines **data controllers** and **Article 4(8)**[4] defines **data processors.**

This distinction is important for compliance. Generally speaking, the GDPR treats the data controller as the principal party for responsibilities such as collecting consent, managing consent-revoking, enabling right to access, etc. A data subject who wishes to

[2]Osterman Research, GDPR Compliance and Its Impact on Security and Data Protection Programs,Osterman Research Inc. (Jun. 7, 2020, 1:15 PM), https://4b0e0ccff07a2960f53e-707fda739cd414d8753e03d02c531a72.ssl.cf5.rackcdn.com/wp-content/uploads/2017/02/GDPR-Compliance-and-Its-Impact-on-Security-and-Data-Protection-Programs-HPE.pdf?v=17.

[3]'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[4]'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

revoke consent for his or her personal data therefore will contact the data controller to initiate the request, even if such data lives on servers belonging to the data processor. The data controller, upon receiving this request, would then proceed to request the data processor remove the revoked data from their servers.[5]

REQUIREMENTS OF THE GDPR

Ability To Demonstrate Compliance

The task wherein the organizations need to have the ability to demonstrate compliance covers both organizational and technological measures. **Article 24**[6]and **Article 28**[7] set out the general obligations for data controller and data processor respectively. Measures which are implemented according to the GDPR may reduce the severity of the fine which is levied in the case of non-compliance to the rules of the GDPR.

Legal Basis for Processing

The right of processing personal data must be lawful i.e. they should lie under the six categories of lawfulness as mentioned in **Article 6**, the first of which states that the data subject has "given consent to the processing ... for one or more specific purposes."

Special Conditions When Processing Special Categories of Data

The GDPR has laid great emphasis on protection of special categories of data. **Article 9(1)**[8] provides the general prohibition whereas **9(2)**[9]list exceptions to these general prohibitions.

Records For Keeping Track of All Processing Activities

Under GDPR, **Article 30**[10] necessitates that controllers "shall maintain a record of processing activities under its responsibility". Processors are also directed to keep a record for all categories of processing activities under the requirements. Both the processors

[5]Data Controllers and Processors (Jun. 8, 2020, 11:20 AM), https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/.

[6]The controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

[7] Implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data Subject.

[8]Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

[9]Consent from the data subject, the protection of vital interests of the data subject, and where the data subject has made such information public, among others.

[10]Lists seven types of information to be maintained, including the purpose of the processing, a description of categories of data subjects and personal data, and who will see the personal data after processing, among others.

and controllers are obliged to maintain these records in both electronic and written form.

Increased Standard of Consent

The gaining of consent has achieved an elevated standard under the GDPR. According to **Article 4(1)** consent must be "by a statement or by a clear affirmative action." Hence there is prohibition on the usage of opt-out consent (assumed consent). There is also the provision whereby the data subject has been given the right to withdraw consent for the processing of their personal information.

Notification of Data Breaches Within 72 Hours

The GDPR requires two levels of actions in a scenario of data breach:

1. In cases of breach of data containing personal and sensitive information which risks the rights and freedoms of these individuals, the organization, once when it comes to its knowledge, has to report to the relevant supervisory authority of the breach within a window of 72 hours as mandated by **Article 33**. **Article 33(3)** also requires four specifications in the issuance of such a notification:

a. The nature of the personal data breach (including categories of data and approximate number of data subjects impacted)
b. The name and contact details of the firm's data protection officer
c. An analysis of the likely consequences of the breach
d. Measures taken or proposed to be taken to mitigate negative effects.

2. To notify individually, all those data subjects whose rights and freedoms are under a risk due to the data breach and must entail detail and specifications similar to that of to the supervisory authority.[11]

Appointment of Data Protection Officer (DPO)

When the processing of personal sensitive data is carried out in a regular and systematic way, the organizations are required to appoint a Data Protection Officer.

The Data Protection Officer has certain requirements:

1. Should have expert knowledge of data protection law and practices.[12]
2. Must have certain freedoms as specified in **Article 38**.
3. Has a list of certain prescribed tasks to execute as provided in **Article 39**.[13]

Right To Data Portability

The data subject possess the right to data portability by which they have the power to request their personal data which has been supplied to a controller in "a structured, commonly used and machine-readable

[11] Article 6.
[12] Article 37(5).
[13] These tasks include informing and advising data controllers, processors, and employees of their obligations under the GDPR, monitoring internal compliance, and cooperating with the supervisory authority, among others.

format" so as to give it to another data controller.

Data Protection by Design and Default

As per **Article 25**, data controllers are necessitated to design the GDPR's protection principles within the very structure of their technical systems and organisational processes.

For the following purpose, an integrated and thoughtful assessment of four specific factors is required-

1. The state of the art (technological advances)
2. The cost of implementation and the nature, scope, context
3. Purposes of processing
4. The risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing

The conceptual understanding of the rights of data subjects as per the GDPR is required and has to be imbibed practically to the technical capabilities and organizational processes.

Further, the organizations will have to select only those IT vendors and cloud services providers who can, by demonstration, prove that the GDPR requirements are built-in by design and default into their solutions so that they are in compliance with the regulation.

OTHER REQUIREMENTS

Right of Access by the Data Subject

The right to ask the data controller by the data subject regarding whether his/her personal information is being processed, and if it's the case, then can request access to both of the personal data as well as that of information on processing, data transfers, recipients and the subsequent rights.[14]

Right to Rectification

If inaccurate personal data of the data subject is held by the data controller, then the data subject has the right to get his personal data updated by supplying the right information, which the controller is required to do without any "undue delay".[15]

Right to Erasure (Right to be Forgotten)

The data subject has the right to request the erasure of his/her personal data by the data controller[16], subject to certain conditions.[17] On the other hand, the data controllers have the power to decline an erasure request, provided it fall within one of the many exception provided under Article 17(3).[18] Hence, nevertheless, it is implied that that the organizations should have the organisational and technological ability to erase all affected data promptly.

[14]Article 15.
[15] Article 16.
[16] Article 17.

[17] Conditions include the withdrawal of consent, previous unlawful processing, and other legal compliance erasure mandates.
[18] Include compliance with a legal obligation, public interest for public health, and legal claims.

Right to Restriction of Processing

Similar to the right to erasure, the data subject, subject to certain conditions[19], has the right to exclude his/her data from future processing activities which can be either temporary or permanent.[20]

Notification Obligation of Controllers

The GDPR requires the data controller to notify each of the recipients whose personal data has been recently impacted by the exercise of any of the data subject's rights in relation to restriction, erasure or rectification. Also the data controller is required to supply details on recipients when requested by the data subject.[21]

Right to Object

The right to object to the processing of personal data is given to the data subject, at any time, where the legal basis is "the performance of a task carried out in the public interest," "the exercise of official authority vested in the controller," or for the purposes of the "legitimate interests" of the controller or a third party.[22]Objection can also be made in cases where the data is processed for the purpose of direct market activities.[23]

Automated individual decision-making, including profiling

Objection can be made by the data subjects towards automated processing and profiling relating to their personal data and at the minimum, have the right to "obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision." The basic aim of the right is to prevent data controllers making significant decisions relating to legal and like matters regarding a data subject on an purely automated basis.[24]

Processor Requirements

If another organization is engaged by the data controller for the purpose of data processing, the processor must have taken required technical and organizational measures, making it in compliance with the regulation and must also help the data controller in responding to the various requests filed in relation to the rights of the data subjects.[25]

Records of Processing Activities

Records of the processing activities done by the data controller must be kept, for which they are responsible, with a list of specific information to be maintained corresponding to each of the record.[26]

Security of Processing

Implementation of organizational and technological measures is to be taken up by

[19] Conditions include contested data accuracy, unlawful processing, and the desire of the data subject to be excluded from processing activities.
[20] Article 18.
[21] Article 19.
[22] Article 6(e) and 6(f)
[23] Article 21.
[24] Article 22.
[25] Article 28.
[26] Article 30.

the data controller to ensure the presence of an optimum level of security for the processing of data, such as encryption, pseudonymization, regular testing of organizational and technological measures etc.[27]

Transfers of Personal Data to Third Countries or International Organizations (Articles 44-50)

The EU-US Privacy Shield Framework was brought in around mid-2016, as the GDPR outlines certain special requirements for the above mentioned cases. The goal of this framework though, is to allow US companies, while maintaining the protections provided under the GDPR, to transfer data on EU residents.

CONSPECTUS

There are three primary implications arising out of the GDPR that is to be considered by decision makers:

1. **Re-examination your data strategy**

- Every affected organization needs to immediately undertake a significant re-examination of its organizational data strategy related to personal and sensitive personal data. Specific requirements in the GDPR need to be planned for, and organizational and technological approaches implemented to resolve problems, strengthen policy and protections, and mitigate against the worst outcomes.

2. **Non-EU Firms to play rapid catch-up**

- The new, level playing field introduced by the GDPR applies to all firms everywhere if they control or process personal data on EU residents. Organizations previously subjected to the data protection directive have had a 20-year head start to develop the appropriate organizational and technological approaches to operating successfully in Europe.

3. **Organizational and Technological responses**

- By all means, every organization should embrace the best technology on offer, but this has to be done as one coordinated element of a wider organizational response. Achieving GDPR compliance is not something the IT department can do alone. Compliance will require a set of coordinated and appropriate responses from the organization as a whole, with strategy, policy, training, and governance processes needed based on expertise from various groups, including Executive Management, Legal, Human Resources, Training, and the IT Department.

GDPR AND INDIA

Economic Survey reveals a top down structure of economy with 66.1% contribution of services sector to GDP. Out of this, information technology – business process management (IT-BPM) sector "is expected to touch an estimated share of 9.5% of GDP and more than 45 per cent in total services exports in 2015-2016 as per NASSCOM."[28] Revenue contribution of Exports in IT-BPM is expected to touch 108 billion US dollars with a comparatively less domestic contribution of 22 billion dollar.[29]"Major markets for IT software and

[27] Article 32.

[28] Pg.168, Economic Survey 2015-2016.

[29] Pg.167, Economic Survey 2015-2016.

services exports are the U.S. and the U.K. and Europe, accounting for about 90 per cent of total IT/ITES exports".[30] According to NASSCOM estimates for 2014, UK and Continental Europe respectively accounted for 17.4% and 11.6% of India's IT/ITES services export.[31]

Therefore, one can clearly see nature of criticality regarding the IT-BPM sector in India and the country must take all measures to protect and promote it. For this, India must be prepared for the global changes taking place regarding regulatory changes like that of the GDPR.

The Indian laws which are in place governing the online data protection are:

- **Information Technology Act, 2000 (IT Act)**
- **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**

THE PERSONAL DATA PROTECTION BILL - 2019

Over the past few years, India's data privacy issues have become increasingly prominent. With the rampant growth in the usage, transmission and collection of personal data in the international sphere, the current applicable legislations in the country don't provide the necessary depth and intricacy required for protection of data in today's world. The introduction of GDPR also acted as a wake-up call to bring in a new legislation which corresponds to the present times.

The origin of the Personal Data Protection Bill lies in the landmark judgment of ***Puttaswamy v Union of India***.[32] The judgment was issued on August 24, 2017. In the ruling, the Supreme Court of India declared that the right to privacy is a fundamental right of the Indian Constitution. On September 26, 2018, the Supreme Court asked the government to formulate strong data protection rules.

Around the same time that the Supreme Court reviewed the evidence in *Puttaswamy v. Union of India*, the Indian government established a data protection expert committee to review issues related to data privacy chaired by a retired Supreme Court judge B.N. Srikrishna. The committee submitted a report and a draft bill a year later. The current bill in Parliament is a modified version of the draft bill.[33]

The Minister of Electronics and Information Technology, Ravi Shankar Prasad, introduced the Personal Data Protection Bill, 2019 in Lok Sabha on December 11, 2019. The bill aims to protect personal privacy data related to individuals, and establishes the Data Protection Authority of India for the above purposes and matters related to personal data. The bill proposes to replace the Information Technology Act of 2000 (Section 43-A) and delete provisions related to compensation payable by companies for failing to protect personal data. In particular, the PDPB stipulates the methods of

[30]Indian Services Sector: Poised for global ascendancy, KPMG-CII, Source 3, 4, 5 NASSCOM Strategic Review 2015, NASSCOM, Pg. 13, April 2016.

[31]CRISIL Opinion, Why India will gain as economic recovery in US and EU gains momentum, July 2014, CRISIL Research.

[32] Writ Petition (CIVIL) NO 494 OF 2012.

[33] What Is in India's Sweeping Personal Data Protection Bill? (Jun. 10, 2020, 12:31 PM), https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985.

collecting, processing, using, disclosing, storing and transferring personal data.

The PDPB recommends the protection of "personal data" related to the identity, characteristics, "sensitive personal data" of natural persons, such as financial data, health data, official identifiers, sex life, sexual orientation, biometric data, genetic data, transgender people Identity, bisexual identity, caste or tribe, religion or political beliefs.

Applicability

The PDPB recommends that it be applied to the processing of personal data collected, disclosed, shared or otherwise processed in India;

- By the government, any Indian company, any Indian citizen or any individual or group incorporated in India, and
- Foreign companies processing Indian personal data.

In addition to anonymous data or other non-personal data, PDPB is not applicable for the processing of anonymous data, so that the central government can better determine the service delivery goals or formulate evidence-based policies.

Obligations of Data Fiduciary

The processing of personal data will be subject to certain purposes, collection and storage restrictions, such as:

- For clear and legal purposes.
- Collection of personal data should be limited to the data required for processing purposes.
- Individuals/data subjects need to be notified to collect or process personal data.
- Only retain personal data for processing purposes and delete it at the end of processing.
- At the beginning of data processing, consent must be obtained from the data subject.
- The data trustee must verify the age and obtain parental consent when processing sensitive personal data of children.

In addition, the data trustee must take certain transparency and accountability measures, such as: (i) formulating a privacy policy, (ii) taking the necessary steps to maintain transparency in processing personal data, (iii) implementing security safeguards (such as data encryption and prevention Abuse), (iv) notify the Authority of any personal data violations by notification, (v) review its policies and policy implementation annually, (vi) conduct data impact assessment of personal data when important data trustees are involved in the processing of new technologies or sensitive data, (vii) The important data trustee should appoint a data protection officer to advise and monitor the data trustee's activities, and (vii) establish a complaint redress mechanism to resolve individual complaints.

Processing Personal Data Without Consent

The bill recommends that the trustee can process the data only if the individual agrees. In some exceptional cases, personal data can be processed without consent, for example: (i) if the state requires the benefit of an individual, (ii) legal procedures, (iii) respond to medical emergencies, (iv) employment

related, (v) Necessary to prevent fraud, mergers and acquisitions, debt recovery and other reasonable purposes

Rights of Individuals/Data Subjects

The bill provides certain rights for individuals (or data subjects), including: (i) Obtain confirmation from the trustee about whether his personal data has been processed, (ii) Seeking corrections, incomplete or updated personal data, (iii) Data portability- in some cases, personal data Reference to any other trustee's data, (iv) The right to be forgotten: if consent is no longer needed or withdrawn, restrict it from continuing to disclose its personal data by the trustee.

Data Protection Authority

The Bill proposes that the Data Protection Authority of India should take measures to protect personal interests, prevent misuse of personal data, and ensure compliance with the Act and raise awareness of data protection. The order of the Authority can be appealed to the Court of Appeal. Appeals for court orders can be filed with the Supreme Court.

Restrictions on the Transfer of Data Outside of India

If the individual expressly agrees and is bound by certain other conditions, sensitive personal data may be transferred outside of India for processing. However, such sensitive personal data should continue to be stored in India. Certain personal data notified by the government as critical personal data can only be processed in India.

Exemptions

If necessary, the central government has the right to exempt any government agency from applying the law:

- for India's sovereignty and integrity, national security and friendly relations with foreign countries,
- Prevent incitement to commit any identifiable crime related to the above matters.

For some other purposes, such as (i) preventing, investigating or prosecution of any crime, or (ii) personal, family, or (iii) journalistic purposes, (iv) for research archiving or statistical purposes, processing personal data is also not restricted by the provisions of this Act.

Risk of non-compliance with PDPB

Penalties and compensation are divided into two levels:

- If the data trustee fails to fulfil its data protection obligations, it may be subject to a fine of Rs 5 crores or 2% of the total global turnover of the previous fiscal year, whichever is higher.
- Anyone who processes data in violation of the PDPB regulations may be subject to a fine of Rs 150 crores or 4% of the data trustee's annual turnover, whichever is higher.

Re-identification and processing of de-identified personal data without consent may be punishable by imprisonment of up to three years, or a fine or both.

Pursuant to the PDPB being enacted into an Act, organizations handling personal data should follow several compliances to ensure the protection of personal privacy related to personal data. Processing personal data will require personal consent. Depending on the type of personal data processed, the organization will have to review and update data protection policies and codes to ensure that these policies are consistent with the revised principles, such as updating its internal violation notification procedures and implementing appropriate technical and organizational measures to prevent data misuse. An important data custodian is to appoint a data protection officer, and establishes a complaint handling mechanism to resolve individual complaints.[34]

As of now, the Bill is being analyzed by a Joint Parliamentary Committee (JPC) in consultation with various groups.[35]

CONCLUSION

"The companies that do the best job on managing a user's privacy will be the companies that ultimately are the most successful."

– **Fred Wilson** (American Venture Capitalist)

It is evident that for the provisions of data protection, the GDPR sets a really high benchmark as compared to the Indian laws. With the penalty for non-compliance involving very high fines, it's of paramount importance that the Indian organizations become GDPR compliant, or else the country will fail to qualify as a data secure destination, prompting diversion of business opportunities to other safer locations. Following on the footsteps of the GDPR and the pressing void in data regulations for the present times, the country hopes to change its domestic regulations too, with the Personal Data Protection Bill, which would require the Indian organizations to maintain the highest standards of data and privacy protection.

India's IT outsourcing industry, worth about $146 Billion, is one of the biggest factors cementing the country's reputation as a technological hub. Indian organizations, from BPOs, KPOs and ITOs are undertaking key operational tasks of both MNCs and smaller enterprises managing in-house processes at a fraction of the cost of establishment, underlying the importance of GDPR compliance for sustainability and future growth.

Given how well-integrated they are with the global business landscape, Indian IT companies that align themselves with the changing dynamics of personal data management through cutting-edge data analytics, can ensure that they are in a stronger strategic position to drive continued

[34] Key Features Of The Personal Data Protection Bill, 2019 (Jun. 9, 2020, 12:31 PM), https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019.

[35] Personal Data Protection Bill: More drama ahead? (Jun. 10, 2020, 12:35 PM), https://www.businesstoday.in/current/economy-politics/personal-data-protection-bill-expect-more-tweaks-post-parliament-panel-consultations/story/392160.html.

growth – for themselves, and for the larger IT services ecosystem in India.[36]

*****

[36] The Impact of GDPR on Indian Data and IT Sector (Jun. 11, 2020, 12:31 PM), https://inc42.com/buzz/the-impact-of-gdpr-on-data-and-it-sector/.