# Regulatory Frameworks on Personal Data Protection: Insights from Different Jurisdictions

## Introduction

As countries increasingly realise the value of data for their economy and recognise the importance of protecting it, they are beginning to develop their regulatory frameworks on privacy, data protection, and related issues. More often than not, such frameworks have unique features informed by respective country's vision of digitalisation and use of digital services for its economy. India is no exception. While India's Personal Data Protection Bill 2019 (PDPB), borrows from the European Union's (EU) General Data Protection Regulation (GDPR), it also has certain unique features. It is, therefore, pertinent to compare and contrast some key features of different privacy and data protection legislations, including PDPB and GDPR, to better understand intent and objectives of different countries. Such comparison becomes even more pertinent as data governance cannot be a solely territorial concept and seamless data flow across jurisdictions is critical to leverage its value and essential for realisation of the vision of digital economy and growing tech industry in many countries.

**Comparison Matrix**

The matrix below compares certain key features of - a) the GDPR framework which is considered one of the most comprehensive data protection framework in the world; b) Asia Pacific Economic Cooperation (APEC) Privacy Framework, which aims to enhance cross border data flows amongst members of APEC, without compromising on standards of privacy and data protection; c) China, which is one of the biggest data regimes focusing on state control over data flows, with its recent adoption of the Cyber Security Law; d) Japan's Act of Protection of Personal Information (APPI), which is now considered to be amended to align with GDPR; e) California Consumer Protection Act 2020, through which California became the first US state to have a specific data protection law and is being called GDPR 'lite'; and f) India's PDPB 2019, which is now under the consideration of Joint Parliamentary Select Committee.

| **Country** | **General Data Protection Regulation- EU 2018** | **APEC Privacy Framework 2015** | **Chinese Cyber Security Law 2017** | **Japan's Act of Protection of Personal Information 2017** | **California's Consumer Privacy Act 2018** | **India's Personal Data Protection Bill 2019** |
|---|---|---|---|---|---|---|
| **Definition of personal data and the segregation between categories of data** | Personal data means any information relating to an identified or identifiable natural person ('data subject'); and means any information that can directly or indirectly identify a person. **Sensitive** | Personal information is information that can be used to identify an individual. It also includes inferences drawn from such information. **There is no differentiation** | Personal data refers to various information which is recorded in electronic or other forms which can be used to identify a person. The law does not itself prescribe any definition of the | Personal information includes any information that makes a person identifiable. **Sensitive personal data is defined as data which needs to be handled carefully so as to** | Personal data is referred as personal information which can identify a person, and includes inferences drawn from such information. **No separate category for sensitive personal data**. | Personal data is defined as data through which a person can be identified, both online and offline, directly and indirectly, and include inferences drawn for profiling. **Sensitive** |

| Country | General Data Protection Regulation- EU 2018 | APEC Privacy Framework 2015 | Chinese Cyber Security Law 2017 | Japan's Act of Protection of Personal Information 2017 | California's Consumer Privacy Act 2018 | India's Personal Data Protection Bill 2019 |
|---|---|---|---|---|---|---|
| | **data does not include financial data and passwords.** | **between personal and sensitive personal data.** | sensitive personal data although standards provides for it as **data which if divulged can lead to person, property, psychological harm or discrimination. It includes information related to bank accounts.** | **not cause discrimination and prejudice and does not include financial data and passwords.** | | **data includes financial data, but does not include passwords.** Government is authorised to notify categories of personal data as sensitive personal data having regard to risk of significant harm on processing and expectation of confidentiality with such data. |
| **Processing of Data** | Processing of data must be done in lawful, fair and transparent manner, only for an explicit and **legitimate purpose and no further processing** | The processing of the data should be lawful and fair. **The data should only be used for the purposes of collection as informed to the** | Processing of data should be lawful, justifiable and necessary. It further explains the **meaning of lawful, i.e. to not deceive, force or inveigle** | There is no specific provision for transparency and requirements of fairness and reasonableness, although **data subject must be** | Businesses have the responsibility to **inform the consumer about the purpose of collecting and the information should be used for** | Data has to be processed in a fair and reasonable manner for the purpose for which it was consented **which includes an incidental** |

| Country | General Data Protection Regulation- EU 2018 | APEC Privacy Framework 2015 | Chinese Cyber Security Law 2017 | Japan's Act of Protection of Personal Information 2017 | California's Consumer Privacy Act 2018 | India's Personal Data Protection Bill 2019 |
|---|---|---|---|---|---|---|
| | **which is incompatible with that purpose.** | **user while collection and other compatible purposes. The framework gives examples of such compatible purposes** | **the data subject. It also provides for 'clear purpose principle' for processing of data**. | **informed about the utilization of their data.** | **that purpose only**. It is the responsibility on business to provide an opt-out option if the consumers do not wish to share the information. | **purpose or the purpose which is connected to the initial purpose.** |
| **Exemptions from data protection** | Exemption for defence, national security, for conviction of offences and general public interest. **Such use includes the condition of necessary and proportionate to the purpose for which the data is used.** | Exemptions are provided for in the case of security, sovereignty, safety and public policy, **although it provides for conditions of limited and proportionate use and authorised by the law and should be made known to the public.** | Exemptions are public interest, law enforcement purpose, national security, voluntary publication of information by individual. The law also gives power to the government to demand data from network operators in the case of emergency. **No legal test for proportionality.** | Exemptions are uses required by law, preventing bodily harm, to improve public health. **No principle of proportionality**. | Exemption relates to compliance of the business with laws, judicial proceedings, criminal proceedings and cooperating with public authorities for the matter of enforcement of the law. **No particular legal text specified.** | Government may for national security or public interest considerations exempt its agencies from any provision with respect to data protection. Exemptions also exist for processing of personal data for legal or judicial purposes. **No** |

| Country | General Data Protection Regulation- EU 2018 | APEC Privacy Framework 2015 | Chinese Cyber Security Law 2017 | Japan's Act of Protection of Personal Information 2017 | California's Consumer Privacy Act 2018 | India's Personal Data Protection Bill 2019 |
|---|---|---|---|---|---|---|
| | | | | | | **condition of legality, necessity and proportionality for applying exemptions.** |
| **Non- Personal Data and Voluntary Verification by Social Media Intermediaries** | GDPR specifically focuses on personal data protection and **does not provide for usage of non-personal data/ information** and **does not provide for voluntary verification provisions** for social media intermediaries | With the aim of promoting information flows **only focuses on the uses of personal information**. There is **no requirement of voluntary verification** by social media intermediaries | Provides for cyber security and privacy provision with respect to **personal information and does not include non-personal data. It does not include the provision for voluntary verification** | It **only focuses on personal data, usage of non-personal data is not included** within the law. There is **no requirement for voluntary verification** by social media intermediaries. | **Only covers personal data of consumers** there are no provisions regarding the non-personal data. There is **no requirement of voluntary verification** by social media intermediaries. | The law **provides for transfer of non –personal data to the government in certain cases** and requires social media intermediaries to **give provisions for voluntary verification of users.** |
| **Data localisation and data flows** | Allows for data flows, and allows for data storage in **GDPR compliant locations.** | Promotes cross border data flows with companies and countries which are **compliant with** | Requirement of data localisation and cross border **data flow is only permitted after** | **Data transfer is allowed after the consent of data subject**. Although such consent is not | **Transfers are not restricted**, although transfers to service provider, requires compliance with | **Data localisation not applicable except in cases of sensitive personal data and** |

| Country | General Data Protection Regulation- EU 2018 | APEC Privacy Framework 2015 | Chinese Cyber Security Law 2017 | Japan's Act of Protection of Personal Information 2017 | California's Consumer Privacy Act 2018 | India's Personal Data Protection Bill 2019 |
|---|---|---|---|---|---|---|
| | | **APEC privacy framework.** | **consent and establishment of appropriate business needs.** | required if the other **country is considered data protection compliant**. Example- EU | data protection provisions within the legislation. | **critical personal data**, which can be transferred outside after approval from the data protection agency or the government, as the case may be. |
| **Consent Mechanisms** | Consent should be informed, free, capable of being withdrawn and demonstrable**.** | Where appropriate, individuals should be provided **with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.** | Provides for consent requirements for lawful processing. **Although does not mention specific modes or mechanism** for obtaining consent. | For the purpose of processing the data, consent is required. **Although there is no prescribed mechanism for obtaining consent** | Consumers need to be informed about the purpose of collection of data and they should **provide consumers with an opt-out option if they font wish to share data.** | Provides for clear, specific, informed consent capable of being withdrawn. It provides for the **mechanism of consent managers** through whom consent can be provided and withdrawn. |

| Country | General Data Protection Regulation- EU 2018 | APEC Privacy Framework 2015 | Chinese Cyber Security Law 2017 | Japan's Act of Protection of Personal Information 2017 | California's Consumer Privacy Act 2018 | India's Personal Data Protection Bill 2019 |
|---|---|---|---|---|---|---|
| **Rights of data subjects/ principals** | Right to be forgotten, right to restrict processing, right of data portability (by automated means), **right not be subject to automated processing** | Right to access and correction, right to be informed about the data transfers | Right to access data, right to rectification of errors, right to deletion /forgotten, right to object processing, right to restrict processing, right to portability is specified cases, right to withdraw consent, **right to object marketing, right to complain to authority** | Right to access, **correction, data portability**, rectification of errors, right to object processing, **right to restrict processing**, right to withdraw consent, right to object marketing, right to complain | Right to view and access data, right to erasure, right to opt-out from sharing of data, right to stop companies from selling data, limited recognition of right to portability | Right to confirmation and access, correction and erasure, data portability and forgotten. The data principal needs to make a request in writing to exercise the rights, and the data fiduciary may charge a fee to comply with certain requests. |
| **Authority for Implementation** | Specifically provides for setting up of **independent authority by member states for the implementation of the GDPR**. It specifically provides that **such authority** | Framework gives member states to autonomy to formulate authority for **enforcement through central authorities, multi-agency enforcement bodies, a network** | **The law does not provide for any specific authority** or regulator rather the powers are distributed amongst various government departments. | **Independent Personal Information Committee (PPC**) is being set up for the implementation of the act, which also provides for collaboration with other sector specific | **There is no independent authority** for enforcement and implementation of the act. | The law provides for setting up **of Data Protection Authority (DPA) without any independent members, to be nominated by selection committee** |

| Country | General Data Protection Regulation- EU 2018 | APEC Privacy Framework 2015 | Chinese Cyber Security Law 2017 | Japan's Act of Protection of Personal Information 2017 | California's Consumer Privacy Act 2018 | India's Personal Data Protection Bill 2019 |
|---|---|---|---|---|---|---|
| | **must not be influenced by external factors and would have complete financial and administrative autonomy in exercising its functions.** | **of designated industry bodies, or a combination of the above, as Member Economies deem appropriate**. | | ministries. | | **comprising government representatives**. |
| **Penalties** | **Provides for administrative fines and penalties based on the level of damage suffered by the data subject.** Although such fines differs on the basis of specific infringements, with highest fines for infringement related to processing, consent and rights of data subjects and | Encourages member states to adopt an appropriate framework to deal with threats and breaches. It provides for member stated to come up with remedies which are commensurate to the degree harm due to the violation. | Provides for penalties in case of infringement and specifically also provides for a person responsible along with revocation of business licence. **Provides for criminal sanctions in cases where network managers refuse to make rectifications after** | Both imprisonment and fine. **Highest penalty which includes both fines imprisonment in the cases of uses of personal database for unlawful gains.** | **There is a right for private action, provides for penalties**. The fines are decided according to the damages suffered | Penalty and criminal sanctions up to three years in certain cases. **Criminal penalties are provided in the cases where the personal data is re- identified without consent of data fiduciary**. Penalties are imposed only if the adjudicating officer |

| Country | General Data Protection Regulation- EU 2018 | APEC Privacy Framework 2015 | Chinese Cyber Security Law 2017 | Japan's Act of Protection of Personal Information 2017 | California's Consumer Privacy Act 2018 | India's Personal Data Protection Bill 2019 |
|---|---|---|---|---|---|---|
| | overhaul of data protection's authority. It emphasise that such penalties or fines imposed must be effective, proportionate and dissuasive. | | **being notified for three years**. | | | considers there is infringement or harm caused as provided under the act and based on the degree of the arm caused. |
| **Grievance Redress** | GDPR gives right to data subject to lodge complaint both to the supervisory authority and **gives right to claim appropriate judicial remedy in case their rights are violated under the regulation** | Encourages member states to come-up with their own frameworks which maybe include **right of individuals to pursue legal actions or industry self- regulation.** | Provides **for the right to make a complaint to authorities which include Cyberspace Administration of China (CAC), telecom authority and the public security authorities and other concerned authorities**. Although it does not | Provides for right to lodge complaint for **data breaches to Personal Information Protection Committee**. There is no right for lodging complaint to the court. | **Consumers have the right to initiative a civil action in the courts** pursuant to their rights being violated in case of data breach. | Provides for the right to data principal to **lodge a complaint for breach of rights and non-compliance by data fiduciaries to the Data Protection Authority (DPA). It does not provide for the right to data principal to lodge** |

| Country | General Data Protection Regulation- EU 2018 | APEC Privacy Framework 2015 | Chinese Cyber Security Law 2017 | Japan's Act of Protection of Personal Information 2017 | California's Consumer Privacy Act 2018 | India's Personal Data Protection Bill 2019 |
|---|---|---|---|---|---|---|
| | | | provide for lodge the complaint to the court itself. | | | **the complaint directly to the court.** |
| **Obligations of Data Fiduciaries/ Controllers** | **Data controllers are to report the data breaches to the data subjects in the cases where there is high risk of breach** of rights of data subjects. If the data controller fails to do so the supervisory authority must inform the data subject of the same. | Gives flexibility to member states to adopt mechanism which ensured accountability of controllers to maintain appropriate security for breaches and provide necessary remedies to the individuals | **It obligates the network operators to report the data breaches to the data subject in a clear language** indicating the nature of the breach and also suggestion to mitigate the breach and also to the concerned authority. | **The law states that it is preferable for handling operator to inform the data subject** of the breach, so that they can take appropriate mitigating measures. | **There is no provision of reporting breaches**, but the consumers have right to access information related to any data transfers and give business notice of 30 days if there is any breach. | The obligation of the **data fiduciary to report the data breach to the data principal rests on the discretion of the Data Protection Authority (DPA)** based on the severity of the harm and the requirement of mitigating responses by the data subjects. |

**Conclusion and Way Forward**

Through the comparison matrix, it can be inferred that GDPR is focused in its approach towards enshrining privacy and data protection as key rights for users. China has its own unique approach, while the APEC framework has established principles for data flows and protection. At the same time, California takes a narrow approach to protection targeting only specific kinds of processing.

GDPR gives a broad definition of personal data and has a separate category for sensitive personal information much of what is reflected in India's proposed PDPB. However, India goes a step further by authorising government to specify categories of personal data as sensitive. Other jurisdictions broadly recognise sensitive information as information which might result in discrimination or cause harm, thus providing clear principle/ rationale for classification.

While most jurisdictions recognise the exemption from data protection provisions for law enforcement and judicial purposes, GDPR provides for the principle of necessity and proportionality which is absent from the PDPB, which authorises government to exempt any government agency.

With respect to cross border data flows, while GDPR allows comparatively free data flows to adequately compliant countries, this is in contrast with China's framework which adopts for localisation requirement. APEC framework in this regard is specifically notable as it establishes principles for protection and data flows considering balanced approach and leaves it on individual states to still frame their own laws based on certain principles as enshrined within APEC framework. Japan is also trying to move towards such balanced approach by allowing transfers with equally compliant countries. India, however, appears to be providing a lot of discretion to the government and the data protection agency to allow or prevent cross border data flows, without any guiding principles in this regard.

With regard to consent mechanisms, apart from the principles of free, clear, legitimate consent which are similar to that of GDPR, India's law is a step ahead and provides for consent managers as a separate set of data fiduciaries to provide and withdraw consent. However, it needs to be ensured that such data fiduciaries do not end up becoming gatekeepers of consent. India can also learn from APEC

framework which requires consent mechanisms to be easily understandable, accessible and affordable. In relation to rights of data subjects and penalties thereof, GDPR has a broad framework which gives complete control of data within the hands of the consumer while APEC privacy framework and California Consumer Protection law have more limited rights. While the PDPB provides several rights, it should include right to restrict processing and right against data processing.

It is necessary to ensure consistency among individual data protection regimes to give shape to a global data governance regime, for fostering data flows and leveraging value of data and ensuring optimum data protection for the users. This is especially important for an economy such as India, which has second-highest internet users after China and immense potential for growth of digital economy. While the government is considering frameworks for non-personal data as well as personal data it will be pertinent to take an approach of reviewing laws from other jurisdictions and reflect on best practices. This will help in designing optimal provisions which can enhance protection and at the same time foster growth of the digital economy.

In lieu of the above, following proposed in the PDPB 19:

- **Definition of Sensitive Personal Data (section 2(36))** – Informed by the Japanese and Chinese frameworks, a guiding principle could be adopted in section 2(36) for considering **such personal data as sensitive personal data, unauthorised use of which could lead to physical, property, or psychological harm to data principals**. In addition, passwords should be inserted in the list of sensitive personal data as it is considered as a data protection tool by users as validated by CUTS consumer perspective study on privacy, data protection and data sharing.
- **Classifying Personal Data as Sensitive Personal Data (section 15)** – To avoid confusion and ensure clarity, the terms 'significant harm' in section 15 should be replaced with 'physical, property or psychological harm'. In addition, for promoting transparency, competitive neutrality and preventing abuse of discretion, **the government must be required to undertake cost-benefit analysis and release its findings in public domain while proposing alteration in the definition of sensitive**

**personal data.** As a result, it will need to justify that the benefits of classifying a set of personal data as sensitive personal data while excluding other similar sets of personal data outweigh the costs of such action.

- **Purpose limitation (section 4(b))** – At present, data fiduciaries are allowed to process the personal data for purposes which is 'incidental to' or 'connected with' the purpose consented to by the data principal. Use of such terms leaves a lot of ambiguity. Informed by the APEC and GDPR framework, these terms should be replaced with **'purposes compatible with such purposes' to ensure direct linkages between consent provided by the data principal and purpose for which the data is processed.** While ensuring data protection, this will also promote innovation. The legislation may also provide examples of compatible purposes, as provided in the APEC framework.
- **Exemptions (section 35)** – Much like the GDPR, and in compliance with the *Puttaswamy* judgment, the PDPB should require the **government to justify that the order exempting its agency from PDPB complies with the principles of legality, necessity and proportionality.** In this regard, the **government must be required to undertake a cost-benefit analysis and release its findings in public domain** to justify that the costs of its action are outweighed by the benefits.
- **Data Flows (section 33 and 34)** – To promote transparency and avoid abuse of discretion, **while notifying critical personal data** under section 33, the **government should be required to undertake cost-benefit analysis** and release its findings in public domain to justify that benefits of its action outweigh the costs. Similarly, **while making a decision under section 34(2)(b)** on whether a transfer prejudicially affects the security and strategic interest of the state, **the government should be required to undertake cost-benefit analysis** and release its findings in public domain to justify that benefits of its action outweigh the costs. In addition, the government should adopt principles from GDPR, APEC and Japanese frameworks to pre-approve transfers of data to jurisdictions adopting high-quality data protection standards. The government should also enter into bilateral and multilateral partnerships for ensuring cross-border data flows.

- **<u>Notice (section 7(2) )</u> –** While the PDPB provides that the notice under section 7(2), is concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable, based on APEC privacy framework, **principles of easy accessibility and affordability of notice should also be adopted** in section 7(2).
- **<u>Data Protection Authority (section 42)</u>** –PDPB prescribes formulating a selection committee for setting up the DPA which consists of the members of the executives of the government, hence, it comprises on the independence of the functioning of the regulatory body through an indirect oversight of the executive. **Both GDPR and Japan's APPI provides for an independent regulator for the implementation of the provisions of the legislation through specifically providing administrative and financial independence and that such authority should not be directly or indirectly influenced by external factors.** Considering that India should reconsider the independence of the regulator with respect to current provision, and should include members of the judiciary, experts in data protection and civil society members in the selection committee to ensure its administrative and financial autonomy along with members of the executive.
- **<u>Non- Personal Data and Voluntary Verification by Social Media Intermediaries (section 91 and 93)</u>**- PDPB Provides for transfer of non- personal to government in certain cases for policy-making or delivery of services and provides for voluntary verification**, both these provisions are not within the scope this bill as this bill specifically focuses on personal data protection**. No such provisions are provided in any other privacy law in other jurisdictions, hence these provisions must be removed from the bill.
- **<u>Grievance Redress (Chapter V and Section 83)</u>** – In the current form, PDPB limits the right of data principals as it restricts the power of the courts to only take cognizance of the offence when the complaint is made by the DPA**. In order to give more powers to data principals regarding handling of their data, the data principal must be given the right to seek adequate judicial remedy in case of data breach and infringement of their rights under Chapter V which provides for rights of data principals and under section 83** as is also provided in the GDPR, APEC privacy framework and California Consumer Privacy Act.

- **Penalties (Chapter X) -** PDPB prescribes criminal sanctions and fines in the case of re-identification of the data without consent, although for other breaches penalties are only provided after the assessment by the inquiry officer regarding harm and violation. Like **the GDPR, the PDPB must include a guiding principle regarding the fines to be effective, dissuasive and proportionate to the harm caused within Chapter X which is focused on deciding penalties.**
- **Information regarding Data Breach ( section 23)** - GDPR, China's Cyber Security Law and Japan's APPI provides for data subjects to be informed about the harm in the case of data breaches. **PDPB should require for data fiduciaries to notify the data principals of the breach in case of likelihood of harm and give directions of mitigating such harm under section 23** as provided under China's Cyber Security law**.** This will give broader protection to the data principals.

**References-**


1. General Data Protection Regulation *(EU) 2016/679 (*GDPR*)*
2. APEC *Privacy* Framework *(2015)*
3. Cyber Security Law of People's Republic of China , Standing Committee of the National's Peoples Congress (2017)
4. Act on Protection of Personal Information 2003, Government of Japan (2017)
5. California Consumer Privacy Act of 2018 (2020)
6. Personal Data Protection Bill , Government of India ( 2019)
7. Wie Sheng, "One Year after GDPR, China Strengthens Personal Data Regulations, Welcoming Dedicated Law · TechNode," *TechNode* (blog), June 19, 2019, https://technode.com/2019/06/19/china-data-protections-law/.
8. Torre, Lydia. "GDPR Matchup: The California Consumer Privacy Act 2018."https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/.


******

For any queries please contact Amol Kulkarni at amk@cuts.org or Shubhangi Heda at sbg@cuts.org