April 8, 2020

Developments in India Data Protection

Melinda Claybaugh
Facebook, Inc.

Suhaan Mukerji
PLR Chambers, New Delhi

Kurt Wimmer
Covington & Burling LLP

Privacy+ Security Forum

1

Current Environment

Privacy+ Security Forum

India

Current Law

- *Puttaswamy v. Union of India* (2017) held that privacy is a fundamental right protected by Article 21 of the Constitution: "No person shall be deprived of his life or personal liberty except according to a procedure established by law."
- Information Technology Act (2000) currently governs data protection
- Reasonable Security Practices and Procedures and Sensitive Personal Data Rules (the "Rules") took effect in 2011
- The requirements of the Rules include: Companies must have a privacy policy, must permit access and correction, must make certain disclosures upon collection, and may collect sensitive personal information only on consent. Transfers and use of sensitive data are restricted.

2

Data Protection Law (2019)

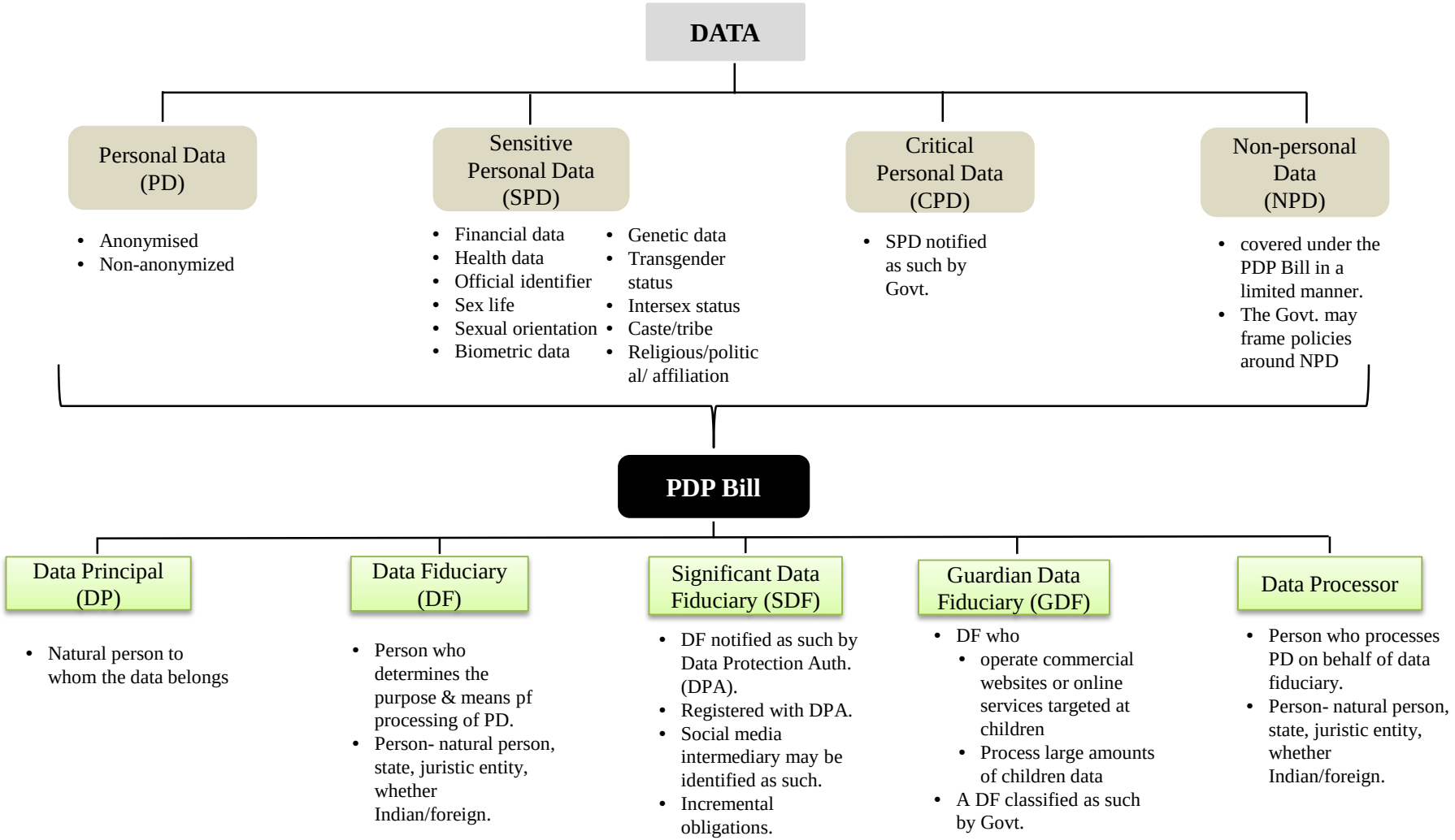
Privacy+ Security Forum

BACKGROUND

- The Personal Data Protection Bill, 2019 was introduced in Parliament in December, 2019 and has been referred to a Joint Parliamentary Committee for review.
- Unless otherwise specified, this presentation will use the following abbreviations –
  - Personal Data Protection Bill ("**PDP Bill**", "**the Act**")
  - Data Protection Authority ("**DPA**")
- Wherever applicable, this presentation will indicate if the Act is General Data Protection Regulation, 2016 ("**GDPR"**) compliant ("**GDPR+**") or not compliant ("**GDPR-**") "GDPR +" indicates an equivalent or higher standard in the PDP Bill and "GDPR –" indicates some aspects of a particular provision falling short of standards in the GDPR.
- This Presentation will set out basic concepts and principles of the PDP Bill and provisions that are applicable to entities handling Personal Data ("**PD**") *i.e*. Data Fiduciaries ("**DF**") and the procedure that must be followed in order for Data Fiduciaries to comply with the Act.

PDP BILL: CONCEPTUAL FRAMEWORK

- Types of data
- Data Principals (“**DP**”)
- Types of regulated entities: Data Fiduciaries (“**DF**”), Significant Data Fiduciaries (“**SDF”**) and Data Processors
- Obligations of regulated entities
- Encryption and anonymization
- Purpose and Collection Limitations
- Notice and consent
- Data Retention
- Data Localization and cross-border data flows
- Processing of Personal Data (“**PD”**) and exemptions
- Treatment of PD belonging to children
- Rights of DP
- Privacy, transparency and accountability
- Reporting data breach
- Harms


DATA
Personal Data (PD)
Anonymised
Non-anonymized
Sensitive Personal Data (SPD)
Financial data
Health data
Official identifier
Sex life
Sexual orientation
Biometric data
Genetic data
Transgender status
Intersex status
Caste/tribe
Religious/political/ affiliation
Critical Personal Data (CPD)
SPD notified as such by Govt.
Non-personal Data (NPD)
covered under the PDP Bill in a limited manner.
The Govt. may frame policies around NPD
PDP Bill
Data Principal (DP)
Natural person to whom the data belongs
Data Fiduciary (DF)
Person who determines the purpose & means pf processing of PD.
Person- natural person, state, juristic entity, whether Indian/foreign.
Significant Data Fiduciary (SDF)
DF notified as such by Data Protection Auth. (DPA).
Registered with DPA.
Social media intermediary may be identified as such.
Incremental obligations.
Guardian Data Fiduciary (GDF)
DF who
operate commercial websites or online services targeted at children
Process large amounts of children data
A DF classified as such by Govt.
Data Processor
Person who processes PD on behalf of data fiduciary.
Person- natural person, state, juristic entity, whether Indian/foreign.

COLLECTION AND PURPOSE LIMITATION

GDPR +

Proposed Law

- Collection of PD is only permitted where it is necessary for the purpose of its processing. The PDP Bill takes away the necessity requirement for the purpose of processing of PD.
- A DF must only process PD for specific, clear and lawful purpose and in a fair and reasonable manner, i.e. in a manner that ensures an individual's privacy is at the centre stage.
- The processing of Sensitive Personal Data is only permitted where the same is necessary for any lawful purpose connected with a function or activity of the body corporate.
- The use of the terms "specific" and "clear" provide for a lesser burden and must be construed to mean that processing shall be permitted so long as the personal data is being processed for a specific purpose which is
  - clearly notified to the DP and for which they have given consent; or
  - where the purpose is incidental to or connected with purpose for which the DP would reasonably expect the PD to be used for given the context and circumstances in which the data is collected.

Recommendation/Impact

- A DF will have to identify the types of data being collected, the purpose for which each of these types of data are needs, and the manner in which each of these types of data will be processed.
- The manner in which disclosures are made to DPs will change accordingly.
- Privacy policies will have to be reviewed and modified to include, in an unambiguous manner, details relating to the types of data that are being collected by the DF along with the purpose for and extent of its processing.

NOTICE

GDPR +

Proposed Law

- At the point of collection of data, a Data Fiduciary must inform the Data Principal of the following details in clear, concise and easily understandable manner, in multiple languages where necessary and practicable –
    - Nature and types of Personal Data being collected along with the duration of its retention;
    - Purpose of processing of Personal Data;
    - The provision of withdrawal of consent and the manner in which it may be withdrawn
    - Complete identification details of the Data Fiduciary and its Data Protection Officer (DPO);
    - Third-parties with whom the collected Personal Data will be shared;
    - Details of any cross-border transfer of Personal Data;
    - Grievance redressal mechanism;
    - Existence of rights of Data Principals and the manner in which they may be exercised;
    - Assigned trust score;
- Notice is not necessary in cases where giving such notice would substantially prejudices the purpose of processing.

Recommendation/Impact

- Existing notice mechanisms will have to be reviewed and accordingly modified.
- The manner in which disclosures are made to Data Principals will change accordingly.
- Data Fiduciaries will have to ensure that requisite disclosures are made before the collection of Personal Data in a clear and concise manner, preferably in multiple languages.
- Data Fiduciaries must ensure that all the details set out in the PDP Bill and reproduced above are disclosed to the Data Principal.

CONSENT

GDPR +

Proposed Law

PERSONAL DATA

- PD cannot be processed without valid consent.
- Explicit consent is necessary where it is being retained for a longer period.
- Consent/explicit consent is to be obtained before processing commences
- Consent is valid when it is –
  - Free
  - Informed
  - Specific
  - Clear
  - Capable of being withdrawn
- Valid informed consent entails communication of information on the likelihood of significant harm which may be caused to DP is conveyed to DP.
- If the DP withdraws consent without a valid reason then all legal consequences to be borne by DP.
- For PD of child, consent of parents or guardians is to be obtained.

SENSITIVE PERSONAL DATA

- SPD cannot be processed without explicit consent.
- Explicit consent is to be obtained before processing commences
- Such explicit consent is valid when it is –
  - Free
  - Informed
  - Specific
  - Clear
  - Capable of being withdrawn
- Information on the likelihood of significant harm which may be caused to DP is conveyed
- Consent is separately obtained for different categories of SPD.

Recommendation/Impact

- A DF must review its existing consent mechanism and match it with the validity of consent under the PDP Bill.
- Consent must be obtained before processing any PD and explicit consent before processing any SPD or PD, as the case may be.
- A DF must ensure they have a clear record of obtaining consent as the burden of proof vests on the DF to show that they had obtained consent before processing,
- A DF must ensure that it does not make the availability/ offering of goods, services or performance of any obligation, enjoyment of any legal right contingent upon consent.
- A DF must allow for consent withdrawal mechanism and record the reasons of such withdrawal of consent.
- A DF must allow for consent managers to manage consent for and on behalf of a DP.
- For PD of child, consent of parents/guardians to be obtained. A DF must confirm whether they are classified as guardian DF.

PROCESSING OF PD WITHOUT CONSENT

Proposed Law

- Grounds of necessity for processing Personal Data without consent are as follows –
  - Where the Data Principal receives any service or benefits from the State,
  - Under any other Central or State Law for the time being in force;
  - In compliance with Court orders;
  - Responding to a medical emergency or in the event of a public health emergency,
  - During disaster or breakdown of public order.

- Such processing is permitted where it is necessary for employment related purposes and where obtaining consent is inappropriate having regard to the employment relationship or disproportionate effort for Data Fiduciaries keeping in mind the nature of processing.

- Processing is necessary for a reasonable purpose, which shall be specified through regulations and also having regard to
  - Data Fiduciary's interest in processing such data and ability to obtain consent from the Data Principal
  - The effect of such processing on the rights of the Data Principal and the Data Principal's reasonable expectations with regard to the same
  - In public interest.
- "Reasonable Purpose" shall include –
    - Prevention and detection of unlawful activities;
    - whistle blowing;
    - mergers & acquisitions;
    - network & information security;
    - credit scoring;
    - recovery of debt;
    - processing of publicly available Personal Data;
    - operation of search engines.

General Obligations on Data Fiduciaries

GDPR +

Proposed Law

- Quality of personal data –
  - Processed Personal Data should be complete, accurate, updated and not misleading.

- Retention of Personal Data –
  - Only for a period necessary for processing;
  - Deleted beyond such period;
  - May be retained beyond such period if explicit consent has been obtained,
  - Personal Data to be deleted where retention not necessary.

- Accountability provisions in the PDP Bill places liability for failure to comply with the PDP Bill while processing of Personal Data by Data Fiduciary or by any other person on its behalf on the Data Fiduciary alone.

- Where the Data Fiduciary processes Personal Data of children, it shall –
  - Do so in a manner which protects the rights of, and is in the best interest of the child;
  - Verify the age of the child in the prescribed manner;
  - Obtain consent of parents/guardians;
  - Comply with regulations governing profiling, tracking, or targeting advertisements at children notified by the DPA, where the Data Fiduciary offers counselling or child protection services.

- As a transparency requirement, the following information must be available and communicated periodically to the Data Principal –
  - Categories of Personal Data being collected, manner of such collection, the purpose of processing, important operations in such processing,
  - Categories of Personal Data processed in exceptional situations/purposes that creates a risk of significant harm
  - Procedure for exercise of rights of DP, including the rights to file complaints to the Authority;
  - Data Trust Scores;
  - Information as applicable to cross-border transfers of Personal Data that Data Fiduciary carries out.

General Obligations on Data Fiduciaries (Contd.)

Proposed Law

- Where the DPA is of the view that any processing by the Data Fiduciary carries risk of significant harm, it shall notify the same and all incremental obligations of SDF shall be made applicable to DF.
- Data Protection Impact Assessment (DPIA) may be mandatory where specified by the DPA.
- A DPA certified Privacy by Design Policy is to be displayed on the DF's website.
- The Data Fiduciary and Data Processor(s) shall, introduce the following security measures and periodically review the same, These being –
    - use of methods such as de-identification and encryption;
    - steps necessary to protect the integrity of Personal Data ; and
    - steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.
- The Data Fiduciary is to notify personal data breaches to the DPA ,in cases where the breach is likely to cause harm to the DP, at the earliest or in such timeframe that may be specified through regulations.
- The Data Fiduciary is obligated to immediately deploy remedial measures to mitigate harm. Where the DPA directs that the breach be disclosed to the concerned DP, the DF must comply with such direction. Disclosure of the breach on the website of the DF may be mandated. [**GDPR—]**
- Grievance Redressal –
    - Data Fiduciary to have an effective and expeditious mechanism for grievance redressal;
    - Data Fiduciary to designate an officer for grievance redressal – the Data Protection Officer (DPO)
    - Complaints are to be resolved within 30 days;
    - Data Principal may file complaint with DPA in the following cases –
        - Data Principal is not satisfied with the resolution;
        - Complaint was not resolved within 30 days;
        - Data Fiduciary rejects the complaint of the Data Principal.

General Obligations on Data Fiduciaries - Recommendations

Recommendation/Impact

- Quality of Personal Data (PD) –
  - The DF will have to undertake steps to ensure that PD is complete, accurate and not misleading. The DF must have regard to whether PD is being used to make decisions about the DP, is disclosed to third parties, and is distinguished as PD obtained from facts and PD obtained from personal opinions and assessments.
  - If any PD is shared with any other DF or Data Processor does not fulfil these quality requirements, it must be notified to such DF or Data Processor.
- Data Retention -
  - Data Retention Policy must be periodically reviewed by the DF to determine the necessity for retention and explicit consent is to be obtained from DP for retaining PD for longer period.
  - All PD that does not need to be retained must be deleted, all PD retained beyond stipulated period and for which consent has not been obtained for such extended retention is to be deleted.
- PD of minors –
  - DFs need to create mechanisms to verify the age of their users.
  - Where the user is a child, the DF will have to create a mechanism to obtain consent from the guardian/parent.
  - DF will need to assess whether they are processing PD of children. Where the entity is a DF, it will have to assess the likelihood of significant harm which may be caused to the child by such processing.
- Accountability measures –
  - DFs must review and update their privacy policy in accordance with the PDP Bill and have the same certified by the DPA
  - Transparency requirements must be prominently displayed/otherwise easily available and communicated to DPs periodically.
- Security and Grievance Redressal Mechanisms –
  - DFs must strictly adhere to security safeguards and proactively monitor for Personal Data Breaches. DFs must inform the DPA in the event of breaches that are likely to cause harm to the DP. DFs must also undertake immediate measures to mitigate harm to the DP.
  - DFs must establish expeditious and efficient Grievance Redressal Mechanism and assign a DPO for the purpose of recording complaints from DPs.

INCREMENTAL OBLIGATIONS ON SIGNIFICANT DATA FIDUCIARIES

GDPR +

Proposed Law

- DFs will need to regularly confirm whether the DPA has notified them or their class of DFs to comply with the incremental obligations of a SDF.

- SDFs must necessarily –
  - Undertake DPIA where SDF intends to undertake any processing involving new technologies, or large scale profiling or use of SPD, or any other processing which is likely to cause significant harm to DP;
  - Appoint a Data Protection officer (DPO), based out of India, to:
    - Advice SDF on fulfilling its obligations under the PDP Bill, carrying out DPIA, on developing internal mechanism for privacy by design policy;
    - Monitoring processing activities and maintaining inventory of records for the SDF;
    - Assisting an cooperating with DPA on compliances with the PDP Bill;
    - Carrying out review of DPIA report and submitting the same to the DPA;
    - Acting as point of contact for grievance redressal
  - Maintain accurate and updated records of important operations of data lifecycle, security safeguard review, and DPIA.
  - Have its policies and processing routinely audited by a Data Auditor (DA) for compliance with provisions of this Act in the prescribed manner. If DPA is satisfied that SDF is conducting itself in a manner to the detriment of DP then it may mandate audit.
  - A social media intermediary notified as a SDF shall provide its Indian users the ability to voluntarily verify their accounts.
  - SDFs that are Social Media intermediaries must have a process to visibly indicate verified accounts by using a distinct mark.

Obligations on Guardian Data Fiduciaries (GDF)

Proposed Law

- A GDF providing exclusive counselling or Child Protection Services need not obtain consent from the guardian or parents before processing the child's PD.
- A GDF is prohibited from undertaking the following –
  - Profiling, tracking;
  - Behaviour monitoring;
  - Targeting advertising at children;
  - Any processing activity which can cause significant harm to the child.

Recommendation/Impact

- As a GDF, The GDF must create mechanisms to verify the age of its users.
- Upon verifying the age of their user(s), a DF must understand if they are classified as a GDF by the DPA or not.
- In case a DF is classified as such, it must –
  - Create a mechanism for obtaining consent from the guardian or parent, as the case may be before processing PD, except where it provides exclusive counselling or child protection services;
  - Not profile, track, behaviourally monitor the child or target advertisements at the child
  - Ensure that no significant harm is caused to the child by the processing of her PD by the DF.

RIGHTS OF DATA PRINCIPAL

GDPR +

Proposed Law

- Right to confirmation and access –
  - DP may seek
    - a confirmation from DF whether her PD is being processed by DF;
    - Details/ summary of PD processed or being processed by DF;
    - Summary of processing activities being undertaken by DF on a DP's personal data.
  - DP may seek identities of all persons with whom any PD or category of PD of DP is being shred by DF.
- Right to correction and erasure –
  - DP may exercise its right to correction, updation, completion of PD which any DF processes;
  - DP may seek erasure where the PD is not necessary for lawful processing;
  - Such request may be denied having regard to the purpose of processing.
  - Where DP is not satisfied with the DF's refusal, DP may ask the DF to mark the said data as disputed.

Recommendation/Impact

- A DF will have to have a mechanism in place to respond to the exercise of any of these rights by a Data Principal.
- A DF will have to provide access to information sought in a clear, concise and comprehensive manner.
- Where a DF agrees to correct, update, erase, complete the Personal Data of a Data Principal, it must notify the same to all persons to whom such PD may have been disclosed. A mechanism to this effect will have to be put in place by the DF.
- Where a DF denies a DP's request for correction, updation, completion or erasure of PD, it must communicate to them such denial in writing along with the justification for the same. A mechanism to this effect will have to be developed.
- A DF shall have to develop a mechanism through which they indicate that a particular PD is disputed.
- DF will have to maintain –
  - a list of persons with whom the DF shares any DP's PD;
  - summary of types of PD being processed and the types of processing being done on any DP's PD.

RIGHTS OF DATA PRINCIPAL (CONTD.)

GDPR +

Proposed Law

- Right to data portability –
  - This right can only be enforced where processing takes places through automated means;
  - Right to receive all data provided by her to the DF, all data generated while using DF's goods/services, and data of DP obtained by DF in any manner for any purpose;
  - Right to get all such PD transferred to another DF.
  - This right cannot be exercised where –
    - Processing is necessary for:
      - Provision of benefits by the State;
      - Comply with law or court order and
      - Complying with the request reveals a trade secret or is not technically viable;

- Right to be forgotten –
  - Can be exercised upon order of Adjudicating Officer (AO) to restrict or prevent the continuing disclosure of PD where–
    - Such disclosure is affected by Purpose Limitation,
    - Consent has been withdrawn;
    - Disclosure was made contrary to applicable law.
- These rights, other than the right to be forgotten, may be exercised by DP either on its own or through a consent manager by making an application to the DF in this regard.

Recommendation/Impact

- DF will have to have a mechanism in place to respond to a DP's exercise of her right to data portability in a structured, commonly used and machine-readable format.
- A DF shall have to comply with the order of an AO directing that right to be forgotten be enforced.
- Where a DF is of the opinion that the Adjudicating Officer has not passed an order on valid considerations under the Bill, it may apply for review of the order. A DF may also file an appeal against such an order.
- Where a DF complies with the request of a DP which wishes to exercise her rights, it must communicate the same within the specified timeframe.
- A DF may charge a fee from the DP when a request for exercise of rights is made by a DP. Note that requests in exercise of right to correction and erasure and right to confirmation are not chargeable and must be complied with free of cost.
- A DF is not obliged to comply with the request of a DP where compliance with the request shall harm the rights of any other DP.

PROCESSING – CROSS BORDER PROCESSING

GDPR +

No restriction on cross- border transfer and processing of PD.

Proposed Law

SENSITIVE PERSONAL DATA

- Conditional transfer is allowed where –
  - Contract or intra-group scheme fulfilling the following and approved by DPA exists that sets out –
    - Effective protection of rights of DP;
    - Liability of DF for any harms caused due to non-compliance
  - Central Govt. approves the transfer on being satisfied of adequacy requirements and where such transfer is not to the prejudice of law enforcement activities;
  - DPA has allowed transfer for any specific purpose.
- SPD can be stored only within India.

Proposed Law

CRITICAL PERSONAL DATA

- CPD is notified by the Central Government.
- Cannot be transferred or processed out of India,
- Except where it is –
  - Necessary for prompt action for health/ emergency services;
  - Transferred to a country where transfer is permissible by Central govt. and such transfer shall not have prejudicial effect on the security and strategic interest of the State.

Recommendation/Impact

- DFs must review and update policies related to the transfer of SPD and CPD in accordance with the PDP Bill.
- A DF must ensure that appropriate consent is obtained for the purpose of cross-border transfer of SPD/CPD.
- DFs must be aware of Central Government notifications on the classification of Data as SPD or CPD.
- A DF must ensure that contracts and intra-group schemes for cross-border transfer are consonant with the PDP Bill and are duly approved by the DPA.
- DF must be mindful of country-specific laws on transfer of PD and any other considerations as prescribed under the PDP Bill.

EXEMPTION FROM THE PROVISIONS OF THE PDP BILL

Proposed Law

- The Central Government may, by notification, exempt the processing of personal data of DPs outside India (pursuant to contract with natural/juristic person outside India) from the PDP Bill**.** This exemption shall equally apply to processing of data by companies outside of India by Data Processors within India.
- The PDP Bill exempts the manual processing of PD by small entities – Note that such exemption is from notice, quality of PD, retention requirements, providing of brief summary of processing activities to DP where the DP exercises its right of confirmation and access, responding to rights requests (apart from right to erasure) transparency and accountability measures.
- DPA may create sandboxes to encourage innovation and eligible DFs may apply for inclusion. Included DFs may be exempted, either fully or with modifications from collection, storage and purpose limitations. The term of inclusion is renewable with the total period not exceeding 36 months.

Recommendation/Impact

- As a DF, a DF must be mindful of notifications by Central Government regarding exemption from application for DPs not within the territory of India.
- DFs must ascertain if they are eligible for qualification as a “small entity” and for inclusion in DPA created sandbox upon furnishing of requisite information as provided under the PDP Bill.
- Applications by DFs for such exemption should furnish the following information –
  - The term of inclusion, which is renewable with a ceiling of 36 months
  - Adequate safeguards, including Terms and Conditions, Consent requirements and compensation to participating DPs and penalties for violation of these safeguards

3

Concerns of U.S. Industry

Privacy+ Security Forum

India

U.S. Industry Concerns

- Data localization – can it change, and how will it work if it does not change?
- Cross-border data transfer restrictions
- Children's privacy – and the definition of children as under-18s
- Requirement to share non-personal data with the government upon request
- Expansive power of the national regulator
    - Ability to define new categories of "sensitive" data
- Consent framework and grounds for processing data
    - Processing data to perform a contract
    - Vagueness of "legitimate interest" grounds

Questions? Thank you!

Privacy+ Security Forum

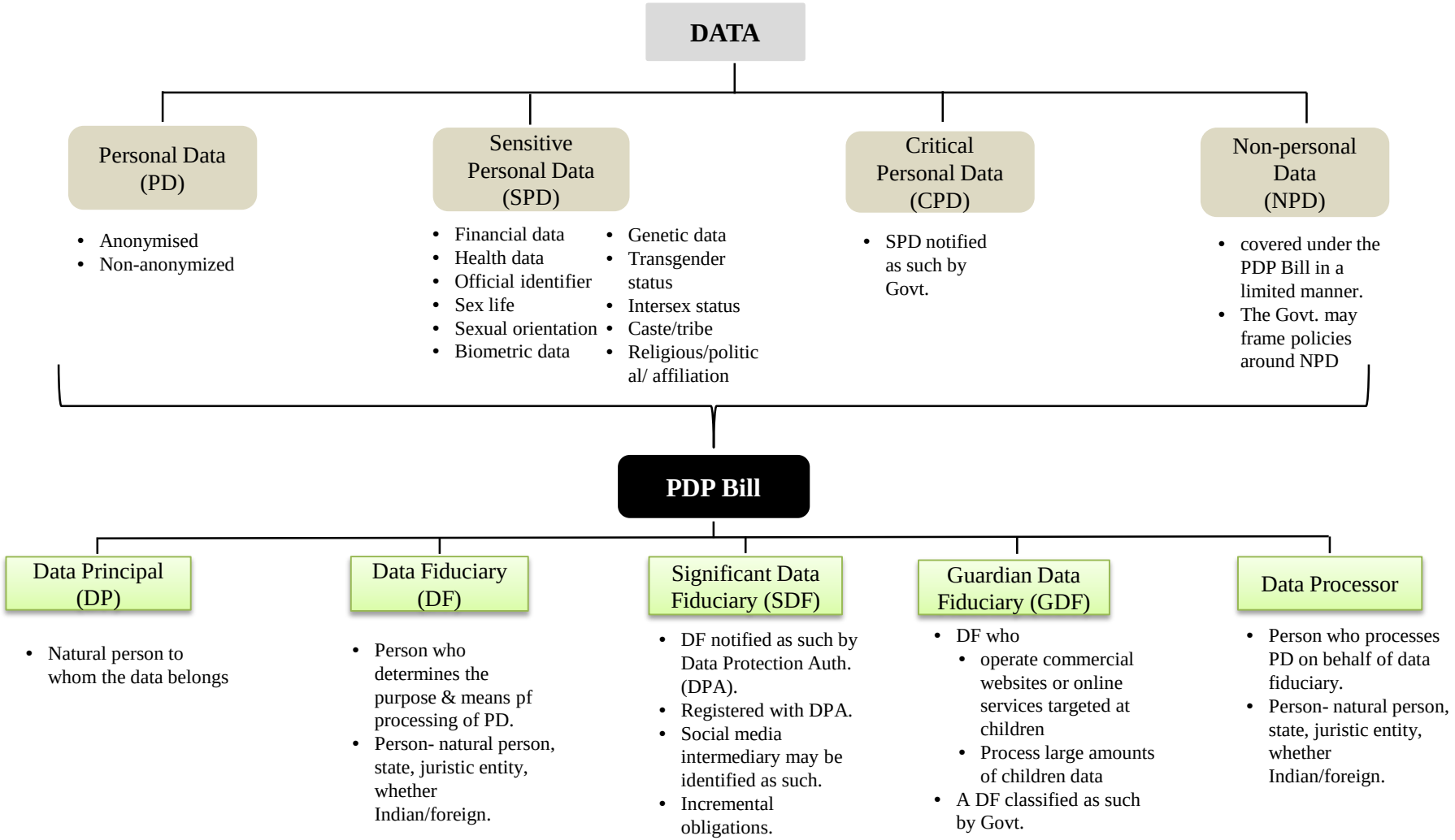
Melinda Claybaugh
Privacy Policy Director, Legislation
Facebook, Inc.
melindac@fb.com

Suhaan Mukerji
Managing Partner
PRL Chambers
suhaan.mukerji@prlchambers.com

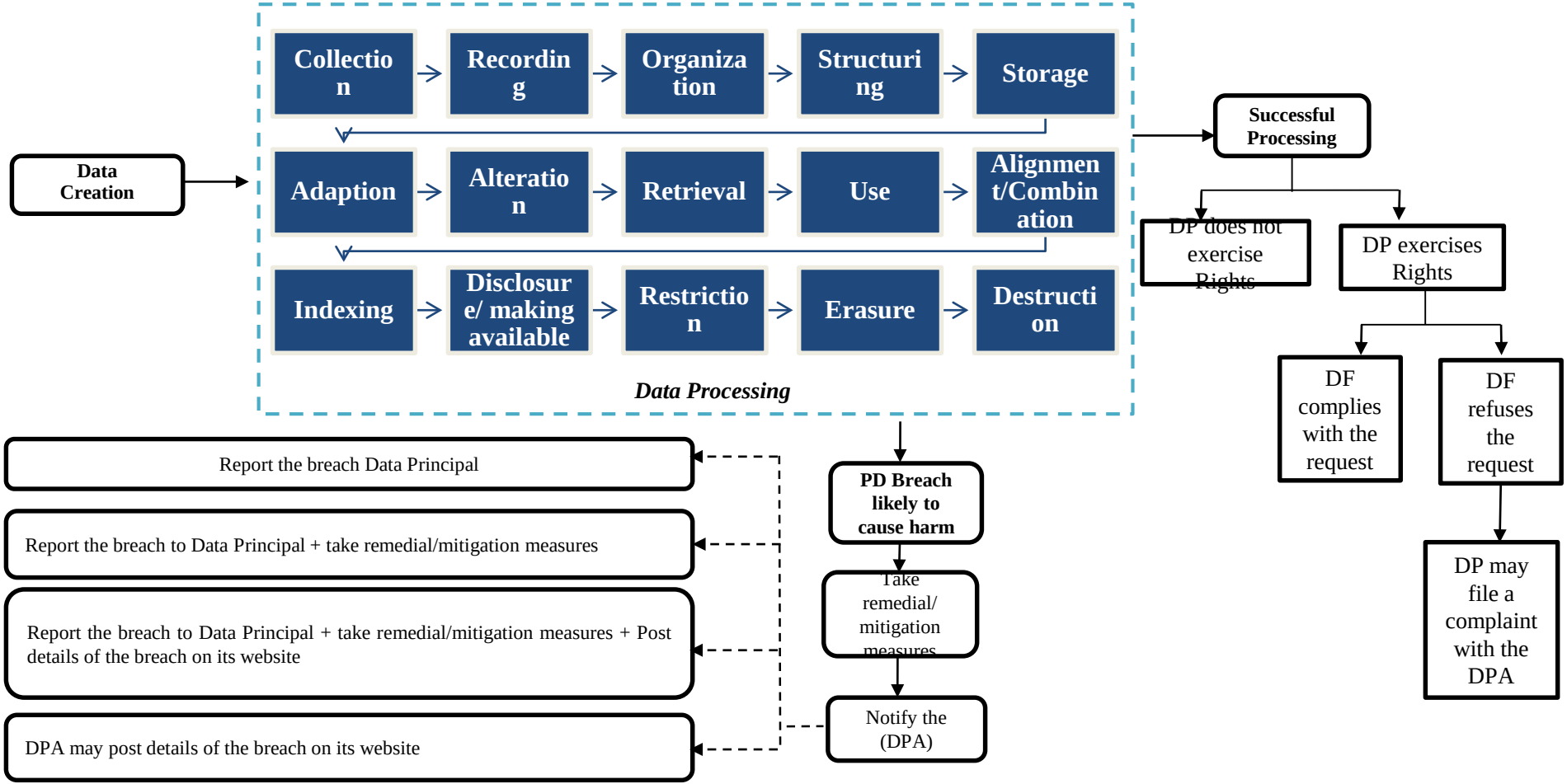
Kurt Wimmer
Co-Chair, Privacy Group
Covington & Burling LLP
kwimmer@cov.com

Appendix

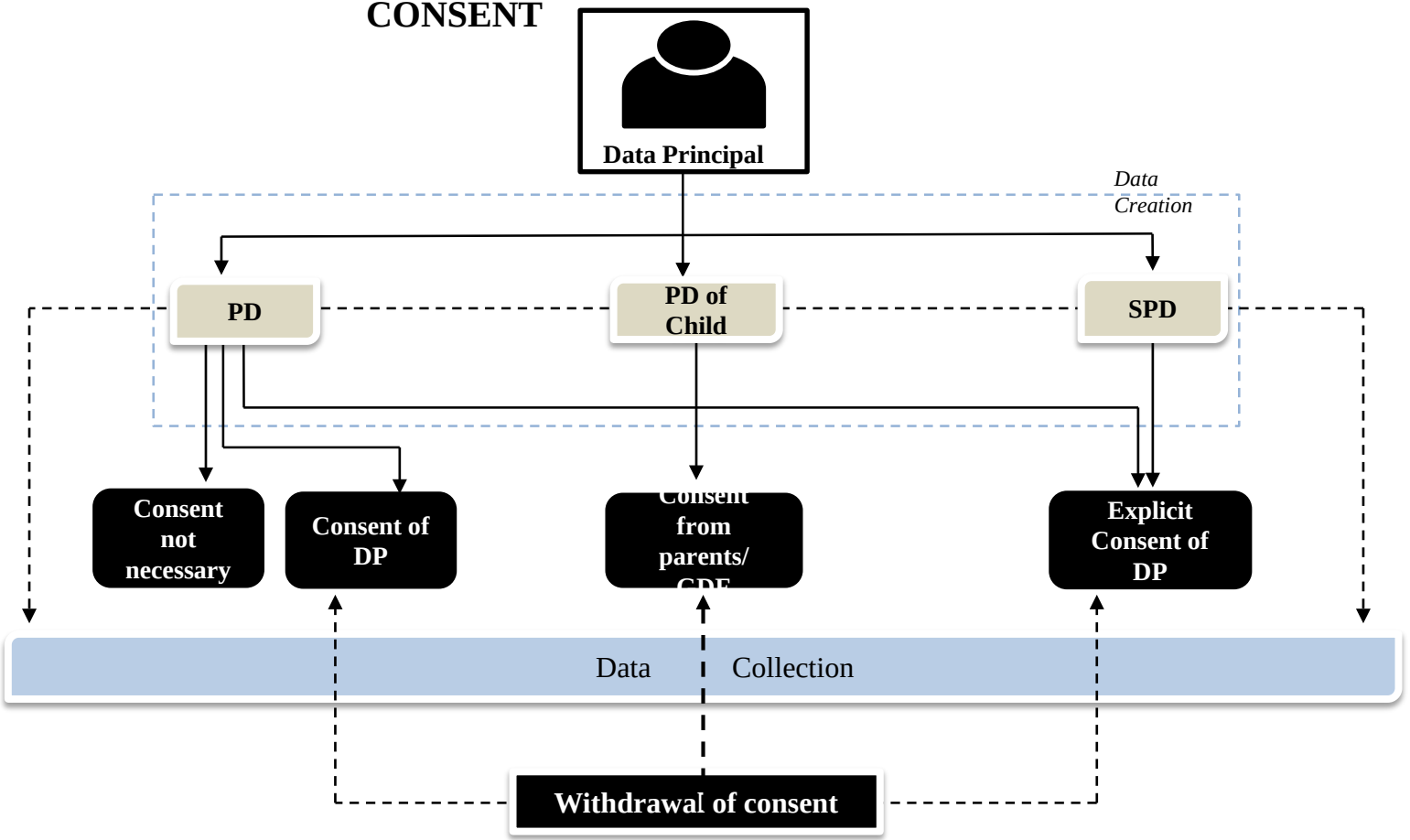
Suhaan Mukerji
Managing Partner
PRL Chambers
suhaan.mukerji@prlchambers.com


DATA
Personal Data (PD)
Anonymised
Non-anonymized
Sensitive Personal Data (SPD)
Financial data
Health data
Official identifier
Sex life
Sexual orientation
Biometric data
Genetic data
Transgender status
Intersex status
Caste/tribe
Religious/political/ affiliation
Critical Personal Data (CPD)
SPD notified as such by Govt.
Non-personal Data (NPD)
covered under the PDP Bill in a limited manner.
The Govt. may frame policies around NPD
PDP Bill
Data Principal (DP)
Natural person to whom the data belongs
Data Fiduciary (DF)
Person who determines the purpose & means pf processing of PD.
Person- natural person, state, juristic entity, whether Indian/foreign.
Significant Data Fiduciary (SDF)
DF notified as such by Data Protection Auth. (DPA).
Registered with DPA.
Social media intermediary may be identified as such.
Incremental obligations.
Guardian Data Fiduciary (GDF)
DF who
operate commercial websites or online services targeted at children
Process large amounts of children data
A DF classified as such by Govt.
Data Processor
Person who processes PD on behalf of data fiduciary.
Person- natural person, state, juristic entity, whether Indian/foreign.

LIFECYCLE OF PERSONAL DATA



CONSENT AND EXPLICIT CONSENT



Penalty	Quantum
SDFs failing to – • Take prompt and appropriate action in response to data security breach, • Register with the DPA • Undertake DPIA • Conduct Data Audit • Appoint DPO	Penalty up to INR 50 million or 2% of Total Word wide Turnover
• Comply with Rights requests of DPs.	INR 5000/day upto a maximum of INR 1 million
• Furnish Reports, returns, information etc.	INR 10,000/day upto a maximum of INR 2 million
• Comply with directions or orders	INR 20,000/day up to a maximum of 20 million
Residuary Penalties	Up to INR 10 million.
DFs failing to – • Take prompt and appropriate action in response to data security breach • Adhere to security safeguards • Cross-Border Data Transfer requirements • Comply with processing requirements relating to the PD of children • Comply with collection, storage and purpose limitation requirements.	up to INR 150 million or 4% of Total Wordwide Turnover
• Comply with provisions relating to non-consensual processing of PD.	INR 5000/day upto a maximum of INR 0.5 million
• Comply with Rights requests of DPs.	INR 10,000/day upto a maximum of INR 0.5 million
• Furnish Reports, returns, information etc.	INR 5000/day upto a maximum if INR 5 million
• Comply with directions or orders	INR 20,000/day up to a maximum of 20 million
Residuary penalties	Up to INR 2.5 million

COMPENSATION & OFFENCES

Compensation/Offences	Quantum
Compensation in case of harm	The quantum of compensation to be determined by the AO. DPs may claim compensations from DFs or Data Processors; The PDP Bill clarifies that no compensation under this Act preclude any penalty/punishment under any other Act.
Intentional, knowing re-identification/processing of de-identified data by any person.	Imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both.
Intentional, knowing re-identification/processing of de-identified data by company – every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.	As determined by adjudicating body.