GDPR–MUMBAI- 10-11-12 APRIL

GDPR, PERSONAL DATA PROTECTION BILL- 2018 -INDIAN CONTEXT

Atul Juvle
atulgjuvle@gmail.com
+91-99208 24036
11th April, 19

Disclaimer

Information/ opinions shared in this PPT is Privileged and meant only for the permitted recipients.

The information shared /views expressed are in personal capacity and should never be considered as views of Schindler/ Schindler GROUP.

Reproduction / recirculation for commercial use is prohibited.

Scope of Discussion

- Overview
- Historical Judicial pronouncements
- Current Regime
- Personal Data Protection Bill-2018
- Way forward
- Industry Specific issues

OVERVIEW

Overview

- The Information Technology (IT) Act- 2000- provided provisions on confidentiality, privacy, security for information stored in Computer.
- The IT (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information (SPDI)) Rules 2011.
- September-2016- Delhi HC- The Users policy of data transfer from WhatsApp to Facebook was upheld, but ordered (a) deletion of user data, who had opted out from service and (b) not to share information which was collected prior to updated user's policy.

Overview

- **2017-** Karnataka HC recognised *right to be forgotten* in sensitive cases and allowed deletion of name of Petitioner's daughter. (WP-62038 of 2016)
- **August 2017-** Justice K.S. Puttuswamy (Retd.) &Anr. v. Union of India & others- recognised a fundamental right to privacy exists under the Article- 19 & 21 of the Constitution and is enforceable against State even though it was not explicitly worded.
- **July 2018-** Draft- Personal Data Protection Bill-2018
- **Sept. 2018-** S/C declared Aadhar constitutional- subject to certain conditions.

HISTORICAL JUDICIAL PRONOUNCEMENTS

Other historical Judicial Pronouncements

- **Year-1953**- S/C held **no fundamental right to privacy** existed under the Constitution of India.- (M.P. Sharma & others v. Satish Chandra)
- **Year 1962-** S/C recognised the right to privacy in **minority opinion** in Kharak Singh v. State of UP. Since its was minority opinion, not binding.
- **Year-1975**- **S/C held first time a common law right to Privacy, even though not guaranteed by the Constitution in Govind Singh v. State of M.P.**
- **Year-1994**- S/C linked the Right to Privacy with Right to life Guaranteed under Article 21 of the Constitution, but also noted that it was not an absolute right- K. Rajagopal v. State of TN.
- **Year 2017-** Justice K.S. Puttuswami……...

CURRENT REGIME

SECTION 43-A OF IT ACT, 2000 & RULES MADE THERE UNDER

Section 43 A of IT Act –Failure to protect DATA

- **Personal Data / Information (PI)-** Rule 2(i)- Any information related to *natural person*, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, *is capable of identifying such person*
  and
- **SPDI-** Rule 3 -Sensitive Personal Data or Information - such personal information relating to –
  - (i) passwords (ii) financial information
  - (iii) physical, physiological, mental health condition
  - (iv) sexual orientation; (v) medical records & history
  - (vi) biometric information.

Exception : ANY information easily available / accessible in public domain or furnished under RTI will not be SPDI

Consent & Purpose

- **Rule 5-** collection of information – ***obtain consent*** in writing form provider of SPDI regarding ***Purpose*** of usage

- **Rule 5 (3)** When consent is obtained from the person concerned, then he must be informed about the purpose, intended recipients of information, name & address of agency collecting information & agency who will retain information.

Applicability & Exception

***The DPR** are applicable to a body corporate that is engaged in collection, receiving, possessing, storing, dealing or handling of SPDI using electronic medium and sets out compliance for protection of SPDI by such body corporate.

***DPR do not apply** to (i) natural persons who collect SPDI (ii) to standalone PI or (iii) Information purely in physical domain.

*DPR are applicable only to **body corporates located in India**

**IT Act, 2001 however applicable to an offence committed outside India, if such act involves a computer, computer system or computer network located in India.

PERSONAL DATA PROTECTION- BILL-2018

INTRODUCTION

- The NEED for data protection grew out of **PUBLIC CONCERN** about **PERSONAL PRIVACY** in the face of rapidly developing computer technology. And also obvious **MIS-USE**
- It works in two ways :

  i. Gives *certain rights* to individuals.

  ii. *Obligate* those who record and use personal information, to be open about that use.

- **Personal Data Protection Bill- July 2018**
  - 15 chapters, 112 sections, 2 schedules.

Certain Terms & definitions- Sec.3

- **'Personal Data'** shall mean all data relating to a *natural person* including data from which an individual may be identified or identifiable, either directly or indirectly.
- **'Processing'** is defined broadly as the *performance of operations* on Personal Data and will include, *inter alia*, collection, storage, retrieval, usage, disclosure, transfer, structuring, alignment or combination, indexation, and erasure.
- **'Sensitive Personal Data'** shall include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. The DPA will be given the residuary power to notify further categories in accordance with the criteria set by law.

Certain Terms & definitions- Sec.3

- **'Data Fiduciary':** any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data; (Data Controller under GDPR)
- **'Data principal':** the natural individual to whose personal data is gathered. (Data Subject- under GDPR).
- **Data processor:** any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary.

APPLICABILITY

The law will cover processing of personal data by both **public and private** entities. The bill administers all processing of personal data:

(i) within India.

(ii) by state, non-state or foreign entities, within India.

(iii) by data fiduciaries or data processors not present within India but having connection with any business in India.

Exception: The bill is not applicable to anonymized data, this exclusion will not extend to mere de-identification, a potentially reversible process where identifiers have been removed, masked, or replaced with unique codes.

OBLIGATIONS OF DATA FIDUCIARY- Chapter II-

- 1. Personal information must be fairly and lawfully processed
- 2. Personal information must be processed for ***limited purposes.***
- 3. It respects principles of *collection limitation* and storage limitation.
- 3. Information regarding data processing must be notified to Data principle
- 4. Such Notification must be easily comprehensible and in multiple languages where necessary

- More or Less similar to GDPR

OBLIGATIONS OF DATA FIDUCIARY-

- Section 8- giving of Notice to data principal- prerequisites of such notice are :

  Reason for which PD is being handled

  Identity & contact details of Data Fiduciary & DPO

  Right of data foremost to pull back assent & system of withdrawal

  Any cross border transfer of PD

  The method of complaint redressal

CONSENT for PD- SECTION 12

- **Free**, having regard to whether it meets the standard under section 14 of the Indian Contract Act, 1872
- **Informed**, having regard to whether the data principal has notified of his/her data that is being processed
- **Specific**, having regard to whether the data principal can determine the scope of consent in respect of the purposes of processing
- **Clear**, having regard to whether it is indicated through an affirmative action that is meaningful in a given context
- Capable to be withdrawn.
- **Section 13-** enables the Parliament & State to process PD if its important to their functions.

CONSENT for SPDI- SECTION 18

- **Explicit** consent is a must in case of collection or processing of sensitive personal data
- Compliance of section 12 and
- **Informed** and draws attention of Data principle to the purpose of processing data
- **Clear** having regard to whether it is meaningful without recourse to inference from conduct in a context
- **Specific,** weather data principles given a choice to separately providing consent to data processing

Grounds for processing of PD- Chapter 3

The Bill allows processing of data by fiduciaries if **consent** is provided.

However, in certain circumstances, processing of data may be *permitted without consent of the individual*.

These grounds include:

(i) if necessary for any function of Parliament or state legislature, or if required by the state for providing benefits to the individual,

(ii) if required under law or for the compliance of any court judgment,

(iii) to respond to a medical emergency, threat to public health or breakdown of public order, or,

(iv) for reasonable purposes specified by the Authority, related to activities such as fraud detection, debt recovery, and whistle blowing.

Grounds For Processing of SPDI- Chapter 4

With **explicit consent** by data principle and

However allows for processing data in following grounds without any consent

in cases :

a. which require 'explicit consent of the principal, as explained under section 12 of the bill'.

b. necessary for any function of Parliament or state legislature, or, if required by the state for providing benefits to the individual, or

c. required under law or for the compliance of any court judgment.

d. for prompt action during medical emergency, incident of public threat or any breakdown of any public order.

Personal and SPDI of Children- Chapter -V

- **Section 23**
- **Data Fiduciaries** are required to implement appropriate mechanisms for *age verification* and *parental consent* before Processing Personal Data of Children *(persons below the age of 18 years)* based on volume, proportion and possibility of harm to children arising out of processing of personal data.
- Data fiduciaries who operate commercial websites or online services or who process large volumes of personal data of children are classified as Guardian Data Fiduciaries.

Personal and SPDI of Children- Chapter -V

- They shall be barred from profiling, tracking, or behavioral monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.

EXCEPTION: Guardian data fiduciary- are providing counseling or child protection services to a child.

Rights of Data Principal- Chapter VI

- **Similar to GDPR**
- **Right to Confirmation & Access:** Section 24-The Data Principal has right to obtain confirmation whether Data Fiduciary is processing or has processed its PD:

- **Right to correction :** Section 25- The Data Principal has right to demand correction of inaccurate or misleading PD, completion of PD if its incomplete, update.

Rights of Data Principal- Chapter VI

- **Right to Data Portability (Section 26) :** Receive the personal data in a structured, commonly used and machine-readable format:

(i) Which such data principal has provided to the data fiduciary;

(ii) which has been generated in the course of provision of services or use of goods by the data fiduciary; or

(iii) which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained.

- **Exceptions:** to Data Portability.

(a) processing is necessary for functions of the State; (b) processing is in compliance of law; or (c) such compliance would reveal a trade secret of any data fiduciary or would not be technically feasible.

Data Principal's rights

- **Right to be forgotten (Section 28):**

The data principal may restrict or prevent continuing disclosure of personal data, in cases where the :

(a) Applicability is determined by Adjudicating officer. (Section 68)

(b) Restriction of disclosure of personal data overrides the right to freedom of speech and expression and the right to information of any citizen.

Transparency & Accountability- Chapter VII

Data Fiduciary is obligated to implement policies and measures to anticipate, identify and avoid harm to **Data Principal**.

Data Fiduciary **must** comply with the following ; (1) categories of collecting and the manner of collection of personal data. (2) the purposes for which personal data is generally processed. (3) any exceptional purpose of processing data that creates risk of significant harm. (4) the existence of and procedure for the exercise of data principal rights. (5) the existence of a right to file complaints to the Authority.

Transparency & Accountability- Chapter VII

(6) **Security Safeguards** to be taken by Data fiduciaries as well as data principles. (7) **Personal Data Breach (separate slide)**

(8) Data Protection Impact Assessment - A data protection impact assessment has to be undertaken if the data fiduciary intends to undertake *any new processing technologies* or *large scale profiling* or *use sensitive PD* or *other processing* which carries a risk of *significant harm* to data principals.

(9) Record Keeping and Audits - Accurate and up-to-date records of important operations in the data life-cycle have to be maintained by the data fiduciary. The data fiduciary has to conduct an annual audit of its policies and processing of PD by an independent data auditor, who will evaluate the compliance of the data fiduciary with the bill.

Breach of Personal Data – Section 32

Any *un-authorised* or *accidental disclosure*, *acquisition*, *sharing* , *use* , *alteration*, *destruction, loss of access* to PD that compromises the *confidentiality*, *integrity* or *availability* of PD to Data Principal.

Data Fiduciary to notify breach of PD to the Authority as soon as possible. *(No time limit prescribed departure from GDPR)*

The notification to Data principle shall be sent only on directions given by DPA. *(departure from GDPR)*

This shifts the burden of deciding the materiality of breaches from the Data Fiduciaries to DPA

Significant Data Fiduciaries

- The DPA shall notify certain data fiduciaries as significant fiduciaries based on the volume and sensitivity of Personal Data Processed.
- They are subject to enhanced obligations such as impact assessment, registration, audit, and appointment of a Data Protection Officer (DPO).
    - ***Departure from GDPR or Current IT Rules***
- Foreign Data Fiduciaries carrying out any processing must appoint an India based DPO.

Grievance Redressal Sec.39

- Every Data Fiduciary shall have an effective grievance redressal mechanism to address the grievances of the data principals.
- Grievance shall be effectively addressed within 30 days
- If the same is not redressed or Data Principal is not happy, he has right to approach Adjudication wing of the Authority.
- **Appeal** shall lie with **appellate Tribunal** established under Bill
- **Appeals** from **Tribunal** shall lie with **Supreme Court**

- **Grievance process is similar to current mechanism**

REGULATORY AUTHORITIES

- Independent body called the **Data Protection Authority of India. DPA**
- Establishment of Independent **Appellate Tribunals**.
- **Wide range of duties of DPA :** such as :
  - identifying additional categories of SPD and grounds for Processing Personal Data;
  - mandating breach notifications to Data Principals;
  - prescribing various codes of practice including for notice, transparency, security standards, de-identification and anonymization, contractual clauses and inter-group schemes for cross-border transfer;

REGULATORY AUTHORITIES

- **Powers of DPA:**

(a) calling for information;

(b) conducting inquiries;

(c) issuing codes of practice; and

(d) issuing directions to Data Fiduciaries or data processors.

These directions may range from restricting operations to prohibiting cross-border data flows. The DPA is also conferred search and seizure powers and powers of attachment of property to recover penalties.

Transfer of Personal Data outside India

- **Critical Personal Data** - Critical Personal Data as categorized by DPA, can be stored only on Indian servers. [Section 40(2)] *Challenge*
- **Cross-Border Transfer** – Personal data (except sensitive personal data) may be transferred outside India under certain conditions. These include: (i) where the central government has prescribed that transfers to a particular country are permissible, or (ii) where the Authority approves the transfer in a situation of necessity. [Section 41]
- **Exemptions** – The Bill provides exemptions from compliance with its provisions, for certain reasons including:

  (i) state security,

  (ii) prevention, investigation, or prosecution of any offence, or

  (iii) personal, domestic, or journalistic purposes.

PENALTIES & REMEDIES

- **If Data Fiduciary contravens any provision of section 69(1)** monetary penalty 2% of total worldwide Turnover or which may extend to Rs. 5 crores INRs, whichever is higher. (Non performance of obligations)
- **If Data Fiduciary contravens any provision of section 69(2)** monetary penalty 4% of total worldwide Turnover or which may extend to Rs. 15 crores INRs, whichever is higher. (violations under Chapter II, III, IV & V)

- Enquiry by Adjudicating authority shall be held.

OFFENCES – CHAPTER XIII

- **Offences such as obtaining, transferring or selling of PD or SPDI. The Re-identification and processing of such data without consent of Data fiduciary or data processor-**
- **Offences non-bailable & cognizable**

- **Section 95- Offence by companies- every person who at the time of offence was committed, was in-charge of and was responsible to company for conduct of Business of the Company**. *Departure*

- When offence committed by Central or State Government's department then Head of the Department shall be guilty of the offence.

OFFENCES & PENALTIES

- A new offense has been proposed for knowingly reversing de-identification
- **Compensation** – The Bill also provides for any data principal who has suffered harm as a result of any violation of any provision under this Act, by a data fiduciary or a data processor, shall have the right to seek compensation from the data fiduciary or the data processor. (Section 74)- un-capped liability.

Proposed Amendments to other regulatory provisions

- The Bill proposes amendments in certain laws:

✓ omission of 43A and Section 87 of the Information Technology Act, 2000, and

✓amendment in Section 8 of the IT Act, 2000 and the Census Act, 1948.

- Bill provides minimum data protection standards for all data processing in the country. In the event of inconsistency, the standards set in the data privacy law will apply to the processing of data.
- The Committee recommended amendments to the Aadhaar Act, 2016 to bolster its data protection framework Section 111 and 112 of the Bill

WAY FORWARD

WAY FORWARD

1. Review current data available with organisation
2. Understand business operations
3. Review Data flow
4. How data is captured?
5. Where data is stored ? Who is responsible? Who has access?
6. Draft POLICY & Notice
7. Review of current system for Modification or Replacement.
8. Agreements- amendments and renewals
9. Review data security practices & flag potential risks.

INDUSTRY SPECIFIC

TELECOMMUNICATION

1. What all DATA to be collected

2. Sharing of DATA with third parties

3. Data of Foreigners availing services

4. Compliance with cross-obligations- TRAI

4. COMMON – issue compliance with the new LAW

HEALTHCARE

1. What all DATA to be collected
2. Data accessibility & data correction
3. Sharing of data with third parties- specific consent
4. When no time to ask for consent- accident/emergency
5. Review of current systems- CCTV, Storage of data

6. COMMON – issue compliance with the LAW

INSURANCE

1. What all DATA to be collected
2. Sharing of DATA with third parties
3. Data of Foreigners availing services
4. Compliance with cross-obligations- IRDA

5. COMMON – issue compliance with the LAW

HOSPITALITY

1. What all DATA to be collected
2. Data- Indian & Foreigner
3. Data- co-travellers
4. Review of current systems- CCTV
5. Sharing of DATA with third party for processing

6. COMMON – issue compliance with the LAW

eCommerce Companies

1. What all DATA to be collected
2. Data- Indian & Foreigner
3. Handling Sensitive Data
4. Consent compliance
5. Compliance with cross-obligations

5. COMMON – issue compliance with the LAW

BANKING COMPANIES

1. What all DATA to be collected
2. Data- Indian & Foreigner
3. Handling Sensitive Data
4. Consent compliance
5. Handling Purpose limitation
6. Compliance with cross-obligations- RBI / Bkg. Regulation

5. COMMON – issue compliance with the LAW

Questions ?

THANK YOU