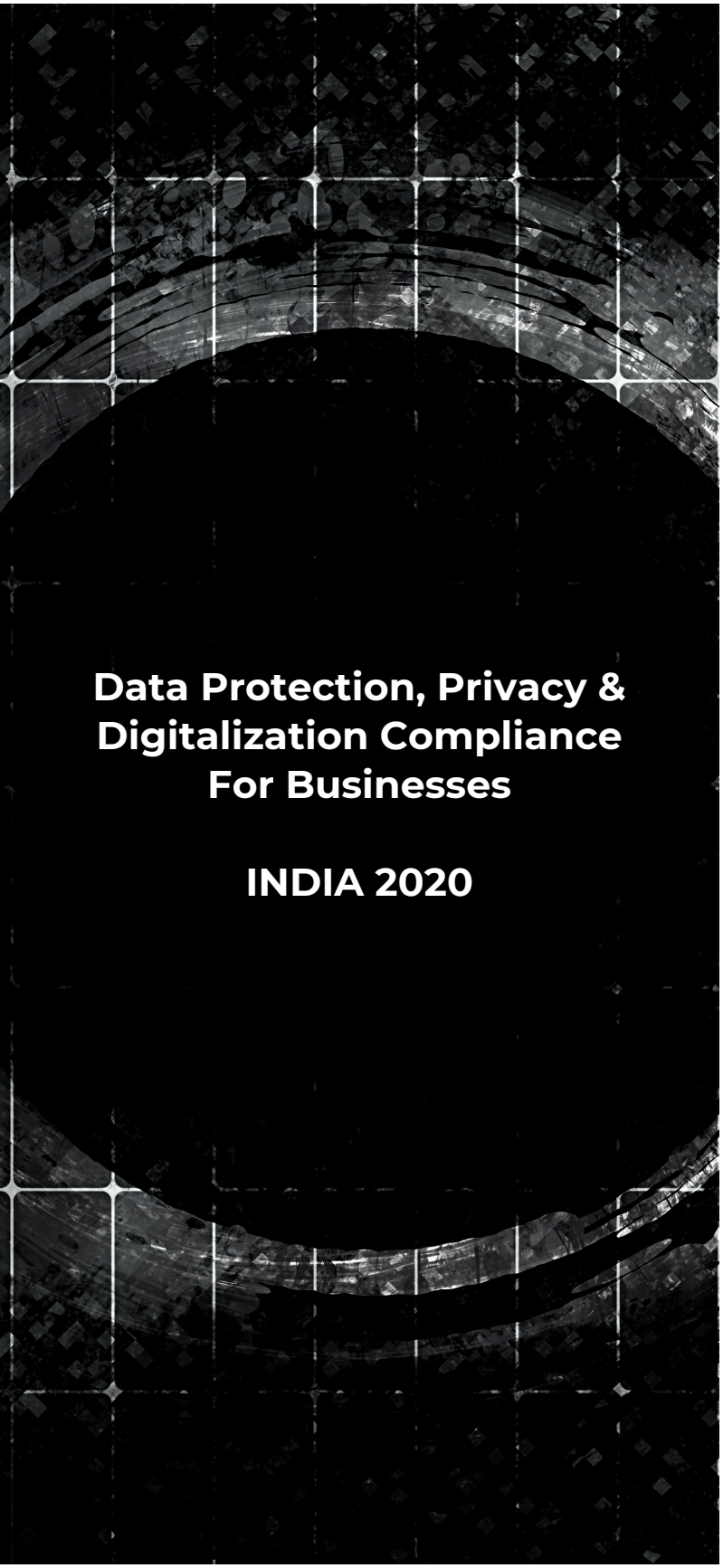
# Data Protection, Privacy & Digitalization Compliance For Businesses - INDIA 2020

## An Outline on Data Protection Regime in India

HAMMURABI & SOLOMON PARTNERS

New Delhi | Gurugram | Mumbai | Bengaluru | Ranchi | Patna
https://www.hammurabisolomon.in/

# CONTENTS



# CHAPTER 1: SCOPE OF APPLICATION OF LAW

## I. Territorial Scope of Application of Law

### GDPR

I. Organizations having an establishment in the European Union and processing personal data "in the context of" the said European Union establishment.

II. Organizations not established in the European Union but processing personal data related to:

- Goods/services in European Union; or
- Monitoring behaviour of individuals in European Union.

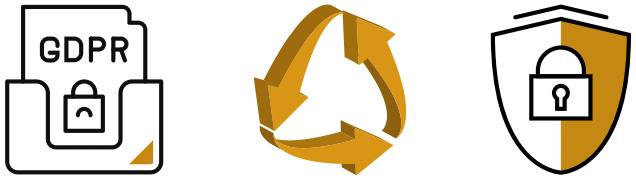
### PRESENT INDIAN LAW

I. Body corporates that are related to the collection, disclosure, and transfer of personal information and sensitive personal data.
Body Corporate (Definition):

- any company
- a firm
- sole proprietorship
- other association of individuals engaged in commercial or professional activities;

II. However, the scope of the present Indian law (comprising the Information Technology Act, 2000 and the Rules thereunder) is limited as it only applies to data processing operations of individuals located in India.

The obligations under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("IT Rules, 2011") are limited in application as they apply only to body corporates collecting personal data from individuals for providing services to the said individuals.




III. Clarification on the Privacy Rules, issued by the former Ministry of Communications and Information in 2011:

EXCLUDES: Indian outsourcing service providers who provide services related to personal information for:

1. collection,
2. storage or
3. handling
4. If they are under contractual obligation with any legal entity located within or outside India.

### PERSONAL DATA PROTECTION BILL (PDP BILL)

I. Processing personal data collected, disclosed, shared or otherwise processed within the territory of India

II. Indian companies, Indian citizens, and any other persons or bodies incorporated or created under Indian law.

III. Organizations that are not present in India, but have a nexus with

1. businesses in India
2. any systemic offering of goods/services to individuals in India;
3. activities involving profiling of individuals in India

## II. Material Scope of Appliacation of Law

### GDPR

1. Personal data — anonymous data is out of the scope of GDPR
2. Automated processing or non-automated processing where a filing system comprises personal data.

EXCLUDING:

- Processing of Personal Data by natural persons for: (a) purely personal or (b) household purposes.
- Data Processing by law enforcement agencies and national security agencies.

### PRESENT INDIAN LAW

The obligations under the IT Rules 2011 only apply to companies collecting data from individuals, for the purpose of directly providing a service to that individual.

Sector and industry specific laws prescribe confidentiality of data, such as: telecommunications, healthcare, banking and financial services.

### PDP BILL

**Personal Data** (including Sensitive Personal Data and Critical Data)

1. Anonymous data is out of the scope of PDP Bill.
2. Exception: the Central Government is empowered to direct disclosure of "anonymized" personal and "non-personal data."

EXCLUDING:

1. Processing of Personal Data by natural persons for:
   - purely personal.
   - household purposes.
   - journalistic purposes (as per the concerned code of ethics)

   Data security principles will however apply to data processing by natural persons.
2. Law enforcement agencies and national security agencies.
3. Courts and Tribunals (in exercise of judicial functions).
4. Crime prevention, investigations and prosecutions of offenses or for violation of laws.

The scope of application of PDP Bill (which is subject of Government Regulations) exceeds that of GDPR by virtue of an entity being subjected to the same by the nexus of processing personal data in India.

# CHAPTER 2:
# KEY LEGAL DEFINITIONS

| Definition | GDPR | Present Indian Law | PDP Bill 2019 | Observations/ Remarks |
|---|---|---|---|---|
| 1. Personal Data | Art. 4(1) "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" | Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011<br><br>Rule 2(i) ""Personal information" means any information that relates to a 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." | Section 3 (11) "data" includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means;<br><br>Section 3(28) "personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling; | The definition of personal data under the GDPR is tied to identification of the concerned individual, however the definition of personal data under the PDP Bill is much wider<br><br>PDP Bill is subject to interpretations as may be expressly encompassed by the scope of the definition of personal data.<br><br>On the other hand, the interpretations of Personal Data under the GDPR seem restricted to the identification of the concerned individual; thereby restricting the scope of most interpretations.<br><br>In terms of anonymised data the PDP Bill empowers the Data Protection Authority to define the anonymisation processes from time to time (as per the advances in technology) and the same effectively excludes such data from its ambit. |

| Definition | GDPR | Present Indian Law | PDP Bill 2019 | Observations/ Remarks |
|---|---|---|---|---|
| 2. Sensitive Personal Data | Article 9(1) Processing of Special Categories of Personal Data<br><br>“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 […]” | Rule 3, IT Rules 2011 Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules. | "sensitive personal data" means such personal data, which may reveal, may relate to, or may constitute— (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15. Explanation.— For the purposes of this clause, the expressions,— (a) "intersex status" means the condition of a data principal who is— (i) a combination of female or male; (ii) neither wholly female nor wholly male; or (iii) neither female nor male; (b) "transgender status" means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure; | The definitions of sensitive personal data in GDPR and the PDP Bill are similar in terms of the elements comprising such data. However, the inclusion of “financial data” within the definition of sensitive personal data in the PDP Bill significantly broadens the same.<br><br>Additionally, the PDP Bill empowers the Government to define further types of sensitive data, unlike the GDPR.<br><br>Another elemental difference is in respect of GDPR uniquely providing for rules pertaining to processing of data of criminal convictions and offenses, unlike the PDP Bill. |

| Definition | GDPR | Present Indian Law | PDP Bill 2019 | Observations/ Remarks |
|---|---|---|---|---|
| 3. Controller | Controller:<br>The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. | NA | 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. | Although the definition under the PDP Bill uses the term "fiduciary" the Bill does not specifically identify any specific obligations arising out of such a legal relationship. |
| 4. Processor | A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller | NA | Any person, including the state, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary | The definitions are identical in nature. |
| 5. Data Subject | An identified or identifiable natural person | NA | Data principal: The natural person to whom the personal data relates. | The definitions are identical in nature. |
| 6. Processing | Article 4(2)<br>'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection,recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; | NA | Article 3(41)<br>"processing" in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction; | The only elemental difference in the definitions concerns the usage of the word "consultation" in GDPR. |

| Definition | GDPR | Present Indian Law | PDP Bill 2019 | Observations/ Remarks |
|---|---|---|---|---|
| 7.Pseudonymisation/De-identification[1] | 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;<br><br>Anonymisation: "personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." | NA | "de-identification" means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal;<br><br>Anonymisation: "anonymisation" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority; | The PDP Bill does not define pseudonymisation, leave alone mention it.<br><br>The Bill however identifies the de-identification of data which can be achieved by pseudonymisation and other such technological means and leaves it upon the Data Protection Authority to identify such methods from time to time to keep pace with the advent of technology.<br><br>Interestingly, however the Bill defines Anonymisation, and it even specifies that except for as may be prescribed by the government in consultation with the Data Protection Authority, the anonymised data will be exempt from the scope of application of the PDP Bill. |

[1] See the 2018 "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians" (Justice BN Sri Krishna Committee Report), available at: https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

" A slightly different approach may be adopted with respect to de-identification, pseudonymisation and anonymisation. It must be acknowledged that there is no consensus on the meanings of these terms and commenters have noted that policy makers and on occasion, legislators have been imprecise in their use of these terms.97 Polonetsky et al bring about a measure of clarity to these terms by analysing a spectrum of identifiability that has data that is obviously personal on one end and anonymised data on the other.98 Pseudonymised data and de-identified data are inflection points on the spectrum nearer to anonymisation. Anonymisation requires the use of mathematical and technical methods to distort data to irreversibly ensure that identification is not possible. In this aspect, anonymisation is distinct from de-identification which involves the masking or removal of identifiers from data sets to make identification more difficult. Given the pace of technological advancement, it is desirable not to precisely define or prescribe standards which anonymisation must meet in the law. It is appropriate to leave it to the DPA to specify standards for anonymisation and data sets that meet these standards need not be governed by the law because they cease to be personal data."

| Definition | GDPR | Present Indian Law | PDP Bill 2019 | Observations/ Remarks |
|---|---|---|---|---|
| 8. Consent | 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; | Indian Contract Act, 1872<br><br>14. 'Free consent' defined.—Consent is said to be free when it is not caused by— — Consent is said to be free when it is not caused by—"<br>1. coercion, as defined in section 15, or<br>2. undue influence, as defined in section 16, or<br>3. fraud, as defined in section 17, or<br>4.misrepresentation, as defined in section 18, or<br>5.mistake, subject to the provisions of sections 20, 21 and 22. Consent is said to be so caused when it would not have been given but for the existence of such coercion, undue influence, fraud, misrepresentation or mistake. | Section 11(2) The consent of the data principal shall not be valid, unless such consent is— (a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872; (b) informed, having regard to whether the data principal has been provided with the information required under section 7; (c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing; (d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and (e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given. | By virtue of incorporating reference to free consent under the Indian Contract Act, 1872, the PDP Bill offers a much more stringent definition of consent as compared to the GDPR. |

# CHAPTER 3: GROUNDS FOR PROCESSING OF PERSONAL DATA

## GDPR

a. CONSENT: Under the GDPR, consent is one of six lawful bases for processing personal data.

1. The GDPR defines consent as, “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."
2. The definition of consent under the GDPR is a continuing one, which requires the controller to manage and update the same from time-to-time as the data cycle develops, giving rise to the requirement of seeking consent for the actions and purposes from the data subject at varying points. The exclusion of the opt-out mode of obtaining consent is critical to the functional aspects of GDPR.

b. NON-CONSENSUAL: The other five lawful bases for processing set out in Article 6(1) GDPR are:

1. Contract: When the purpose of processing data arises from a contractual obligation on part of the controller to fulfil its contractual obligations towards the data subject.
2. Legal obligation: When processing is mandated by virtue of legal obligation emanating from EU or member state law.
3. Vital interests: When processing is essential for safeguarding the vital interests.
4. Public task: When processing is necessary for performing a task in public interest or while exercising state functions by virtue of the authority as may be vested in the data controller.
5. Legitimate interests: When processing of data is necessitated for the legitimate interests of the controller/third party. The exception to the same being that the rights of the data subject interests take precedence over the legitimate interests. Processing data in legitimate interests is not a ground available to state/official authorities.


c. SENSITIVE DATA PROCESSING:
GDPR employs a negative permission to sensitive data processing by specifying that unless the sensitive data is processed on a lawful basis derived from the below grounds, the same is prohibited. The lawful bases identified under Article 9, GDPR are as below:

1. Explicit Consent
2. Employment or social security and social protection law
3. Vital interests
4. Foundation, association or not-for-profit
5. Public Data (Data available publicly)
6. Legal Claims
7. Public Interest
8. Healthcare
9. Public health (element of Public Interest)
10. Archiving, Research or Statistical Purposes in Public Interest

## PRESENT INDIAN LAW

a. Lawful basis for processing Personal Information:

1. Presently Indian Law does not mandate obtaining consent to collect data, or for disclosing the same to a third party.
2. The law mandates there being a privacy policy and the same must specify the data that is sought to be collected and the purpose thereof.

b. Lawful basis for processing Sensitive Personal Data:

1. Consent; defined as "in writing, through letter or Fax or email"; and
2. Disclosing the following information at the time of sensitive data collection:
   - The fact that the data is being collected
   - Purpose of data collection
   - Intended recipients of data
   - Name and address of the collecting agency and retaining agency

c. Notably, the present Indian Law on data protections does not apply to:

1. Personal information or data stored in a non-electronic format
2. Freely available information which is accessible in public domain.
3. Information furnished under a law which in force at the time of collection.

d. Purpose:

1. The information is restricted from being used for any purpose other than the one for which it is collected and upon exhaustion of the purpose the information ought not to be retained, unless the requirement emanates from legal obligations.
2. Sensitive personal data can be collected only if necessary for the lawful purpose associated with the activities of a body corporate.

## PDP BILL

a. The PDP Bill exhibits much more stringency with regard to grounds
for data processing.

b. PDP Bill prescribes separate standards of consent for personal data
and sensitive personal data

c. Personal data can only be processed, on the following basis:

1. Consent
2. State Functions, with emphasis on:
   - the entity performing the function,
   - the nature of the function,
   - the extent of processing of data.
3. Legal Compliance: Legal obligations can range from:
   - Complying with the requirements outlined in law; or
   - Complying with court or tribunal orders. These grounds essentially ensure that the legal process is not hindered by the data protections laws.
4. Prompt Action, such as emergencies arising out of health and safety conditions, where only ex-post consent can be obtained.
5. Employment; such as for recruitment purposes or during the course of employment for necessary functions such as disbursal of remuneration, or disciplinary actions, attendance, and medical records.
6. Reasonable Purposes; such as for prevention and detection of unlawful activities.

# CHAPTER 4:
# KEY OBLIGATIONS OF DATA CONTROLLERS/DATA FIDUCIARIES


## GDPR – OBLIGATIONS OF DATA CONTROLLERS

### I. PROCESSING OBLIGATIONS

**Article 5 read with Recital 39 of GDPR- Principles of Personal Data:**

1. LAWFULNESS, FAIRNESS, TRANSPARENCY:
   - Information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
   - Where personal data is collected directly from the individual, notice must be provided at or before the time of collection.
   - For personal data collected indirectly notice must be provided within one month (or upon first contact with the individual, if earlier), unless providing notice would be impossible or would require disproportionate effort. The notice must necessarily provide information such as purpose and parties with whom the data will be shared, and consent must be explicitly sought for sharing the data with cross-border parties.
   - Controllers and processors, subject to GDPR, but not established in the European Union are required to appoint a representative in the European Union. Exception: when processing is rare and occasional and not involving large scale processing of sensitive data.
2. **Collected for specified, explicit and legitimate purposes ('Purpose Limitation').**
3. **Adequate, relevant, limited ('Data Minimization')**
4. **Accurate -** Data is required to be maintained in an accurate and up to date manner and it is required to be erased or rectified without any delay.
5. Storage Limitation
   - Data ought not to be stored in a way that allows the data subject to be identified after for purpose of processing is satisfied.
   - EXCEPTION: Data storage for longer periods can be allowed only when processed in public interest, scientific research, historical research or statistical purposes.
   - Proper technical and organizational measures are essential to safeguard rights of Data Subjects.
6. Integrity and Confidentiality
   - Ensuring security of data through manner of processing.
   - Unlawful processing, accidental losses, and destruction or damage of data needs to be prevented.
7. Accountability of the Controller
   - Controller ought to comply with all of the above.

### II. DATA PROTECTION OFFICERS

1. Required for private entities only where a "core activity" of the controller or processor involves either
   - the regular and systematic monitoring of data subjects on a large scale; or
   - the large-scale processing of sensitive data.
2. The Data Protection Officer must be sufficiently independent and functionally skilled and must be able to report to the highest levels of management.
3. Data Protection Officers can be outsourced.
4. Data Protection Officers should be EU-based.

III. RECORD OF PROCESSING: Controllers and processors are obliged to retain records of processing activities.

Article 30: All Data Controllers and Processors are responsible for the maintenance of the record of processing activities in written form including electronic form, containing information of:

1. Details of the Controller/Processor
2. Purpose of Processing
3. Description of Categories of Personal Data and of Data Subjects
4. Categories of Recipient
5. Transmission of third country / international organization, if applicable
6. Time limit for erasure of data
7. Description of general and organizational security measures.

Exception – obligation mentioned above shall not apply to the enterprises or an organization employing fewer than 250 persons unless the intended processing is likely to result in a risk to the rights and freedoms of the data subject.

## Application of Law to Data Processors Under GDPR

1. Processors and controllers, both, are obligated to maintain records of personal data and processing activities.
2. Data Controllers are obligated to ensure that the Processor is GDPR compliant and responsibly ensures security of the data.
3. Obligations of the controller while electing the Processor are as below:
   - Choose a data processor that provides "sufficient guarantees" about its security measures;
   - Execute a contract obliging the processor, among other obligations, to undertake to implement the same security measures that the controller would have taken for data processing;
   - Ensure that the processor shares all requisite information to enable the controller to ensure compliance, including convening of audits and inspections;
4. In case the Controller lacks the ability to ensure implementation of requisite measures the Processors can help the Controller ensure compliance with security obligations pertaining to data processing.

## PRESENT INDIAN LAW

I. REASONABLE SECURITY: Any "body corporate" handling sensitive personal data is obligated to implement "reasonable security practices and procedures" with respect to sensitive personal data commensurate with protecting the information assets.

II. INTERNATIONAL STANDARD REQUIREMENTS: Such requirements can be agreed upon by the parties, or in absence thereof, the Rules recommend employing International Standards or a code established by trade associations and approved by the Central Government.

III. DATA BREACH: Upon the occurrence of a data breach the body corporate may be called upon to demonstrate that the standards have been followed.

# PDP BILL – OBLIGATIONS OF DATA FIDUCIARIES

## I. KEY PRINCIPLES

### i. Processing Obligations Clauses 4-10 of PDP Bill - deals with the Principles of Data Protection, which are similar to the principles under GDPR.

1. Personal data may not be processed by any person "except for any specific, clear and lawful purpose".
2. Personal data must be processed "in a fair and reasonable manner and ensure the privacy of the data principal."
3. Personal data must be processed "for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected".
4. Personal data must be "collected only to the extent that is necessary for the purposes of processing of such personal data."
5. Data Fiduciaries are obligated to "take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed," taking into account whether:
   a. the data is likely to be used to make a decision about the data principal;
   b. the data is likely to be disclosed; or
   c. the data is kept in a form that distinguishes facts from opinions or personal assessments.
6. Data fiduciaries are "responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf."

### ii. Purpose Limitation and Data Minimisation

1. Data Fiduciaries may "not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing" in the manner as may be specified under regulations, unless the data principal explicitly consents or so is required by law.
2. Data Fiduciaries are obligated to "undertake periodic review to determine whether it is necessary to retain the personal data in its possession."

### iii. Transparency

1. Notices must be clear, concise and easily comprehensible to a reasonable person.
2. There is a requirement to translate notices to multiple languages where necessary and practicable.
3. Notice must be provided at the time of collection, or, if not collected directly from the individual, as soon as reasonably practicable, unless providing notice would "substantially prejudice the purpose of processing."
4. Detailed requirements for the contents of notices, including:
   - Detailed disclosures of the "individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared."
   - The procedure for redressing grievances (in addition to responding to rights requests).
   - Any rating of data trust score assigned to the data fiduciary.
   - Any other information specified by regulations.

## II. DATA PROTECTION (SECURITY)

a. Encryption – Precautionary Data Protection and post-facto Legal Protection

**i. General Perceptions:**

- The process of protecting data through encryption is an accepted method of data protection.
- Encryption Policies add value to compliance with data protection laws
- The requisite level of encryption is directly proportional to the sensitivity of the data.

**ii. Safeguard against Liability in the event of Data Breach**

- Encryption prevents data stealth from qualifying as a data breach.
- Encryption safeguards organizations from liabilities arising from instances of data breach
- Encryption plays a key in reporting compliances to Data Protection Authorities.

**iii. Encryption in Indian law and Jurisprudence:**

- It is noteworthy, that the Hon'ble Supreme Court of India in the landmark judgment of Justice K. Puttaswamy v. Union of India, while deciding upon the vires of Aadhar, the Indian social security equivalent, determined that encryption was key to determining that the Central Identities Data Repository was not a soft target.
- The Supreme Court of India even noted in Justice K. Puttaswamy v. Union of India that end to end encryption qualifies as a protected system under the Indian Information Technology law; and even when the data is lost or stolen it need not result in a breach provided the same remains inaccessible.

b. Privacy by Design (PBD)

**i. Technological designs resulting in protection of privacy include:**

- Implementation of Technical and Organisational Measures, such as pseudonymisation.
- Data minimization.
- Processing only essential data.
- Period of storage.
- Restricted accessibility.

**ii. Benefits:** PBD ensures cost-effective protection for personal data and ensures higher quality of data for business functions.

**iii. Developments in Indian laws:**

- PDP Bill mandates PBD as part of transparency and accountability measures. Each organisation that collects data is required to prepare a Privacy by Design Policy.
- The PDP Bill also states that an organisation "may submit its privacy by design policy to [the proposed Data Protection] Authority for certification within such period and in such manner as may be specified by regulations", after which the policy would be "published on the website of the [organisation] and the Authority".

c. Security Safeguards - The PDP Bill identifies the obligation of Data Fiduciary and Data Processor to implement Security Safeguards having regard to: (i) nature, (ii) scope; and (iii) purpose of processing personal data undertaken, AND (iv) the risks associated with such processing, and (v) the likelihood and severity of the harm that may result from such processing.

The Bill further prescribes:

- use of methods such as de-identification and encryption
- steps necessary to protect the integrity of personal data;
- steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

d. Periodical Review

Data Fiduciaries and Data Processors shall review security safeguards periodically.

e. Registration Obligations

1. "Significant data fiduciaries" are required to register with the Data Protection Authority in accordance with procedures that will be set out in regulations (S. 26(2)).

2. The DPA is required to notify data fiduciaries or classes of data fiduciaries as significant taking into account the following factors:

- The volume and sensitivity of data processed.
- Company revenue.
- Risk of harm.
- Use of new technologies

### f. Record of Processing Activities

Significant data fiduciaries shall maintain accurate and updated records of:

- Important operations in the date life-cycle collection, transfers and erasure of personal data
- Periodic review of security safeguards
- DPIA
- Any other aspect of processing.
  *The above also apply to the state.*

The Record of Processing obligations under PDP Bill are more relaxed in comparison with GDPR and are likely to apply to a fewer companies that are subject PDP Bill.

## Application of law to Data Processors under PDP BILL

Section 24. (1) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including—

- 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.

(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.

Section 31. (1) The data fiduciary shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor.

(2) The data processor referred to in sub-section (1) shall not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorisation of the data fiduciary and unless permitted in the contract referred to in sub-section(1).

(3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary and treat it confidential.

The PDP Bill prescribes much more specific storage limitations than GDPR:

1. Unlike GDPR, which allows data retention in a form that no longer identifies an individual, the PDP Bill mandates data deletion.
2. The PDP Bill mandates data fiduciaries to conduct periodic reviews of personal data retention.

## DATA PROTECTION IMPACT ASSESSMENT

### GDPR

1. The GDPR requires controllers to conduct a Data Protection Impact Assessment for "high risk" activities, including
   - Systematic and extensive profiling;
   - Large scale sensitive data processing; and
   - Large scale systematic monitoring of a publicly accessible area.
2. The controller must consult with the Data Protection Authority before engaging in the processing where high risks are mitigated.
3. EXCEPTIONS:
   - Where the relevant Union law or member state law prescribes a legal basis.
   - Where sectoral/specific laws regulate specific processing operations or set of operations.
   - Data Protection Impact Assessment forms part of a general impact assessment.

### PRESENT INDIAN LAW:

No such express law under the existing laws in India.

### PDP BILL

DPIA provisions apply to significant data fiduciaries only, where processing involves:

- new technologies;
- large-scale profiling or use of sensitive data; or
- any other activities that carry a significant risk of harm as may be specified by regulations.

All Data Protection Impact Assessments must be submitted to the Data Protection Authority for review, and the Data Protection Authority may direct the data fiduciary to cease processing.

COMMENT: Unlike under the GDPR, the PDP Bill mandates all Data Protection Impact Assessments to be reviewed by the Data Protection Authority.

## KEY POINTS OF DIFFERENCE BETWEEN GDPR AND PDP BILL:

1. GDPR obligates all Data Collectors to undertake Data Protection Impact Assessments and maintain records of the same. The PDP Bill, however, mandates 'Significant Data Fiduciaries' only to carry out Data Protection Impact Assessments.
2. The grounds for determining the necessity of Data Protection Impact Assessments are wider under the GDPR.
3. Details to be provided in the Data Protection Impact Assessments are narrower under PDP Bill as compared to GDPR.

## DATA PROTECTION OFFICER (DPO)

### GDPR

1. Essential Qualifications:
   - Expert knowledge of data protection law and practices
   - Knowledge of relevant regulations applicable within the field in which the controller or processor carry out activities
   - Detailed knowledge of data processing processes and technologies employed by the controller or processor

2. Tasks:
   - Data Protection Officer essentially is an extended arm of the Data Protection Authority.
   - Data Protection Impact Assessment: Consult with Data Protection authority in case of high risk.
   - Point of contact for Data Subjects

3. Challenge: Conflict of Interest:
   - The Data Protection Officer cannot have other duties conflicting with monitoring obligations of the Data Protection Officer.
   - Such conflicts of interest crop up if the Data Protection Officer is the head of other departments that process personal data.
   - Why Legal? If the legal counsel may represent the company in a legal proceeding (especially with regard to legal actions against employees or customers, which may include data privacy related aspects), the legal counsel is subject to conflict of interest and, therefore, not independent.

4. Solution: Positioning Data Protection Officer as a secondary defence mechanism
   - The primary tasks of Impact Assessments and related compliances need to be handled through an expert who is not a designated Data Protection Officer.
   - Conducting regular Internal Audits by the experts who can then guide the Data Protection Officer to the compliances to be performed.

5. Point of Contact
   - The Data Protection Officer is the point of contact for Data Subjects. However, the Data Protection Officer need not be designated with responding to or resolving concerns and complaints.
   - It is essential for experts to maintain active communication channels with Data Protection Officer and resolve and respond to Data Subjects.
   - Documenting processes through experts to demonstrate compliance and have the same accessible to the DPO will therebygive the DPO the onus to review the compliances rather than be compelled to conduct a full-fledged audit

### PRESENT INDIAN LAW

The existent Indian law does not provide for Data Protection Officers.

### PDP BILL

- The PDP Bill identifies Significant Data Fiduciaries (a subset of the Data Fiduciary, equivalent of Data Controller in GDPR) as full-fledged regulated entities required to appoint Data Protection Officers.
- The Bill even mandates offshore entities qualifying as Significant Data Fiduciaries to appoint Data Protection Officers based in India.

# CHAPTER 5: KEY RIGHTS OF DATA SUBJECTS

| Definition | GDPR | Present Indian Law | PDP Bill 2019 | Observations/ Remarks |
|---|---|---|---|---|
| 1. Right to Access | **Article 15 of GDPR**<br><br>Data Subject have the right to obtain confirmation from the controller – concerning the processing of his/her personal data.<br><br>Exceptions apply where providing information, would adversely affect the rights and freedom of others, including intellectual rights. | **Rule 4 of SPDI Rules, 2011**<br><br>Body corporate to provide policy for privacy and disclosure of information | **Clause 17 of PDP Bill**<br><br>Data Principal have the right to obtain:<br>• confirmation about the processing of his personal data<br>• a brief summary of processing activities<br>• identities of data fiduciaries with whom his personal data had been shared.<br>• category of personal data shared.<br><br>Exception (Clause 21(5)): Data fiduciary shall not entertain any such request, which may harm the personal date of any other data principal. | **Broadly similar** under GDPR and PDP Bill<br><br>Burden of identifying all the data fiduciaries with whom personal data has been shared.<br><br>The exception provided under PDP Bill – protecting other data principals may not permit withholding personal data on intellectual property grounds. |

| Definition | GDPR | Present Indian Law | PDP Bill 2019 | Observations/ Remarks |
|---|---|---|---|---|
| **2. Right to be forgotten** | **Article 17 of GDPR Right to erasure ('right to be forgotten')**<br><br>• Data subject have the right to obtain erasure of his/her personal data without undue delay and the controller shall is obliged to do so without undue delay – on the following grounds:<br>◦ Personal data no longer necessary<br>◦ Data subject withdraws consent<br>◦ Data subject objects to the processing<br>◦ Personal data processed unlawfully.<br>◦ the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject<br>◦ personal data collected in relation to offer of information security services. | **Rule 5(6)**<br><br>Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:<br><br>Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to such boy corporate or any other person acting on behalf of such body corporate. | **Clause 18 of PBP Bill – Right to correction and erasure**<br><br>• Data Principal have the right to –<br>◦ the correction of inaccurate or misleading personal data;<br>◦ the completion of incomplete personal data;<br>◦ the updating of personal data that is out-of-date;<br>◦ the erasure of personal data which is no longer necessary for the purpose of which it was processed.<br>.<br>• Data fiduciary can reject the application of data principal, giving written justification for the same. | The PDP distinguishes between two separate rights — one for erasure and one for restricting the disclosure of personal data (i.e., the right to be forgotten).<br><br>Unlike the GDPR, the PDP places responsibility for determining the scope of application of the right to be forgotten on adjudicating officers appointed by the DPA, rather than the controller.<br><br>Since, the adjudicating officer has to consider a number of contextual factors, the interpretation of the right to be forgotten will be narrower than then corresponding right provided under GDPR right. |

| Definition | GDPR | Present Indian Law | PDP Bill 2019 | Observations/ Remarks |
|---|---|---|---|---|
| | • Where controller has made personal data public, controller is obliged to:<br>◦ erase the personal data<br>◦ shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.<br>• The above stated shall not apply –<br>◦ For exercising the right of freedom of expression and information;<br>◦ For compliance with a legal obligation<br>◦ For reasons of public interest in area of public health<br>◦ In the public interest, scientific or historical research or statistical purposes<br>◦ For establishment, exercise or defense of legal claims. | Rule 5(7)<br><br>Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought. | **Clause 20 of PDP Bill - Right to Freedom**<br><br>• Data principal have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure –<br>◦ has served the purpose for which it was collected or is no longer necessary<br>◦ consent has been withdrawn<br>◦ was made contrary to the provisions of this Act or any other law for the time being in force.<br><br>• Above right to freedom can be enforced only by an order of an Adjudicating Officer – on an application filed by the Data Principal. | |

| Definition | GDPR | Present Indian Law | PDP Bill 2019 | Observations/ Remarks |
|---|---|---|---|---|
| **2. Right to be informed** | **Article 12** Transparent information, communication and modalities<br><br>Article 13 Information to be provided where personal data are collected from the data subject<br><br>Article 14 Information to be provided where personal data are collected from the data subject | Rule 6 of SPDI Rules<br><br>Disclosure of information | Clause 7 read with Clause 11(b)<br><br>Requirement of notice for collection or processing of personal data. | There is significant overlap between the transparency requirements of both frameworks.<br><br>However, the PDPB does include additional disclosure requirements that may not already be included in a privacy notice drafted for GDPR, such as details on the procedure for handling individual requests and grievances, and, if applicable, a data trust score assigned by a data auditor pursuant to the PDPB's audit provisions (discussed below).<br><br>In addition, requirements to provide the contact details of the data protection officer, and to provide notice in multiple languages, may require the localization of global privacy notices.<br><br>Finally, the requirements for disclosing recipients under the PDPB may require more specific disclosures of data processors than is required under the GDPR. |

# CHAPTER 6: CROSS-BORDER DATA TRANSFERS AND DATA LOCALIZATION

## GDPR

Localization is not required unless international data transfer requirements are not met.

## PRESENT INDIAN LAW

*Rule 7 of IT Rules 2011 - Transfer of information*

"A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules.

The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

## PDP BILL

CHAPTER VII RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA

Section 33. Prohibition of processing of sensitive personal data and critical personal data outside India.

1. Subject to the conditions in sub-section (1) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India.
2. The critical personal data shall only be processed in India.

   Explanation.—For the purposes of sub-section (2), the expression "critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data

Section 34. Conditions for transfer of sensitive personal data and critical personal data.

1. The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where—
   a. the transfer is made pursuant to a contract or intra-group scheme approved by the Authority: Provided that such contract or intra-group scheme shall not be approved, unless it makes the provisions for—
      i. effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and
      ii. liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; or
   b. the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organisation on the basis of its finding that—
      i. such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and
      ii. such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction: Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed;
   c. The Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.

2. Notwithstanding anything contained in sub-section (2) of section 33, any critical personal data may be transferred outside India, only where such transfer is—
   a. to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action under section 12; or
   b. to a country or, any entity or class of entity in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause (b) of sub-section (1) and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State.
3. Any transfer under clause (a) of sub-section (2) shall be notified to the Authority within such period as may be specified by regulations.

## RECOMMENDATIONS OF JUSTICE BN SRIKRISHNA COMMITTEE:

1. Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee.
2. Intra-group schemes will be applicable for cross-border transfers within group entities.
3. The Central Government may have the option to green-light transfers to certain jurisdictions in consultation with the DPA.
4. Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data). The Central Government should determine categories of sensitive personal data which are critical to the nation having regard to strategic interests and enforcement.
5. Personal data relating to health will however permitted to be transferred for reasons of prompt action or emergency. Other such personal data may additionally be transferred on the basis of Central Government approval.
6. Other types of personal data (non-critical) will be subject to the requirement to store at least one serving copy in India.

## STANDARD CONTRACTUAL CLAUSES AND INVALIDATION OF EU-U.S. PRIVACY SHIELD.

**Case No. C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems[1]**

1. **Validity of Standard Contractual Clauses**

   a. In an investigation led by the Irish Data Processing Commission it was provisionally found that the processing of personal data of citizens of the European Union by the U.S. authorities was not in conformity with Article 7 – "Respect for private and family life" and Article 8 – "Protection of personal data" of the Charter of Fundamental Rights of the European Union.
   b. The Irish Data Processing Commission also preliminarily opined that citizens of the European Union were not provided with legal remedies in conformity with Article 47 – "Right to an effective remedy and to a fair trial" of the Charter of Fundamental Rights of the European Union.

In view of the above the Court of Justice of the European Union ruled that:

   i. If the European Commission has made an adequacy decision, a Data Protection Authority cannot conclude that a jurisdiction does not offer adequate protection.
   ii. For all the other third countries where the European Commission has not made an adequacy decision a Data Protection Authority may decide that the Standard Contractual Clauses cannot be complied with and that requirements of the GDPR for the protection of the data of the Data Principal in European Union cannot be ensured by other means.

RULING: The Court of Justice of the European Union ruled that where the adequacy decision is not in place and the Data Protection Authority determines that the third-country cannot ensure adherence with GDPR and EU Law, the Data Protection Authority must suspend or prohibit the transfer, unless, the suspension has been given effect by the Data Controller or the Data Processor.

2. **Invalidity of EU-US Privacy Shield**

   a. The European Commission had acknowledged that the Privacy Shield Framework needs to be complied with to the "extent necessary to meet the national security, public interest, or law enforcement requirements."
   b. The limitations within the Privacy Shield Framework on data processing on the grounds of national security, public interest or law enforcement requirements were not in consonance with the GDPR and could allow processing of data in contravention with the GDPR and EU Law on the basis of the domestic law of the US in addition to grounds of nationals security and public interest.

RULING: The Court of Justice of the European Union ruled that Article 47 of the Charter were not honoured as Data Subjects did not have access to courts against US authorities and that the Privacy Shield Ombudsperson "cannot remedy the deficiencies" concerning judicial protection of Data Subjects, specifically on grounds of lack of independence of the Privacy Shield Ombudsperson from the US Executive as the same directly reported to the US Secretary of State. Moreover, the Privacy Shield Framework did not ensure that the Ombudsperson could issue decision binding on US intelligence services.

[1] Judgment of the Court of Justice of the European Union (Grand Chamber), 16th July 2020, Case C-311/18, titled 'Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems'. Click here to view full jugement

# ABOUT US

Hammurabi & Solomon Partners was founded in the early 2001 and is ranked amongst the top #15 law firms in India. Our journey has been marked by stellar growth and recognition over the past 2 decades with over 16 partners handpicked from the top of their fields. Paving our way into the Indian legal landscape we believe in providing complete client satisfaction with a result driven approach.

We have always aimed at being the change-maker for a newer India and the world around us. With our portfolio of services - law, public policy, regulation and justice converge to enable solutions to our client needs within the legal framework to operate in India with ease and predictability.

Our main aim is to provide world-class legal services with a unique client-centric approach. We aim at providing the utmost quality and result-oriented solutions with our out of the box thinking and teamwork. We focus on being very approachable and highly reliable legal advice with a practical and relevant approach, we tailor solutions with each client's needs.

Our firm implements a holistic approach towards client satisfaction by offering higher level of services, in-time solutions and exercising greater insights to understand the clients' sectors.

Our offices are located in New Delhi (HQ), Mumbai, Bengaluru, Gurugram, Patna & Ranchi.


**HEAD OFFICE**
405A & 405B, Rectangle One - 4th Floor
Saket District Centre, Saket
New Delhi - 110017

Visit us at
www.hammurabisolomon.in/