Comparative Guide

Data Privacy and Cybersecurity

Indonesia & India Law

Prepared by:

Nusantara Legal Partnership

S&P

SINGHANIA & PARTNERS LLP

SOLICITORS AND ADVOCATES

Indonesia

Marshall Situmorang and Audria Putri | Nusantara Legal Partnership

Data Privacy and Cybersecurity Comparative Guide

A. Definition and Scope of Data Privacy and Cybersecurity

Data Privacy

1. **Is there any specific definition of "*personal data*" in your jurisdiction? Do the prevailing laws provide distinction between personal data and sensitive personal data?**

   Personal data is defined as *"a certain personal data that is stored, maintained, kept true and its confidentiality is protected"* (Art. 1 (1) of Minister of Communications and Informatics ("**MoCI**") Regulation No. 20 of 2016 on Personal Data Protection within the Electronic System ("**MoCI Regulation 20/2016**")). However, the applicable laws and regulations on personal data protection in Indonesia do not provide any specific definition of "*sensitive personal data*" and are silent on these matters.

   Therefore, there is no clear distinction between "*personal data"* and "*sensitive personal data"*.

2. **What is the scope of "*personal data*" pursuant to the relevant laws and regulations in your jurisdiction?**

   Indonesian prevailing laws do not provide any specific scope of personal data. There are merely provisions under MoCI 20/2016 as outlined above.

   The concept of data privacy is interpreted as a part of the privacy right, which, pursuant to Law No. 11 of 2008 as amended by Law No. 19 of 2016 ("**EIT Law**"), is defined as:

   a. the right to enjoy a private life and be free from all kinds of disturbances;
   b. the right to communicate with other persons (without being spied on);
   c. the right to supervise the access to information on his/her personal life and data (Elucidation of Art. 26 (1) of EIT Law).

   In addition to the above, Personal Data Protection Bill **("PDP Bill")** sets out a more specific scope of personal data:

(i) General personal data consists of a person's full name, gender, citizenship, religion, and/or combined personal data to identify a person;
(ii) Specific personal data, which consists of, among other things, information on a person's health, biometric data, political view, etc. (Art. 3 (1), (2), and (3) of PDP Bill).

However, PDP Bill has not been enacted up to the publication of this comparative guide.

3. **Who are the relevant stakeholders (i.e., data processor, controller, etc.) under the data protection regime in your jurisdiction?**

Stakeholders of data protection under the Indonesian prevailing laws include: (i) personal data user; and (ii) Electronic System Operator **("ESO")**, each of which has different obligations. Please note that the current prevailing laws and regulations for personal data protection do not specifically stipulate data processor and data controller, but merely the party collecting and processing personal data and the relevant data subject. PDP Bill, however, provides specific definitions of data processor and data controller.

With regard to ESOs, Art. 2 of Government Regulation **("GR")** No. 71 of 2019 on Administration of Electronic Transactions and Systems **("GR 71/2019")** stipulates two categories of ESOs, namely (i) public ESO and, (ii) private ESO.

Public ESOs include state administrator agencies and other agencies as formed by virtue of laws and/or appointed by the relevant agencies. Meanwhile, private ESOs include individuals, business entities, and the public that run portals, websites, or online applications on the internet, regulated or supervised by the Minister of Communication and Informatics, and/or the institutions based on the relevant regulations.

Cybersecurity

4. **Is there any specific definition of "*cybersecurity*" in your jurisdiction? Do the prevailing laws provide distinction between "*data protection*" and "*cybersecurity*"?**

Cybersecurity in Indonesia is governed by EIT Law and GR 71/2019, but they provide no specific definitions or terms on cybersecurity itself. A bill on cybersecurity was once proposed, but it was eventually rejected and failed to be enacted in 2019.

Based on EIT Law and GR 71/2019, the general concept of cybersecurity provisions focuses on cyber incidents including prohibitions of hacking, denial of service, phishing and identity theft, as well as cybercrimes.

5. **What are the subjects of cybersecurity? Does cybersecurity apply to certain industries and types of information?**

The government has established an institution that oversees cybersecurity and encryption namely, the National Cyber and Crypto Agency/ *Badan Siber dan Sandi Negara* **("BSSN")**, which functions include but not limited to identification, detection, protection, monitoring of the implementation of technical policies regarding cybersecurity in e-commerce protection, cyber-attacks, and/or cyber incidents in Indonesia.

In addition to the above, the government stipulates protection over certain strategic information of these sectors: (i) Government Administration; (ii) Energy and Mineral Resources; (iii) Transportation; (iv) Finance; (v) Health; (vi) Information and Communication Technology; (vii) Food; (viii) Defense; and (ix) other sectors as determined by the President.

B. Governing Authority of Data Privacy and Cybersecurity

Data Privacy

6. **Is there any specific government agency that oversees data privacy legislation in your jurisdiction? Please define what powers and authorities such agency has in the data privacy enforcement?**

Indonesia has **no** specific government agency or independent body overseeing the data privacy legislation given that neither data privacy nor cyber security bills have been passed. Considering data privacy provisions within the scope of EIT Law and MoCI 20/2016, the enforcement of data privacy is supervised by (i) MoCI and several sector-specific authorities, (ii) BSSN; and (iii) an agency under BSSN i.e., Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center (Id-SIRTII).

MoCI, the main supervisory body, can be supported by Indonesian police in the enforcement of data privacy protection. There are also sector-specific authorities that supervise data protection along with MoCI, e.g., Central Bank of Indonesia for data protection in the banking sector, and the Ministry of Health in the health sector.

BSSN's duty, function, and authority are not limited to data privacy enforcement. They cover a broader scope overseeing the overall matters under EIT Law, including cybersecurity. BSSN carries out the government's duties in the field of cyber and crypto security, focusing on cyber resilience, and resistance against possible attacks by crime organizations on the national level, and those with private interests.

Furthermore, the duty and function of Id-SIRTII mainly focus on supporting the internet growth in Indonesia through various awareness campaigns on securing the technology and information systems, monitoring the potential security incidents, supporting the law enforcement, and providing the relevant technical supports in the interests of the general public.

7. **Can the data protection authority in your jurisdiction cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?**

   MoCI 20/2016 stipulates that MoCI may coordinate with the sectoral supervision and regulatory body to (i) address complaints of data subjects for breaches of personal data protection committed by ESOs; and (ii) impose administrative sanctions for such breaches. MoCI further delegates the authority for the supervision and dispute settlement to the Directorate General of Informatics Application/ *Direktorat Jendral Aplikasi Informatika* (**"Ditjen Aptika"**).

   In this regard, MoCI and BSSN may work with other relevant authorities, for instance, Indonesian police and the intelligence service agencies (**i.e.,** the State Intelligence Agency/ *Badan Intelejen Negara* **(BIN)** and the Strategic Intelligence Agency/ *Badan Intelejen Strategis* **(BAIS))**.

Cybersecurity

8. **Is there any specific government agency that oversees cybersecurity legislation in your jurisdiction? Please define what powers and authorities such agency has in the cybersecurity enforcement?**

   Cybersecurity in Indonesia is supervised by MoCI, BSSN, and Id-SIRTII.

9. **How does the cybersecurity authority cooperate with Data Protection Office ("DPO")? Does your jurisdiction provide certain guidelines for this matter?**

   Indonesia has yet to establish a specific, independent office in-charge of Data Protection. However, MoCI Regulation 20/2016 requires the appointment of a person-in-charge that can be contacted by the relevant personal data owners regarding the management of their personal data.

   Although appointing a DPO is not a requirement, please note that Art. 45 of PDP Bill obliges any data controller or processor to appoint a DPO. This obligation applies to any data controller or processor: (i) who works on data processing to provide public services, (ii) whose main activity requires large-scale, frequent, and systematic monitoring of personal data; and (iii) whose core activity includes processing specific personal data in a large scale, and/or processing personal data related to criminal activity.

C. Regulatory Framework and Registration

Data Privacy

10. **What are the applicable laws and regulations that govern data privacy and personal data protection in your jurisdiction? Please identify further laws on data protection in specific sectors, if any.**

    Data privacy and personal data protections are governed under the following laws and regulations:

    a. EIT Law;
    b. GR 71/2019;
    c. GR No. 80 of 2019 regarding Trading through Electronic System; and
    d. MoCI Regulation 20/2016.

    MoCI Regulation 20/2016 also stipulates that a data owner reserves the right to file a lawsuit for a breach of his/her personal data, in accordance with Art. 1365 of Indonesia's Civil Code/ *Kitab Undang-Undang Hukum Perdata* regulating that any person violating the law is liable for any losses caused by his/her action. The enforcement of data protection refers to Indonesia's Criminal Code/ *Kitab Undang-Undang Hukum Pidana* for the criminal sanction.

    Other relevant sectors also governing the legislation on data privacy and personal data which include the banking, health, and capital market sectors under:

    a. Law No. 36 of 1999 on Telecommunications as amended by Law No. 11 of 2020 on Job Creation;
    b. Law No. 10 of 1992 on Banking as amended by Law No. 10 of 1998;
    c. Law No. 8 of 1995 on Capital Market;
    d. Law No. 36 of 2009 on Health; and
    e. Law No. 14 of 2008 on Disclosure of Public Information.

11. **Are there any exemptions under the data privacy and personal data protection rules in your jurisdiction?**

    The prevailing laws and regulations do **not** provide any exemption with respect to the mandatory registration of ESO.

12. **Do the data privacy applicable laws and regulations apply extraterritorially? If yes, how do DPO and the government exercise such duties?**

Yes. Art. 2 of EIT Law explicitly states that it applies extraterritorially, including to foreign legal subjects regardless of their presence in Indonesia. Therefore, any legal action regarding data protection carried out outside the jurisdiction of Indonesia by Indonesian citizens or legal entities, or foreign citizens or legal entities that have legal consequences in Indonesia shall be subject to EIT Law. Furthermore, Article 50 of PDP Bill also provides that the Indonesian PDP laws shall be applicable to any breach of personal data protection occurring domestically or abroad.

The provision was built on the concept where the misuse of information technology for electronic information and transactions might, in the future, threaten and harm the interests of Indonesia, which might be detrimental to the nation's (i) economic interests, (ii) protection of strategic data, (iii) dignity, (iv) defense and state security, (v) sovereignty, citizens, and (vi) legal entities. Given the authority over DPO has yet to be established, MoCI shall be the authority that oversees and responsible for coordinating with the ESOs in cross-border, personal data transmissions.

13. **Is the registration of data controllers and processors mandatory in your jurisdiction? If <u>yes</u>, how is the registration procedure completed, and what are the consequences for failing to conduct the registration?**

In general, Indonesia's prevailing regulations do not specifically distinguish a data controller from a data processor. Both are recognized as ESOs. Pursuant to GR 71/2019, any public or private ESO, located onshore or offshore, is obliged to conduct ESO registration to MoCI **("ESO Registration")** through the OSS system prior to conducting any business activity.

The required documents for ESO Registration are (i) registration form including the corporate documents, tax identification number of the company, contact person; and (ii) supplemental documents i.e., general information regarding the electronic system including the system's profile, URL website, IP address, descriptions on the system's functions and business process, and the ESO's statement of willingness to conduct the personal data protection.

Failure to comply with the mandatory ESO registration will be subject to administrative sanctions in the form of warning letters, administrative fine, temporary suspension, access termination, and/or removal from MoCI's list.

Cybersecurity

14. **Is there any specific laws and regulations that govern cybersecurity for data privacy and personal data in your jurisdiction?**

As outlined in Points 4 and 5 above, Indonesia has no specific regulation on cybersecurity for data privacy and personal data. But EIT Law, GR 71/2019, and MoCI Regulation 20/2016 stipulate general provisions on data protection, including cybersecurity for data privacy and personal data.

15. **Is there any specific threshold on the number of personal data subjects that requires a certain level of cybersecurity system?**

    There is **no** specific provision regarding this matter.

D. Data Processing

16. **What are the recognized, legitimate grounds of personal data processing in your jurisdiction?**

    The lawful basis for personal data processing in Indonesia is to obtain consent from the relevant data subject. Such data processing should be carried out in accordance with the specific purposes, expressly elaborated during the data obtainment. Therefore, the use of electronic information involving any personal data must be made with the approval of the relevant person and only for the specified purposes.

    Nevertheless, there are certain exceptions where the lawful basis may be waived if: (i) the disclosure of personal data is for law enforcement purposes; and (ii) the personal data interception is for the legitimate interest of the ESO as the data controller. The laws allow the legitimate interest basis as long as the relevant ESO adheres to the prevailing laws and regulations.

17. **What are the key requirements (*such as notification or consent from the personal data subject*) when processing personal data in your jurisdiction?**

    Please refer to our response in Point 16 above.

18. **Are there other requirements, restrictions, and best practices that should be considered when processing personal data in your jurisdiction?**

    As outlined in Point 16 above, the purposes of data processing shall be restricted and clearly expressed during the time of data collection. Therefore, ESOs are not allowed to process any data that is not in the scope of processing purposes stated in the data subject's consent form.

    In addition, GR 71/2019 stipulates that the management, processing, and/or retention of the electronic system and data for ESO in the public sector shall be done within the Indonesian territory. The exemption of this provision is available if the required retention technology is not available domestically. This clearly

provides that any data processing done by a Public ESO is still subject to the data onshoring requirements.

Another provision worth considering is the Personal Data retention period. MoCI Regulation 20/2016 stipulates that the retention period of personal data is five years. In this instance, any obtained data should be retained for, at least, five years, from the last date it is used by the data subject.

E. Data Transfer

19. **What are the requirements that apply to a transfer of data to third parties?**

There is no specific requirement on this matter. However, it is important to note that a transfer of personal data is prohibited without the consent of the data subject.

20. **Are there restrictions that apply to a transfer of data abroad? Are there any exemptions on this matter?**

MoCI Regulation 20/2016 requires any cross-border transfer of personal data to fulfill the following requirements:

a. Submission of a notification regarding the intended transfer of Personal Data abroad, containing, at least, information on: (i) the country of destination; (ii) the name of recipient; (iii) the date of transfer, and (iv) the purpose of transfer.
b. A request for advocacy if required; and
c. Submission of report on the result of such cross-border transfer,

Additionally, no personal data may be transferred abroad unless the receiving country has been declared to have the equivalent protection standard by the Minister of Trade.

21. **Do the prevailing law and regulations on cybersecurity provide certain requirements for a local data transfer? If yes, do they require certain methods or procedures for a data transfer?**

We note that no certain methods or procedures specifically apply to local data transfers apart from the principles discussed in Points 19 and 20 above.

F. Rights of Data Subject

22. **What are the rights of data subject in connection to personal data processing? Are there any exemptions to such rights? Please elaborate.**

The rights of a data subject pursuant to Art. 26 of MoCI Regulation 20/2016 are as follows:

a. the right to confidentiality of his/her personal data;
b. the right to access data alternation, supplementation, as well as renewal. This right should include the access to historical record of his/her personal data already transferred to the ESO;
c. the right to delisting, a data subject exercising this right is required to submit a petition to the relevant district court. If the petition is granted, the court decision should become the basis to request a delisting of the irrelevant electronic information and/or document to the ESO (under GR 71/2019);
d. the right to request the erasure of his/her personal data; and
e. the right to file a complaint in the dispute settlement for the failure to get the needed protection to maintain the confidentiality of his/her Personal Data.

In addition to the above, PDP Bill also provides that the personal data controller must ensure the implementation of the "*right to be forgotten*".

23. **Is there any procedure for data subjects to exercise their rights in your jurisdiction?**

There is no specific procedure under the prevailing laws, but there are legal provisions as discussed in this article.

24. **What remedies are available to data subjects in case of a breach of their rights?**

EIT Law provides the right for a data subject to file claim of monetary damages to the relevant ESOs by providing evidence of the actual damages due to the transpired security breach.

G. Data Protection Officer

25. **Is the appointment of a Data Protection Officer ("DPO") mandatory in your jurisdiction? If <u>yes</u>, what are the consequences of failing to appoint the officer?**

The prevailing laws do not stipulate mandatory appointment of a DPO, nor consequences for failing to conduct such appointment. The laws, however, require ESOs to provide accessible contacts to data subjects. The term DPO was introduced in PDP Bill.

26. **What are the key responsibilities of a DPO in your jurisdiction?**

The current prevailing laws do not stipulate this matter, given that PDP Bill has not been passed.

Nonetheless, PDP Bill provides the following key responsibilities of a DPO:

(i) informing and advising the personal data controller or processor to comply with the prevailing laws and regulations;
(ii) supervising and ensuring the relevant data controller's or processor's compliance with PDP law and the privacy policy related to the assignment, including taking the responsibility, raising the awareness, providing the training for the related parties in the personal data process, and conducting the audit;
(iii) providing the advice in the evaluation on the impact of personal data protection, and monitoring the performance of the personal data controller and/or processor; and
(iv) coordinating the relevant stakeholders and acting as the liaison officer in managing issues related to personal data processing, including providing the consultancy on risk mitigation and/or other matters.

H. Data Breach

27. **Is it mandatory to provide a notification in the event of a data breach? If <u>yes</u>, who must be notified (<u>i.e.</u>, the data protection authority, the data subject, etc.) and what kind of information must be provided?**

Indonesian prevailing laws and regulations requires an ESO experiencing a data breach to immediately notify the relevant personal data subject and authorities, then go through the process in the following details:

a. **Relevant Authorities:** An ESO experiencing a data breach is obliged to notify the owner of the leaked data, and later on, file a complaint to the Directorate General of Informatics Application of MoCI. This complaint is intended to resolve a possible dispute caused by the data breach.

b. **Personal Data Subject:** The notice of breach to the Data Subject should include the following information:

a) the reasons and causes of the data breach;
b) the notice of breach can be submitted electronically provided that the Data Subject has agreed to such submission method during the collection of his/her Personal Data;

c) the confirmation that the Data Subject will receive a report if the data breach leads to a potential loss; and

d) the written report submitted to relevant Data Subject within 14 days after the occurrence of the breach.

28. **Are companies required to share details of actual or potential cybersecurity threats, or other cyber-intelligence information, with industries or other stakeholders? If yes, what kind of information must be shared?**

No requirements have been imposed on companies in this sense. The prevailing laws only require the ESOs to notify the relevant parties in the event of data breaches as explained in Point 27.

29. **How would a breach of data protection be handled by the authority? Can such breach lead to administrative sanctions or criminal penalties?**

Administrative and criminal sanctions can be imposed on persons committing unlawful acts, which include but not limited to all activities that violate the provisions of the prevailing laws and regulations on data protection and cybersecurity, carried out in bad faith. These sanctions are regulated by EIT Law, and other relevant regulations.

The applicable administrative sanctions are as follows:

a. MoCI Regulation 20/2016 provides the following sanctions:
   (i) verbal warnings;
   (ii) written warnings;
   (iii) suspension of business activities; or
   (iv) announcement of the breacher in MoCI's website.

b. GR 71/2019 provides the following sanctions:
   (i) written warnings;
   (ii) administrative penalty;
   (iii) suspension of business activities;
   (iv) termination of access to the electronic system; or
   (v) expulsion of the relevant platform as registered ESO.

In addition to the above, criminal sanctions in the form of fines and/or imprisonment are also applicable.

a. fine of IDR 600,000,000 (six hundred million rupiah) to IDR 800,000,000 (eight hundred million rupiah), and/or 4 to 8 years imprisonment for unlawful access;

b. fine of IDR 800,000,000 (eight hundred million rupiah) to IDR 1,000,000,000 (one billion rupiah), and/or 6 to 10 years imprisonment for illegal interception or wiretapping of transmission;
c. fine of IDR 2,000,000,000 (two billion rupiah) to IDR 5,000,000,000 (five billion rupiah), and/or 8 to 10 years imprisonment for unlawful alteration, addition, reduction, transmission, tampering, removal, transfer or concealment of electronic information or record; and
d. fine of IDR 10,000,000,000 (ten billion rupiah) to IDR 12,000,000,000 (twelve billion rupiah), and/or 10 to 12 years imprisonment for unlawful manipulation, creation, alteration, destruction, or damage of electronic information or document with a purpose of creating a certain assumption or conducting other violations in the processing of electronic information or documents.

30. **What other requirements, restrictions, and best practices should be considered in the event of a data breach?**

The government of Indonesia is aiming to complete the enactment of PDP Bill soon. When the bill is enacted into law, stricter provisions on Personal Data Protection and cybersecurity will be enforced. PDP Bill is expected to provide a more comprehensive guideline for personal data protection practitioners.

We still have to wait and see whether PDP Bill will have further changes prior to its enactment.

Nusantara Legal Partnership

Marshall S. Situmorang
marshall.situmorang@nusantaralegal.com

Andhitta Audria Putri
audria.putri@nusantaralegal.com

Sampoerna Strategic Square, North Tower, Level 14, Jendral Sudirman Kav.45-46 Jakarta 12930
021 - 50980355
www.nusantaralegal.com

India

Ravi Singhania and Dipak Rao | Singhania & Partners LLP

Data Privacy and Cybersecurity Comparative Guide

A. Definition and Scope of Data Privacy and Cybersecurity

Data Privacy

1. **Is there any specific definition of "*personal data*" in your jurisdiction? Do the prevailing laws provide distinction between personal data and sensitive personal data?**

   In India the term of personal information has been defined rather than personal data. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**SPDI Rules**") defines Personal Information as "*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*."

   Further, "sensitive personal data or information" of a person under SPDI Rules has been defines as "*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 conditions;*
   (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 services;*
   (viii) *Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise"*

   The Government of India has formulated a new legislation on personal data protection through introduction of the Personal Data Protection Bill, 2019 ("**PDP Bill**") in the Indian Parliament, which on the date of publication of this guide, is still under debate and has not become a law. The PDP Bill defines the term "Personal Data" as 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. Personal Data under PDP Bill has been further classified as sensitive personal data[1] and critical personal data[2].

2. **What is the scope of "*personal data*" pursuant to the relevant laws and regulations in your jurisdiction?**

Indian laws do not provide any specific scope of personal data. However, personal data as discussed above includes data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual.

3. **Who are the relevant stakeholders (i.e., data processor, controller, etc.) under the data protection regime in your jurisdiction?**

Current laws governing data privacy and protection do not specifically define data processor or data controller. However, following entities can be attributed as stakeholders under the current Indian laws:

a) A body-corporate[3] or person on its behalf who are collecting, storing or processing data;
b) Data Provider, to whom the personal data relates to.
c) Adjudicating Officer appointed by Government of India ("Adjudicating Officer"), has powers to adjudicate on the contraventions committed under Information Technology Act, 2000 ("IT Act").
d) Appellate Tribunal, has powers to receive appeals from any person aggrieved from the orders of an Adjudicating Officer.
e) Indian Computer Emergency Response Team ("CERT-In") entrusted with handling and responding to any cyber security incident and creating awareness in relation to cyber security. It interacts and seeks responses to respond and prevent cyber security incidents, from its following stakeholders:

    i) Sectoral Computer Response Teams;
    ii) Intermediaries;
    iii) Internet Registry and Domain Registrars;
    iv) Industry;
    v) Vendors of information Technology products including security products and services;
    vi) Academia, Research and Development Organizations;
    vii) Security and Law Enforcement Agencies;
    viii) Individuals or group of individuals;
    ix) International Computer Emergency Response Teams, Forums and expert groups;
    x) Agency engaged for the protection of Critical Information Infrastructure, such as National Critical Information Infrastructure Protection Centre ("NCIIPC"); and

[1] PDP Bill defines "sensitive personal data" as such personal data, which may, reveal, be related to, or 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.
[2] PDP Bill defines "critical personal data" as such personal data as may be notified by the Government of India to be the critical personal data.
[3] IT Act defines "body corporate" as means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

xi) Department of Telecommunications.

The PDP Bill has defined following stakeholders in a data protection regime-

a) 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.

b) Significant Data Fiduciary- The Data Protection Authority ("Authority") having regard to following factors, can notify any data fiduciary as significant data fiduciary:
   i) volume of personal data processed;
   ii) sensitive personal data processed;
   iii) turnover of data fiduciary;
   iv) risk of harm by processing by the data fiduciary;
   v) use of new technology for processing; and
   vi) any other factor causing harm from such processing.

c) Data Principal- the natural person to whom the personal data relates.

d) 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.

Cybersecurity

4. **Is there any specific definition of "*cybersecurity*" in your jurisdiction? Do the prevailing laws provide distinction between "*data protection*" and "*cybersecurity*"?**

Cybersecurity has been defined under the provisions of IT Act, as protecting information, equipment, devices, computer, computer resource, communication device an information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

The current laws in India do not distinguish between incidents concerning 'data protection' and 'cybersecurity', as it does not separately define "data protection". However, the IT Act does provide separate penalty for offences concerning breach of data or information as mentioned hereinafter.

5. **What are the subjects of cybersecurity? Does cybersecurity apply to certain industries and types of information?**

The Government of India has authorized CERT-In to overlook and respond to the cyber security incidents and assist cyber users in the country in implementing measures to reduce the risk of cyber security incidents. The functions of CERT-In include following services-

a) Response to cyber security incidents
b) Prediction and prevention of cyber security incidents
c) Analysis and forensics of cyber security incidents
d) Information security assurance and audits

e) Awareness and technology exposition in the area of cybersecurity
f) Training or upgrade of technical know-how.
g) Scanning of cyber space with respect to cyber security vulnerabilities, breaches and malicious activities.

The National Critical Information Infrastructure Protection Centre ("**NCIIPC**") is the national nodal agency for protection of critical information infrastructure from any cyber incident. NCIIPC has identified the following industries as critical sectors-

a) Power and energy
b) Banking, financial services and insurance
c) Telecom
d) Transport
e) Government agencies
f) Strategic and public enterprises

B. Governing Authority of Data Privacy and Cybersecurity

Data Privacy

6. **Is there any specific government agency that oversees data privacy legislation in your jurisdiction? Please define what powers and authorities such agency has in the data privacy enforcement?**

There is no specific government agency which oversees data protection in India, since there are various rules governing data collection, storage and usage concerning various industries.

Cybersecurity frameworks or guidelines have also been laid down by financial sector regulators such as Reserve Bank of India ("**RBI**"), Insurance Regulatory and Development Authority of India ("**IRDAI**") and Securities Exchange Board of India ("**SEBI**"). These guidelines are comprehensive in nature as they relate to both data privacy and cybersecurity. Guidelines issued by IRDAI and RBI also cover data localization norms and requirements for the regulated entities.

RBI requires organizations such as banks operating in India, payment service providers authorized by RBI and other entities engaged by payment service providers to store payment data which includes customer data, bank account details, payment credentials and transaction data, in India.

Similarly, IRDAI (Maintenance of Insurance Records) Regulations, 2015 requires insurers to store data relating to all policies issued and claims made in India in data centers located in India.

Financial Sector: The Credit Information Companies (Regulation) Act, 2005 ("**CIC Act**") imposes an obligation on credit information companies to adhere to privacy principles at the stage of collection, use

and disclosure of credit information, and requires them to ensure that credit information held by them is accurate, complete and protected against loss or unauthorized use, access and disclosure also to ensure data security and secrecy.

Further, RBI Master Direction on Know Your Customer (KYC) Direction, 2016 limit the categories of information that banks and financial institutions can seek from their customers. Once such information is collected, there is an obligation on banks to keep it confidential. Further, multiple instruments such as the Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs, the Master Circular on Customer Services, 2009 and the Code of Banks Commitment to Customers etc. all provide for privacy and customer confidentiality obligations that have to be adhered to by various entities in the financial sector.

Telecom: Data protection norms in the telecom sector are primarily dictated by the Unified License Agreement issued to Telecom Service Providers ("**TSP**") by the Department of Telecommunications ("**DoT**"). The format in which, and the types of information that are to be collected from the individual is prescribed by the DoT. A TSP has an obligation to take necessary steps to safeguard the privacy and confidentiality of the information of individuals to whom it provides a service and from whom it has acquired such information by the virtue of the service provided.

CERT-In is designated as the national nodal agency for responding to computer security incidents as and when they occur. CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

a) Collection, analysis and dissemination of information on cyber incidents;
b) Forecast and alerts of cyber security incidents;
c) Emergency measures for handling cyber security incidents;
d) Coordination of cyber incident response activities; and
e) Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

The PDP Bill provide for establishment of the Data Protection Authority of India ("**Authority**") to protect the interest of the Data Principals, prevent any data breach and promote awareness about data protection.

7. **Can the data protection authority in your jurisdiction cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?**

The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties Rules, 2013 ("**CERT Rules**") stipulates CERT-In to exchange information relating to attacks, vulnerabilities and solutions in respect of critical sector with NCIIPC.

Further, CERT Rules stipulates CERT-In to co-operate and collaborate with (i) the organisations within and outside India engaged in protecting and responding to cyber security incidents; (ii) organisations engaged in collection of intelligence, law enforcement, or investigation; (iii) industry, service providers and research and development institutions; and (iv) individual or group of individuals.

The Authority under PDP Bill can cooperate and collaborate with various stakeholders of data regime to protect the interest of Data Principals, prevent any data breach and promote awareness about data protection.

Cybersecurity

8. **Is there any specific government agency that oversees cybersecurity legislation in your jurisdiction? Please define what powers and authorities such agency has in the cybersecurity enforcement?**

In India, CERT-In is a functional organisation under Ministry of Communications and Information Technology with the objective of securing Indian cyber space and responding to any cyber security incidents. It provides incident prevention and response services as well as cyber security management services to various stakeholders as discussed under point 35 and 36.

9. **How does the cybersecurity authority cooperate with Data Protection Office ("DPO")? Does your jurisdiction provide certain guidelines for this matter?**

There is no concept of DPO in India. However, SPDI Rules provide for the appointment of a grievance officer by body corporates collecting or processing the data to address any discrepancies and grievances of their provider of information. The grievance officer needs to redress the grievances or provider of information expeditiously but within one month from the date of receipt of grievance.
However, there are no specific guidelines for co-operation of CERT-In with the grievance officer.

The PDP Bill mandates appointment of DPO by the Significant Data Fiduciary. The Bill does not provide any guidelines for cooperation of the Authority with the DPO.

C. Regulatory Framework and Registration

Data Privacy

10. **What are the applicable laws and regulations that govern data privacy and personal data protection in your jurisdiction? Please identify further laws on data protection in specific sectors, if any.**

Applicable laws and regulations that govern data privacy and personal data protection in India are-

a) Information Technology Act, 2008;
b) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011;
c) Information Technology (Intermediaries Guidelines) Rules, 2011;
d) Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013;
e) Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.

Laws on data protection in specific sectors-

a) Guidelines on Information and Cyber Security for insurers dated 07.04.2017 by Insurance Regulatory and Development Authority of India.
b) Cyber Security Framework in Banks dated 02.06.2016 by Reserve Bank of India.
c) Cyber security and Cyber Resilience framework for Stock Brokers / Depository Participants dated 03.12.2018 by Securities and Exchange Board of India.
d) Recommendations on Privacy, Security and Ownership of the Data in the telecom sector dated 16.07.2018 by Telecom Regulatory Authority of India.

The PDP Bill, 2019, is yet to become a law and is limited to the protection of personal data. The PDP Bill, when effective, will have overriding effect over any other law or rules for the time being in force.

11. **Are there any exemptions under the data privacy and personal data protection rules in your jurisdiction?**

As discussed under point no 31, under SPDI Rules, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law is not to be regarded as sensitive personal data or information.

SPDI Rules, further provides that, no prior consent of the information provider would be required by the data collector in case information is being shared with any government agency for law enforcement purposes.

The PDP Bill, 2019 empowers the Government of India to exempt any agency of government from the application of the PDP Bill, in the interest of sovereignty, integrity and security of India, friendly relations with foreign states and public order. Exemptions of certain provisions for processing of personal data is provided for following reasons-

a) In the interest of prevention, detection, investigation and prosecution of any offence or any other contravention of any other law for the time being in force;

b) Disclosure of personal data is necessary for enforcing a legal right, seeking any relief, defending any charge or obtaining legal advice from an advocate in any impending legal proceeding;
c) Processing of personal data by any court or tribunal in India, is necessary for the exercise of any judicial function;
d) Personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or
e) Processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organisation.

12. **Do the data privacy applicable laws and regulations apply extraterritorially? If yes, how do DPO and the government exercise such duties?**

The IT Act provides for the applicability of its provisions to any offence or contravention which is committed outside India, if such an offence or contravention involves a computer system or computer network located in India.

Further SPDI Rules restricts sharing of information outside India with only those organizations adhering to the same standards of data protection, as stipulated under SPDI Rules.

Any person aggrieved due to contraventions of any of the above provisions can file a complaint with the appropriate Adjudicating Officer and seek for appropriate remedial measures.

The PDP Bill prohibits processing of sensitive personal data and critical personal data outside India. Any transfer of sensitive personal data outside India will require consent of the Data Principal and needs to be approved by the Authority. Such transfer will be allowed only if the transfer is subject to an adequate level of data protection as per the prevailing law.

13. **Is the registration of data controllers and processors mandatory in your jurisdiction? If yes, how is the registration procedure completed, and what are the consequences for failing to conduct the registration?**

The IT Act and the related rules do not recognize the concept of data controllers and processors. However, SPDI Rules mentions body corporates who either themselves or through any person on their behalf collects, receives, possess, stores, deals or handle information.

The PDP Bill mandates registration of Data Fiduciaries with the Authority in such manner as may be specified by regulations.

Cybersecurity

14. **Is there any specific laws and regulations that govern cybersecurity for data privacy and personal data in your jurisdiction?**

Following law and regulation govern cybersecurity for data privacy and personal data in India-

a) Information Technology Act, 2000;
b) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011;
c) Information Technology (Intermediary Guidelines) Rules, 2011.

15. **Is there any specific threshold on the number of personal data subjects that requires a certain level of cybersecurity system?**

There is no threshold of information providers which an organization needs to have, for them to have a certain level of cybersecurity system. Any organization which collects information from the information providers needs to maintain reasonable security practices and procedures as stipulated under SPDI Rules.

Under PDP Bill the Authority may notify any Data Fiduciary to be a Significant Data Fiduciary based on the volume of personal data processed being one of the factors among other factors. Once a Data Fiduciary has been designated as a Significant Data Fiduciary, it is required to follow additional compliances, few of which are appointment of DPO, carrying out data protection impact assessment and submission and approval of the assessment report from the Authority.

D. Data Processing

16. **What are the recognized, legitimate grounds of personal data processing in your jurisdiction?**

The SPDI Rules mainly provides provisions concerning, the collection, use and transmission of sensitive personal data or information.

Under the SPDI Rules, sensitive personal data or information can be collected only for a lawful purpose of the data collector and if a valid written consent has been obtained from the provider of personal data regarding purpose of usage before information is collected. As per the rules such data / information should be used only for the purpose for which it has been collected.

However, no prior consent of the information provider would be required in case information is being shared with any government agency for law enforcement purposes.

Additionally, SPDI Rules restricts a data collector from retaining the information for any duration longer than it is required for the purpose for which it was collected.

The PDP Bill however, covers provisions concerning processing of personal data which also includes sensitive personal data.

17. **What are the key requirements (*such as notification or consent from the personal data subject*) when processing personal data in your jurisdiction?**

Please see Point 46 above.

18. **Are there other requirements, restrictions, and best practices that should be considered when processing personal data in your jurisdiction?**

As outlined in Point 46 above, the purpose of sensitive personal data or information collection and its usage by the body corporate collecting data is to be clearly expressed to the provider of information during the of collection of information. Therefore, a body corporate or any person acting on its behalf is not allowed to use any data that is not in the scope of processing purposes as stated in the data provider's consent. The data collector is required to provide a privacy policy for handling of or dealing in personal information including sensitive personal information, which needs to be published on the website of the data provider.

The data collector is required to implement security practices and procedures for protecting the sensitive data or information, in the form of standards as prescribed by IS/ISO/IEC 27001 (Information Technology – Security Techniques – Information Security Management System - Requirement) or any other code of best practices for data protection other than IS/ISO/IEC 27001 in case of any industry association whose members are self-regulating by following such standards. Such standards or code of best practices for data protection needs to be approved and notified by Government of India.

Further, a data collector cannot retain sensitive personal data or information for any longer duration than it is required for the purpose for which information was collected.

Additionally, in case the data collector possessing or handling any sensitive personal data or information in a computer resource owned by it, is negligent in maintaining reasonable security procedures and causes wrongful loss or gain is liable to pay compensation to the affected person.

Under the PDP Bill every Data Fiduciary and Data Processor, considering the nature, scope and purpose of processing personal data, the risks associated, and severity of the harm that may result from such

processing, is required to implement necessary security safeguards such as use of methods like de-identification, encryption etc.

Additionally, a Significant Data Fiduciary is required to undertake a data protection impact assessment before the commencement of any processing involving new technologies or large-scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals.

E. Data Transfer

19. **What are the requirements that apply to a transfer of data to third parties?**

Under the SPDI Rules, a body corporate collecting or processing data ("**Transferor**") can transfer sensitive personal data or information including any information[4] to any other body corporate or a person ("**Transferee**") in India or outside India, if:

i) It is necessary for performance of contract between the data collector and data provider or

ii) If the data transfer has been consented by the data provider.

However, no data/information can be transferred unless the Transferee is adhering to the same level of data protection as is being followed by the Transferor as required under the SPDI Rules.

20. **Are there restrictions that apply to a transfer of data abroad? Are there any exemptions on this matter?**

As discussed in point 49 above, Transferor may transfer the sensitive personal data or information including any information, if, either it is necessary for performance of the contract between the data collector and data provider, or if the data transfer has been consented by the data provider. Also, no sensitive data or information may be transferred outside India unless the Transferee adheres to same level of data protection as being followed by the Transferor in India in accordance with the SPDI Rules.

As discussed hereinabove, RBI, has made it mandatory for all banks, intermediaries and other third parties to store all information pertaining to payments data in India. However, in case of an international transactions, the data of the foreign transaction can be stored in a foreign location.

The PDP Bill puts a restriction on transfer and processing of personal data without express consent of the Data Principal. It prohibits processing of critical personal data outside India, except in cases where the information is being transferred to (i) entities engaged in health services where such transfer is

[4] The IT Act defines "information" as data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.

necessary for prompt action to be performed under any given law or (ii) any country or entity where such transfer is permitted by Government of India. Further, subject to an approval by the Authority, the PDP Bill allows transfer of sensitive personal data outside India, however, such data should be continued to be stored in India.

21. **Do the prevailing law and regulations on cybersecurity provide certain requirements for a local data transfer? If yes, do they require certain methods or procedures for a data transfer?**

Please see Point 49 above.

F. Rights of Data Subject

---

22. **What are the rights of data subject in connection to personal data processing? Are there any exemptions to such rights? Please elaborate.**

The rights of a data provider as contained in IT Act read with SPDI Rules are as follows:

a) right to be informed about:
   i. the fact that the information is being collected;
   ii. the purpose of for which the information is being collected;
   iii. the intended recipient of the information; and
   iv. the name and address of the agency that is collecting and retaining the information.
b) right to refuse to give sensitive personal data or information;
c) right to withdraw the consent granted to data collector at the time of collection of information including sensitive personal data or information. Such a withdrawal request needs to be in writing;
d) right to confidentiality of the information/data of the data provider;
e) right to access, alternation, supplementation of the information including personal and sensitive personal data or information provided to data collector;
f) right to compensation; in case of any a body corporate possessing, handling sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing the data protection procedures; and
g) right to seek redressal of any grievance in relation to the processing of any information from the body corporate collecting data.

In addition to the above rights, the PDP Bill provides that a Data Principal can request for erasure of the personal data which is no longer necessary for the purpose it was processed. It also provides Data Principal the right to restrict or prevent the disclosure of its personal information by Data Fiduciary.

23. **Is there any procedure for data subjects to exercise their rights in your jurisdiction?**

A data provider aggrieved due to any breach of its rights under the IT Act or rules thereunder may approach the Adjudicating Officer and file a complaint with prescribed fees within the jurisdiction where the computer resource is located. The complaint should be filed in a prescribed format mentioning details of the complaint including the time and place of the contravention, brief facts of the case, details of the person against whom breach was committed, details of the respondent, and details of damages claimed.

24. **What remedies are available to data subjects in case of a breach of their rights?**

In the event a body corporate collecting, storing and processing sensitive personal data is negligent and fails to enforce appropriate security procedures resulting in wrongful loss or wrongful benefit to any individual, the affected individual is entitled to seek appropriate compensation from the said entity. Additionally, a data provider can also seek penalty for any disclosure of information, if such a disclosure has been done without the data provider's consent or is in violation of the lawful contract or is in violation of provisions of the IT Act.

G. Data Protection Officer

25. **Is the appointment of a Data Protection Officer ("DPO") mandatory in your jurisdiction? If <u>yes</u>, what are the consequences of failing to appoint the officer?**

There is no DPO in India. However, a body corporate collecting and processing data under SPDI Rules is required to appoint a grievance officer to address any grievance of the data provider, and is required to publish the name and contact details of the grievance officer on its website. Any organization who fails to appoint a grievance officer would be liable to pay a penalty extending to INR .025 million (approx. USD 335).

The term DPO has been introduced in the PDP Bill and every Significant Data Fiduciary is required to appoint a DPO having required qualifications and experience, who needs to be based in India. Any Significant Data Fiduciary who fails to appoint a DPO would be liable to pay a penalty extending to INR 50 million (approx. USD 666,665) or 2% of its total worldwide turnover whichever is higher.

26. **What are the key responsibilities of a DPO in your jurisdiction?**

As discussed above there is no DPO under the India laws and instead each of the data collector is required to appoint a grievance officer. A Grievance Officer under SPDI Rules is required to address any discrepancy or any grievance that a data provider may have with respect to the processing of information

provided by them. The Grievance Officer is required to redress any such grievance within a period of one month from the date of receipt of the grievance.

The PDP Bill provides following key responsibilities of a DPO:

i) providing information and advice to Significant Data Fiduciary on compliance of the provisions of PDP Bill;
ii) carry out data impact assessment in case processing by Significant Data Fiduciary involves new technologies, sensitive personal data or which has risk of significant harm to data providers, submit the assessment report to Authority and seek its approval for the intended processing;
iii) provide advice to Significant Data Fiduciary on preparation of "privacy by design policy" containing best practices designed to identify and avoid harm to data providers;
iv) coordinating and cooperating with the Authority on matters of compliance of the provisions of PDP Bill by Significant Data Fiduciary.

I. Data Breach

27. **Is it mandatory to provide a notification in the event of a data breach? If yes, who must be notified (i.e., the data protection authority, the data subject, etc.) and what kind of information must be provided?**

Yes, as per the CERT Rules, intermediaries, data centers and body corporate are required to report any cyber security incident including a data breach to CERT-In, within a reasonable time of the occurrence or discovery of occurrence, so that timely action can be initiated. Additionally, any affected individual or organization may also report any cyber security incident including any data breach to CERT-In within a reasonable time, so that timely response action can be initiated.

The notice reporting the cyber security incident to CERT-In includes few of the following important information:

- Information of the affected computer system;
- Type and description of the cyber security incident;
- Security infrastructure already in place; and
- Action taken to mitigate any further attacks or intrusion.

Under PDP Bill every Data Fiduciary apart from reporting the breach to the Authority, may also be required to post the details concerning the data breach on its website.

28. **Are companies required to share details of actual or potential cybersecurity threats, or other cyber-intelligence information, with industries or other stakeholders? If yes, what kind of information must be shared?**

Any company which is an intermediary or a data center or a body corporate collecting or processing data is required to report to CERT-In any cyber security incident in a reasonable time, which has occurred or has potential to occur, so that timely remedial action may be initiated by CERT-In.

29. **How would a breach of data protection be handled by the authority? Can such breach lead to administrative sanctions or criminal penalties?**

CERT-In serves as central point for reporting incidents. It analyses trends and patterns of intruder activity, develop preventive strategies for the whole constituency and take an in-depth look at an incident report or an incident activity to determine the scope, priority and threat of the incident. It sends out recommendations for recovery from, and containment of damage caused by the incident and help system administrators take follow up action to prevent recurrence of similar incidents.

Further any complaint in relation to the breach of data protection can be reported to the Adjudicating Officer in a prescribed format by the aggrieved person. The consequence of breach of data protection are the following:

a) A body corporate negligent in dealing or handling any sensitive personal data or information, would be liable to pay damages to the person so affected. There is no upper limit specified for the compensation that can be claimed by the affected party.
b) Any disclosure of information, without the consent of the person concerned and in breach of the lawful contract is punishable with imprisonment for a term extending up to three years and fine extending to INR 0.5 million (approx. USD$ 6,665).
c) Fraudulent or dishonest use of the electronic signature, password or any other unique identification feature of any other person, is punished with imprisonment for a term extending to three years and would also be liable to fine extending to INR 0.1 million (approx. USD$ 1335).
d) Indian Penal Code, 1960 also penalizes breach of data protection and data privacy.
    i. Anyone who dishonestly takes any movable property out of the possession of any person without that person's consent, is said to have committed theft, which is punishable with imprisonment upto three years or a fine or both.
    ii. Anyone who being entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law, or of any legal contract, is said to have committed "criminal breach of trust" which is punishable with imprisonment upto three years or a fine or both.

Under the PDP, a Data Fiduciary is required to inform the Authority about any breach of personal data, if such breach is likely to cause harm to any Data Principal. Upon receipt of breach notice, the Authority after taking into consideration the likely harm that may be caused to the Data Principal, may direct the Data Fiduciary to take remedial actions as soon as possible and post the details of the breach on its website.

As per the PDP Bill, any breach of personal data will have the following consequences:

i. Where a Data Fiduciary fails to adhere to the security safeguards as provided under the PDP Bill or contravenes any provision pertaining to the (a) processing of personal data; (b) processing of personal data of children; and (c) transfer of personal data outside India. Such offences are punishable with a penalty up to INR 15 million INR (approx. USD$ 2 million) or four percent of its total worldwide turnover of the preceding financial year, whichever is higher.
ii. Any person who re-identifies and processes personal data which has been de-identified5 by a Data Fiduciary, without the consent of such Data Fiduciary or Data Processor, is punishable with imprisonment up to 3 years or with a fine which may extend up to INR 0.2 million (USD$ 2700) or both.
iii. A Data Principal who has suffered harm as a result of any violation of any provision of the PDP Bill or the rules or regulations made thereunder by a Data Fiduciary or a Data Processor, has the right to seek compensation from the Data Fiduciary or the Data Processor.

30. **What other requirements, restrictions, and best practices should be considered in the event of a data breach?**

As discussed above, SPDI Rules in India require every data collector to implement reasonable security practices and procedures either through the procedures which are compliant of IS/ISO/IEC 27001 or any other procedures which have been approved and notified by the Government of India.

Additionally, CERT-In through its designated officer may issue directions or advisories for improving cyber security of information infrastructure, to the intermediaries, data centers, body corporates or any other concerned person through email, fax or registered post. Such directions or advisories are to be implemented by the concerned entity and should be reported back to CERT-In, within the time period as specified in the direction or advisory issued by CERT-In.

As discussed above in this guide, under PDP Bill a Data Fiduciary is required to inform the Authority about any breach of personal data, if such breach is likely to cause harm to any Data Principal. Upon receipt of breach notice, the Authority after taking into consideration the likely harm that may be caused

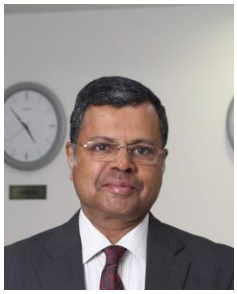
[5] PDP Bill defines 'de-identification' as 'the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal.

to the Data Principal, may direct the Data Fiduciary to take remedial actions as soon as possible to restrict the harm to the Data Principal.

SINGHANIA & PARTNERS LLP
SOLICITORS AND ADVOCATES

Ravi Singhania

ravi@singhania.in



Dipak Rao

dipak@singhania.in

P-24 Green Park Extension, New Delhi 110016, India

t: +91 (11) 4747 1414

e: delhi@singhania.in

www.singhania.in