Ujvala Consultants Private Limited
#37, Ujvala, 20th Main
BSK First Stage, Bangalore 560050
Web: www.ujvala.com:E mail: naavi@naavi.org: Mob: 9343554943
CIN:4140KA1994PTC015224

Data Protection Standard of India

Proposed Expansion of the Scope of PDPB 2019

From the legal perspective, "Data" is classified as "Personal Data" (PD) and "Non Personal Data".(NPD) Data becomes "Personal" if the data can be identified to a living natural person. Any other data is "Non Personal".

PD can be further divided into Non Sensitive PD, Sensitive PD and Critical PD as per the definitions that the PDPA-In (Personal Data Protection Act of India), may define. At present part of Information Technology Act 2000 (ITA 2000) consisting of Section 43A, 72A and other sections such as 67C or 79 address the requirements of obligations for "Notice", "Consent", "Data Minimization", "Minimal Retention", "Cross border data transfer", "Data security" etc in respect of personal data. The PDPB 2019 (Personal Data Protection Bill 2019 which will eventually become PDPA-In) elaborates the regulatory structure for "Personal Data Protection" including setting up of an authority called the "Data Protection Authority of India" (DPA).

When DPA was named as such, the functions of the DPA was restricted to the contents of PDPB 2019 and hence the DPA was actually Personal Data Protection Authority of India (PDPAI).

As per the PDPB 2019, "Anonymized Data" was defined as personal data from which the personal identity elements are permanently removed in such a manner that it cannot be re-identified. The "Permanent" removal means that the identify parameters are removed and destroyed so that even the "Anonymizing entity" cannot reverse the process. For this purpose the DPA is expected to develop a "Anonymisation Standard".

While the standard of anonymization is expected to make the anonymized data incapable of being re-identified, it cannot be technically infeasible to re-identify a set of anonymised NPD into an identified PD. This could be accomplished through a forensic level effort with unlimited resources of time and processing or with criminal conspiracy. Just as a "One Way Hash" is considered in law as "Infeasible of being broken or "Encryption of a certain standard" is accepted as "Adequate level of security", the "Standard level of Anonymization" that the DPA has to identify should be considered as the level below which anonymized PD cannot be re-identified. As long as this level is sufficiently high, the re-identification is considered "infeasible".

On the contrary "De-identification" of Personal data is identified as removal of identity parameters and keeping them aside and creating a set of personal data which cannot be identified with any individual but if the mapping information which is removed and set aside is brought back, the data can be re-identified. "Pseudonymization" is a form of de-identification where the identity parameters are removed and replaced with other proxy data so that the structure of the Personal data set is

maintained but the identity of the data principal is hidden. Again the mapping data is preserved so that the data can be de-pseudonymized if required.

The PDPB 2019 considers de-identified and pseudonymized PD as “Personal Data” while the “Anonymized Personal Data” is out of scope of PDPB 2019 and is considered “Non Personal Data”.

When the Kris Gopalakrishnan committee on Non personal Data Governance gave its recommendations, it focussed on how NPD can be monetized. For this purpose it defined categories of NPD, the roles of different collectors and processors of NPD etc. It also suggested standards of Anonymization which was the boundary between Personal and Non Personal Data. The Kris Gopalakrishna committee suggested that there is a need for a separate regulator for NPD Governance and a set of legal provisions which could be codified as the Non Personal Data Governance Act.

It should be noted that Kris Gopalakrisha Committee (KGC) envisaged an act for “Governance” and not “Protection”. The reason was that “Protection” of NPD was already covered under ITA 2000. In fact, ITA 2000 covers “Protection” of both PD and NPD and imposes civil and criminal liabilities for non compliance of ITA 2000. The enforcement of ITA 2000 is divided between the “Adjudicator” who enforces the Civil liability provisions and the “Police” who impose the criminal liability provisions. The Judiciary takes over the responsibility for adjudication of civil proceedings at the High Court level. In the Criminal proceedings, Judiciary takes over at the trial stage itself.

The PDPB 2019 actually created the DPA and the Adjudicator/Appellate Tribunals under PDPB 2019 and created a parallel structure to administer compliance of the Act and impose administrative fines etc. The administration of NPD related non compliance as per ITA 2000 remained with the authorities under ITA 2000.

It is now being speculated that the scope of the PDPAI would be expanded to make it a “Reporting authority for Breach of Non Personal Data” which is presently handled by the CERT-In and also consider the PDPAI as the Non Personal Data Governance Authority also.

While in principle, this means an advancement of at least one of the recommendations of the KGC and creation of one “Super Data Regulator”, in the absence of detailed “NPD Governance Act”, the “Personal and Non Personal Data Protection and Governance Authority of India “ (Super Data Regulator) would have clear action points only about the PD protection and vague perceptions on NPD Governance.

It is likely that the vested interests who are trying to delay the passing of the PDPB 2019 will raise the bogey that we need to add the provisions of the recommendations of the KGC into the draft of PDPB 2019 before it is passed and thereby create an indefinite delay in the passing of the Act. Also by adding the NPD Governance provisions into the current PDPB 2019, the law will lose the focus expected by the Supreme Court and it could be one of the grounds on which the law may be challenged in the Courts as being created in haste and without proper application of mind.

It is a valid argument that it is desirable not to tamper with the PDPB 2019 to expand its scope to NPD Governance now and subsequently deliberate and pass a Non Personal Data Governance Act where in the regulatory responsibilities can be merged with the PDPAI so that it can be designated as the “Super Data Regulator” as a part of such a new Act.

We leave it to the wisdom of the new Joint Parliamentary Committee to consider this aspect and take an appropriate decision.

Scope of Data Protection Requirements in the Industry

The industry presently considers “Information Security” as an obligation necessary to preserve the confidentiality, Integrity and Availability of information for decision making. Accordingly, even without the legal obligations, industry follows the “Best Practices” and created standards such as the ISO 27001.

In view of the high levels of “Administrative Penalties” envisaged under the PDPB 2019 as compared to the concept of “Compensation for damages” envisaged under the ITA 2000, and the possibility of penalty being imposed under PDPB 2019 even without a “Victim” suffering a damage to be compensated, it was necessary for the industry to look for fine tuning their “Information Security Management Systems” (ISMS) from the “Best Practice Objective” to “Law Compliance Objective”. Hence the industry moved from ISMS to PIMS as a focussed approach to personal Information management and later to the laser sharp focus of “Personal Data Protection Compliance Management”.

The PDPSI or the Personal Data Protection Standard of India therefore focussed on the “Personal Data Protection Compliance Management System” or PDP-CMS instead of ISMS or PIMS.

Now if the PDPB 2019 is modified to include some aspects of Non Personal Data Protection, such measures will automatically become part of the PDPSI.

However, organizations need to continue compliance of ITA 2000. Compliance requirements of ITA 2000 expanded slightly after the recent amended notification of “Intermediary Rules” under Section 79 of ITA 2000 with effect from 25th February 2021.

The notification of February 25, 2021 has been questioned in some High Courts and interim orders have already been passed by some of the High Courts. It is likely that the Supreme Court may take a final view on the order in due course. However, from the compliance point of view, it is considered necessary to incorporate the provisions of the Intermediary Guidelines of 25th February 2021 into the ITA 2000 compliance framework.

The undersigned as part of his advisory services under Ujvala Consultants Private Limited followed a framework titled IISF 309 (Indian Information Security Framework) which was tailored for the compliance of ITA 2008. This framework has now been revised and expanded as “DPSI” (Data Protection Standard of India) to incorporate the ITA 2008 after the notification of February 25th and also taking in the possibility of the PDPB 2019 becoming a law soon.

In order to meet the compliance requirements of ITA 2000 as well as PDPB 2019 it has become necessary to introduce DPSI as the twin compliance standard of PDPSI so that DPSI+PDPSI would be serve the Data Protection Compliance requirements of Indian organizations. This will be future ready even if the PDPB 2019 is expanded now and later merged with the Non Personal Governance act.

The following paragraphs discuss the envisaged requirements of DPSI as the Version of 2021.

DPSI Framework

Objective

The objective of DPSI as a framework is to provide a guideline to an organization to be compliant with the Information Technology Act 2000 (ITA 2000) as amended from time to time and the regulations associated therewith.

The implementation of DPSI is meant to fulfil the concept of “Due Diligence” under Section 79 which also percolates through other Sections including Section 43A, 43, 72A etc. Until the PDPB 2019

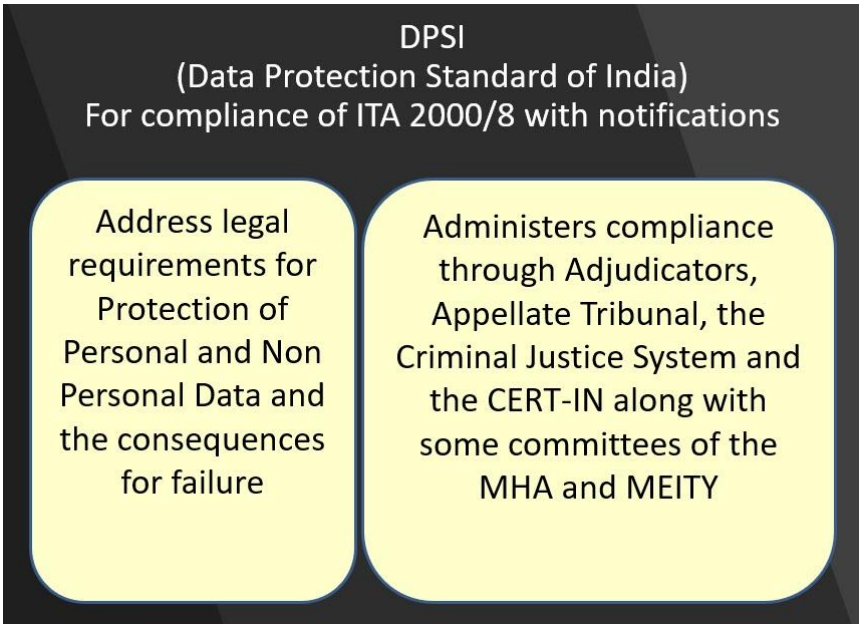
becomes an act in India, the "Reasonable Securities" under Section 43A will substitute the provisions of PDPB 2019 and hence DPSI will subsumes the responsibility for Personal Data Protection as envisaged under PDPB 2019.

Background

India adopted Information Technology Act 2000 (ITA 2000) with effect from 17th October 2021. The act for the first time gave legal recognition to "Electronic Documents" and "Digital Signature" and enabled "Judicially Recognized Electronic Contracts". The act also provided enablement of E-Governance. The Act prescribed Civil contraventions and Criminal offences and prescribed the system of Adjudication and Appellate Tribunal to redress civil compensation issues for victims of contravention of law. It also enabled the criminal justice system to take up issues related to Cyber crimes by making suitable amendments to the Indian Evidence Act to accommodate recognition and admission of electronic evidence in courts of law.

In December 2008, the act was substantially amended to introduce several sections to harden the Cyber Security aspects and introduce Personal Data Protection features in the Act. The amendments were notified on 27th October 2009 and some of the relevant notifications were issued on 11th April 2011 making the Act double up as the Personal Data Protection Act of India.

During the two decades since the Act has been in force, there have been several judgements of the Supreme Court making some amendments and reading down some provisions of the Act and the notifications all of which define the compliance requirements under the Act.



Organizations which contravene the law may face the liability for payment of compensation and aslos face criminal action some of which may be enforceable against the business executives, the Directors and other officials associated with the organization.

In view of the wide ramifications of non compliance of ITA 2000, it is necessary for every organization which comes within the scope of ITA 2000, to initiate appropriate compliance measures to systematically ensure compliance as part of its "Due Diligence".

The technical standards such as ISO 27001 has often been used as a guideline for ITA 2000 compliance but they are not focussed on compliance of ITA 2000 and hence there is a need for a focussed framework that the organizations need to follow to remain compliant.

DPSI endeavours to fill this gap.

40 Clauses of DPSI

The current version of DPSI identified as DPSI-2021 emerged out of the Indian Information Security Framework (IISF 309) which has been in use since March 2009 and had been updated to a 30 point framework before the introduction of the evolved version in the form of DPSI.

The 40 clauses are organized under 5 different responsibility centres namely

1. Management (12)
2. Compliance Officer (3)
3. Legal (5)
4. HR (5)
5. Technology (15)

The Responsibility for compliance of 40 controls are distributed as follows

1.Management and Business

1.1 : Governance Committee Constitution

1.2: Designation of a Compliance Officer

1.3: Risk Assessment and Risk Mitigation Policy

1.4: Whistle blower Policy

1.5: Data Valuation and Accounting Policy

1.6: Business Associate Relationship

1.7: Audit Policies

1.8: E- Audit

1.8: Internal and External Communication

1.9: Website and Cloud security

1.10: E Mail Policy

1.11 : Distributed Responsibility

1.12: Digital Signature/Authentication policy

2. Compliance Officer

2.1: Privacy Notice and Policy

2.2: Information Security Policy

2.3: Documentation and Record Keeping

3. **Legal**

3.1: Business Contract Management

3.2: Online Contract Policy

3.3: Grievance Redressal

3.4 Data Disclosure policy

3.5: IPR Policy

4. **HR**

4.1: Sanctions and Incentives
4.2: Work From Home
4.3: Onboarding, Evaluation and Termination
4.4: Internet access, Resource usage
4.5: Awareness and Training

5. **Technology**

5.1: Information Classification and Tagging
5.2: Hardware and Software Purchase
5.3: Physical Security
5.4: Access Control
5.5: Storage Security
5.6: Transmission Security
5.7: Process Security
5.8: System updation
5.9: Incident Management and Data breach reporting
5.10: Malware Control
5.11: BYOD
5.12: Data Destruction
5.13: Data Leak prevention
5.14: Data Retention and archival Policy
5.15: DRP/BCP

Description of clauses

1.1: Governance Committee Constitution

Constituting a Governance Committee is a best practice suggestion to ensure that the compliance issues that cut across different operating divisions can be effectively handled with the cross functional team of decision makers in the Governance Committee. (GC). The GC can be called “Data Protection Committee” (DPC). Since Personal Data Protection is part of the responsibilities of the management, there can be one DPC which takes care of both Personal and Non Personal Data Protection. Since in the coming days, “Monetization” of the Non Personal data is also the responsibility of the management, the DPC can be constituted as “Data Protection and Governance Committee” (DPGC).

The DPGC shall have representation from all stake holders in the organization who are associated with the Compliance requirements under the Data Protection laws such as ITA 2000 and Personal Data Protection Act if any.

The DPGC shall be constituted with the representation from the Business, Legal, HR, and Technology divisions. In case the organization maintains a Compliance division and Risk Management division, representatives from these divisions may also be added. From the management side, the CEO and one of the independent directors of the Board (in the case of a board managed companies) shall also be part of the DPGC.

The Compliance official/s responsible for compliance shall be part of the DPGC. Any other executive such as the CFO, Company Secretary or head of a unit etc who is considered as a Key decision maker shall also be part of the Committee. Where services of any external consultant is used for data protection or Governance, such a consultant shall also be part of the DPGC.

The DPGC shall meet periodically as may be required and document its proceedings. In each of the meetings the Committee shall review the report to be submitted by the compliance officer/s for the relevant previous period which shall also include a review of the Incident register for the period, the environmental developments etc.

1.2: Designation of a Compliance Officer

ITA 2000 mandates the designation of a "Grievance Redressal Officer" under Section 79. The requirement may also be considered as a requirement under Section 43A which now gets transferred to PDPB 2019.

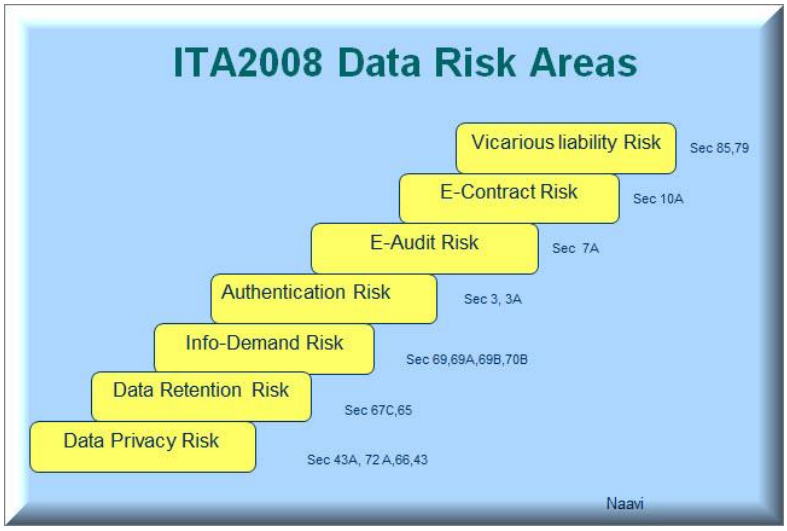
As a requirement under law as well as a best practice, a "ITA 2000 Compliance Officer"(ICO) shall be designated to closely monitor the requirements of compliance. If there is a designated DPO in the organization, the ICO and DPO shall complement each other under the guidance of the DPGC to ensure that the organization meets its compliance requirement.

The designated ICO shall be conversant with the provisions of ITA 2000 as well as the PDPB 2019 and the general principles of Information Security and Privacy protection. The ICO shall coordinate with the HR in terms of creation of awareness building and training of manpower and also with the technology and legal departments as required. He shall also manage the relationship with the CERT In and ensure coordination with the compliance counterparts in Business Associates, Customers and other external agencies with which the organization exchanges data in some form.

1.3: Risk Assessment and Risk Mitigation Policy

The organization shall conduct a Risk Assessment of its operations from the perspective of potential non compliance of any of the provisions of the ITA 2000.

The following diagram provides a rough indication of the risks represented by ITA 2000 provisions.



7 types of risks have been identified in the above diagram. A brief explanation of what kind of risks these represent are as follows.

1.3.1: Data Privacy Risk

Data Privacy risk represents the risk of non compliance of Sections 43A, 72A, 66 and 43. Section 43A applies to the need for practicing "Reasonable Security Practice" in respect of Sensitive Personal information and is getting converted into the provisions of the proposed personal data protection Act. In the interim period before the new act is passed, PDPB 2019 shall be considered as the "Due Diligence" requirement under Section 43A of ITA 2000. Section 43A may however not apply to Government bodies.

Section 72A applies to Non Sensitive Personal information and the compliance requirements under ITA 2000 was based on the contract. Consequent to the PDPB 2019 being available now, the compliance requirements can be tagged with PDPB 2019 as the legislative intent. However Section 72A is a criminal penalty section and read along with Section 85, escalates the criminal punishments to the executives of the Company.

Section 43 and the associated criminal section 66 has been added since they refer to "Non Sensitive information" also and defines "Compromise of data value" in very general terms such as "Diminution in the value of information residing a Computer or causing injury to information". It recognizes compromise of information whether personal or otherwise with the introduction of computer contaminants and in the form of "Providing assistance" to another person. These provisions can be applied for any data breach arising both for sensitive and non sensitive information.

1.3.2: Data Retention Risk

Data retention risk recognizes that under Section 67C as well as under Section 65 there are certain provisions which require retention of data for a reasonable period and in a proper format. Deletion of information before the period represented by these sections would be considered non-compliance. Similar retention is also defined under the rules notified under Section 79 and a minimum period of 6 months is designated as the data retention period in most cases.. In every case of deletion, ITA 2000 expects a due diligence to be exercised to document why there is no need to retain the data and not be deleted at the particular point of time.

Since the need for retention is defined for the purpose of retention of evidence, the archival has to also be done under the broad requirements of evidentiary requirements under law represented by Section 65B of Indian Evidence Act.

1.3.3: Info Demand Risk

The Info-demand risk represents the requirements of Sections 69,69A,69B and 70B where certain authorities are designated as having power to demand information from information owners and if they are not provided, there could be adverse criminal consequences. In order not to be caught in non-Compliance of these sections, organizations need to be aware of what kind of information may be demanded by the authorities and make technical and organizational provisions to enable meeting of such demands as and when they arise. This is a contingent requirement but the consequences of non compliance are serious and hence forms an important compliance requirement for the organization.

1.3.4: **Authentication Risk**

ITA 2000 has specific provisions of when an electronic document may become an evidence in a Court of law (Section 3, read along with Section 65B of Indian Evidence Act) as well as provisions of authentication under Sections 3 or 3A. Since organizations need to document certain documents with authentication and the non compliance may deny such authentication, the risks need to be assessed and mitigated.

1.3.5: E Audit Risk

Under Section 7A of ITA 2000, there are certain provisions regarding the conduct of data integrity audit in certain contexts. Non Compliance could lead to associated adverse consequences which need to be mitigated.

1.3.6: E Contract Risk:

Under Section 11, 12,13 and 14 of the Act there are provisions of attribution of an electronic document, determination of place and time of a contract, the need for acknowledgement etc. These provisions some time create a contract or accountability when it is not envisaged by the sender of a message or some times denies the operation of the message when the sender may want the accountability to be recognized. This risk needs to be mitigated to avoid both civil and criminal consequences of noncompliance.

1.3.7: Vicarious liability Risk:

Sections 85 and Section 79 of ITA 2000 represent instances when a contravention made by one person may attach to another person or organization because the other organisation is an intermediary or a company whose data assets were used in the commission of a contravention. In such cases all the provisions of liability in Chapter IX and XI of the Act can get transferred to the organization if it cannot defend through "Due Diligence". Hence taking measures to prevent commission of contravention through assets controlled by an organization becomes a compliance requirement, noncompliance of which is a risk to be mitigated.

Thus ITA 2000 Risk assessment is a risk assessment different from the risk assessment procedure in other ISMS risk frameworks and hence DPSI requires assessment to be done under the Techno Legal Risk assessment perspective. This is similar to the "Assessment of Harm" as a risk which is used in Personal Data Protection regulation.

Under DPSI, an assessment has to be made on what kind of harm may arise to the company, its executives as well as the public who may use the services of the organization.

Some of these risks are also addressed as separate clauses in the DPSI.

As a Risk assessment policy, the Risks are to be assessed, Mitigation measures should be applied and residual gaps should be documented as "Absorbed" or "Insured" or "Avoided". This will result in the Risk Mitigation Charter with documentation of the "Risk Absorption Policy" of the organization.

1.4: Whistle Blower Policy

The organization shall establish a whistle blower policy with adequate incentivisation and witness protection to develop early warning of risk arising out of either internal or external human threats or vulnerabilities. This is part of the due diligence and Reasonable Security practice.

1.5: Data Valuation and Accounting Policy

The organization shall establish effective policy for identifying, classifying and valuing data and providing visibility to the value on the financial statements of the organization. This is a measure to enhance the due diligence level and to provide adequate budgeting support for information security and Cyber Insurance.

1.6: Business Associate Relationship

The organisation shall ensure adequate verification and controls based on contractual binding to ensure that risks arising out of the business associates and any supply chain network is identified and mitigated. This is part of the due diligence and Reasonable Security practice.

1.7 Audit Policies

The organization shall establish policy controls for undertaking periodic security audits of all systems and manpower that interact with the data both internally and externally. This is part of the due diligence and Reasonable Security practice.

1.8: E Audit

As per Section 7A of the ITA 2000, wherever an audit provision existed in the legacy paper based systems under law, the same shall be carried out for the electronic documents also.

1.9: Website and Cloud Security

In order to mitigate the risk of unauthorized modifications of the cloud based data assets, including the website of the organization, appropriate measures shall be taken to maintain an effective access control and data integrity audit from time to time.

Where an organization maintains a public website, appropriate disclosures such as the ownership of the website, contact particulars of the organization, its grievance redressal officer etc shall be disclosed.

Where an organization is a Social Media Intermediary, it shall comply with regulations as may be required including content classification and participation in the industry level dispute resolution mechanisms.

1.10: E Mail Policy

The organization shall establish effective policy to ensure that no employee shall use the organization e-mail for personal use and shall be accountable to provide access of all data in the e-mail servers to the custody of the organization. The employees shall be accountable to turn over unstructured sensitive data in the e-mails to the custody of the organization.

1.11: Distributed Responsibility

Though the designated compliance official is responsible for compliance, every employee of the organization having access to a restricted data space within a folder, or within a computer or within an application or within a network shall be considered responsible for security of his data space and shall be accountable for any security breaches affecting data within the data space.

1.12: Digital Signature/ Authentication policy

Effective measures would be taken to ensure that all sensitive e-mails are digitally signed by authorized persons in the organization and only judicially acceptable digital/electronic signature systems shall be used for authentication.

2.1: Privacy Policy and Privacy Notice

The Compliance officer shall ensure that the organization meets the obligations under Section 43 A and under Section 79 (for activities in the capacity of an intermediary). If the organization maintains a website, a limited privacy policy for website visitors need to be disclosed on the website. Apart from the website policy, the organization shall meet the privacy requirements for employees through an internal policy document. The Privacy Notice/Policy shall meet the requirements of the PDPB 2019 including the consent requirements.

2.2: Information Security Policy

The organization shall adopt a comprehensive Information security policy which outlines how the Confidentiality, Integrity, availability, authentication and Non reputability of information is ensured.

The information security architecture shall adopt the best industry practices which are context based and use Identity and Access management strategies to meet the Work from home and BYOD requirements.

It shall incorporate the best practices represented by internationally accepted standards and include sub policies on Access Control, Encryption etc.

The policy shall cover, technical, organizational and operational controls necessary for the context in which the organization functions.

2.3: Documentation and Record Keeping

DPSI is essentially a techno legal compliance requirements and shall have a robust policy of documenting what is proposed, how the measures were communicated, how the implementation was tracked and what observations were made and how the issues are resolved. Documentation is the essence of compliance and should be reliable, authenticated and presentable to an external agency including the regulator or the Court when necessary.

3.1.: Business Contract Management

Business is a bundle of contracts and involves organization to customer or organization to contractor or organization to employee contracts. Every such contract needs to be documented and shall ensure that accountability for information security arising out of the contract is addressed. An inventory of contracts with necessary details are maintained for effective follow up.

3.2: Online Contract Policy

All contracts entered into online are made compatible with the Sections 11,12,13 and 14 of ITA 2000 and ensure that a proper contact person is designated and jurisdictional and grievance redressal issues are clarified. All contracts are properly authenticated as required under the law either by the use of recognized electronic signature or through other legally acceptable means.

3.3: Grievance Redressal Policy

The organization shall institute an appropriate policy to receive and resolve grievances from any stake holder through a system of negotiation, ombudsman, mediation and arbitration. All issues captured by the complaint handling system and the Incident management system that may have legal implications shall be suitably escalated to the grievance redressal system. Appropriate information shall be made available to the public and the stake holders about the availability of the alternate grievance redressal mechanisms. The Compliance officer himself or any other person may be designated exclusively as a grievance redressal officer and his contact details are made available on the website. Where an organization is considered a Significant Social Media intermediary, it shall ensure that it is part of the industry level dispute resolution mechanism also.

3.4: Data Disclosure Policy

The Organization shall adopt and implement necessary policies to ensure that disclosures necessary for the regulatory agencies, the law enforcement agencies and the authorized members of the public are in accordance with the law. Such disclosures shall be properly authenticated and documented.

3.5: IPR

The Organizations shall adopt and implement necessary policies to identify, documents and register where necessary intellectual property rights (IPR) that may arise as part of their activity. The data that represents IPR shall be appropriately valued and the value brought into the books of account appropriately.

4.1: Sanctions and Incentives

The Organization shall adopt and implement necessary policies to motivate the employees to adopt a security culture through appropriate incentives and dis-incentives built into the policy. The sanctions shall be proportionate to the seriousness of the lapses determined on the basis of the legal consequences arising out of the non compliance

4.2: Work From Home

The Organization shall adopt and implement necessary policies to ensure that there is accountability of individuals from the point of view of information security in the context of the users using their home based computing systems, open internet based connectivity and lack of supervision of the activities of the employee. This could include monitoring apps and special configuration software installed in the user's device and contractually binding the employee under a distributed responsibility concept to be his own IS manager.

4.3: Onboarding, Evaluation and Termination

The Organization shall adopt and implement necessary policies to ensure that employees are considered outsiders before onboarding and post termination. During the term of the employment, appropriate measures are initiated to ensure that the legitimate interest of the organization in terms of security and need for performance evaluation is properly addressed.

4.4: Internet access, Resource usage

The Organization shall adopt and implement necessary policies to ensure that the use of digital assets belonging to the organization shall be adequately monitored to ensure that they are not used for committing any offences or contraventions of law. The assets shall always be secured against presence of malware and unauthorized use. Every digital asset shall be assigned to a recognized owner who shall be accountable for any contraventions committed with the use of that asset.

4.5: Awareness and Training

The Organization shall adopt and implement necessary policies to ensure that all employees and other persons who are likely to access the digital assets of the organization shall be aware of the requirements of compliance and the steps to be taken for the purpose. They shall be provided with adequate training to empower them with the necessary skills and tools.

5.1: Information Classification and Tagging

The Organization shall adopt and implement necessary policies to classify information firstly as personal and non personal. Information shall be further classified as types of personal information personal information as required for compliance of the relevant law. The non personal data is classified on the basis of the severity of the harm that may be caused to the organization in the event of compromise of its security.

5.2: Hardware and Software Purchase

The organization shall implement appropriate policy to ensure that at the time of acquisition of any computer resource used for processing of personal data, it shall be secured against vulnerabilities that may be exploited subsequently.

Shall also ensure appropriate sanitization at the time of disposal of the computer resources when no longer required, to prevent any data leakage.

5.3: Physical Security

The Organization shall adopt appropriate controls to ensure the physical security of the data assets from unauthorized access and loss.

The policy shall ensure that persons in charge of physical security are also part of the overall information security team of the organization.**5.4: Access Control**

5.5: Storage Security

The organization shall adopt appropriate polices to ensure that the personal data in storage is appropriately secured from unauthorized access, modification, and denial of access.

The policy shall ensure that the encryption keys are appropriately managed allowing for contingent requirements arising out of technical or manpower failures.

5.6: Transmission Security

The organization shall implement appropriate policy to ensure that Personal data in transmission is secured.

The policy shall ensure where possible appropriate authentication so that reliability of information in transmission is achieved on an end-to-end basis. Where digital or electronic signature is used, they shall conform to the applicable laws.

5.7: Process Security

The organization shall adopt appropriate measures to secure personal data during processing.

The policy shall ensure that where possible, appropriate measures for encryption even during processing by use of techniques such as homo morphic encryptions are used based on the criticality of the data.

5.8: System updation

The organization shall implement an appropriate policy to keep every system resource updated from authenticated sources.

Policy shall ensure that all system updates are pre-screened for security vulnerabilities from the information security department.

5.9: Incident Management and Data breach reporting

The organization shall adopt an appropriate Techno Legal incident management policy to identify potential and fructified incidents based on the risk of harm to the data subjects, record, and a system to resolve and document the learning created out of the incident.

The policy shall ensure that appropriate knowledge is imparted to the incident gateway managers such as the call centre employees to identify incidents from the legal aspect and initiating appropriate action.

The policy shall be integrated with the Whistle-blower policy for generation of early warnings with appropriate protection for whistle-blowers and prevention of nuisance reports.

The policy shall also ensure appropriate reporting of the data breach as required under law.

5.10: Malware Control

The organization shall implement appropriate measures to ensure that malware infections do not adversely affect the security of the personal data.

The policy shall ensure use of appropriate anti-virus/anti-malware measures including sandboxing of incoming data from unverified sources, prevention of downloading of software from unreliable sources, blocking of unwanted processes and ports from the user's computers, whitelisting and blacklisting of websites etc are built into the system which is kept updated from secured sources.**5.11:**

BYOD

The organization shall implement appropriate policy to secure the access and processing while adopting "Bring Your Own Device" (BYOD) to mitigate the risks that arise thereof

5.12: Data Destruction

The organization shall adopt appropriate policy for deletion of personal data when required using forensic destruction methods.

The policy shall ensure that appropriate documentation of all systematic destruction of data is maintained.

The policy shall ensure that periodical scanning of personal data in the custody of the company is taken up to verify when data destruction needs to be undertaken based on the data retention policy and execute the same in a systematic manner.

5.13: Data Leak prevention

The organization shall initiate appropriate measures to prevent unauthorized exfiltration of data with appropriate detection, prevention, and correction measures.

The policy shall include identification of all suspicious activities including a pattern of unusual activities within the system and at the time of data moving out of the organization.

5.14: Data Retention and archival Policy

The Organization shall adopt and implement necessary policies to ensure that data shall be retained and archived as required under law and appropriate control is exercised against wrongful and premature deletion.

5.15: DRP/BCP

The Organization shall ensure that stored data shall be suitably protected through an appropriate secure disaster recovery system and Business continuity measures.

The policy shall ensure that Data is authenticated before backing up and while importing back from back up to ensure that the data has not undergone any unauthorized modification.

The policy shall ensure that trojans which may lie dormant does not corrupt the backup data by scanning the data before it is re-used.