Data Protection Journal of India

No: 2/2021: 14th **April 2021**

The Era of PDPSI unfolds

Journal published For

Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

Publisher: Na.Vijayashankar

What is Inside

From the Chairman's Desk

The Era of PDPSI

When we launched this journal in the first quarter of 2021 we spoke of the new dawn in India emerging with the FDPPI as the focus.

This copy is dedicated to the raise of another highly significant development in the Indian Data Protection Scenario namely a "Framework" for compliance of data protection laws in the form of "Personal Data Protection Standard of India" or PDPSI.

This is a "Made in India for the World" service that is designed to work along with other frameworks such as ISO 27701 which have descended from a very well known dynasty and have a wide acceptance in the Corporate circles.

However, informed corporate professionals will now have a dilemma whether they have to go to the International frameworks which were designed for a different purpose and have to be adopted for Indian needs or look for an indigenously developed system.

I also urge all HR professionals who write specifications for recruiting DPOs to realize that FDPPI certified professionals come with a far more in depth knowledge in Indian Privacy regulations and global regulations further peppered with internal data audit skills which are not matched easily by other certification systems.

FDPPI awaits the HR and Data protection professionals to look at FDPPI and it's activities with an open mind and understand the long term benefits of FDPPI initiatives.

During this quarter, FDPPI has made further progress in developing the DDMAC services which perhaps will gain further momentum in the coming days.

FDPPI has already created several benefits of Corporate membership which includes privileged provision of services related to Data Protection within a corporate entity.

The Symbol of Compliance

India has moved into an era of Privacy Protection through Data Protection. The Justice Puttaswamy Judgement followed by Justice Srikrishna Committee report, the Draft bill PDPB 2018 and now the draft bill PDPB 2019 as modified by the JPC headed by Mrs Meenakshi Lekhi has brought India to the threshold of a new era where every user of Personal Data is

confronted with the challenge of regulatory compliance of the Personal Data Protection Act of India. Though the passage of the Act has now been put off by atleast one more parliamentary session the passage of the Act is imminent.

The essence of the Act is an establishment of a "Right of a Data Principal to determine how his personal data may be collected, used, shared and disclosed by others".

Since the Act is a seamless continuation of the existing law called Information Technology Act 2000 (ITA 2000) representing the replacement of Section 43A with the new law with nearly 100 sections, it is a representation of "Due Diligence" and "Reasonable Security Practice" as mandated in the current law. The difference would be that in the current law, a person who has suffered a wrongful loss on account of the failure of an organization to comply with due diligence can only invoke a claim for damages as compensation, the new law will have a regulator to monitor the proactive implementation and impose fines for non compliance whether or not there is a data breach or a wrongful loss to any data principal.

In this context, while the Government has so far shown its inclination to pass the law and also show its inclination to implement the law as due diligence as they appear to have done in the NDHM scheme. It is now for the private sector to show its commitment to Privacy Protection by starting implementation of the Privacy Protection principles envisaged in the proposed Act, bit by bit.

FDPPI is conscious of its responsibility as an organization dedicated to the welfare of the Data Protection eco system in India and responded with several initiatives towards making the Indian data processing industry voluntarily adopt a compliance regime.

In this endeavour, FDPPI is releasing a system that guides the industry towards Data Protection compliance through the sponsorship of the "Personal Data Protection Standard of India" . The accompanying symbol of PDPSI has therefore is raising on the horizon as the symbol of Data Protection for a corporate entity.

Let us welcome this raise of the symbol of Personal Data Protection…. And dedicate this issue of the journal to the PDPSI concept.

Collaboration with DNV

We are also proud to announce that FDPPI has entered into a collaboration with DNV to jointly develop Certification systems including a Data Trust Score system.

DNV (earlier known as DNV-GL) is a well known global organization involved in providing digital solutions for managing risk and improvement of safety and asset performance in industries such as oil and gas, and energy management.

DNV is one of the world's leading certification bodies, helping businesses assure the performance of their organizations, products, people, facilities and supply chains and is engaged in conducting all Management Systems (MS) audits including ISO 20000,27001,22301 etc besides Cyber Security maturity assessment and GDPR.

The FDPPI-DNV Data Trust Score system is obviously the first assessment system for data protection compliance in India and perhaps the world. It evaluates a company's implementation of data protection over 50 implementation specifications of PDPSI framework, rates it on a scale of 1-10, assigns some weightages and arrives at the net DTS score.

It is expected that the Data Protection Authority of India will being out its own suggestions in due course on how to compute the DTS and our system will incorporate such suggestions as required.
With this prestigious tie-up FDPPI-DNV will be able to reach out to a large section of the Indian Corporate world and provide a hand of assistance to the regulators in making India a respected Privacy Protected Data Processing country.

Through such measures, FDPPI should help the Data Protection Authority of India and the Government, to re-define the term "Adequacy" in the field of International cooperation for Personal Data Transfers.

In due course, we expect that India will create its own "Data Union" as a group of countries which implement Privacy Protection without surrendering the sovereignty of the nation and collaborate for free movement of data for business purpose.

Naavi

14th April 2021

News Section

From the News Room

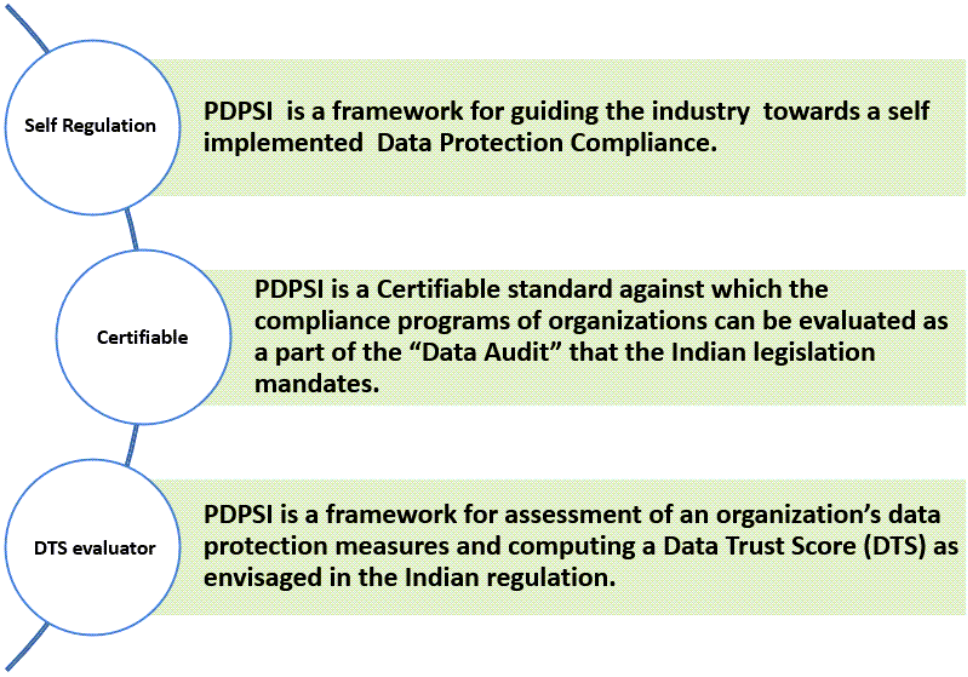
1. MobiKwik, a mobile app company in India was reported to have suffered a personal data breach of about 10 crore data sets which involved the KYC details of the app owners. This is said to be one of the largest data breaches in India. The Company has however denied the breach. RBI has issued a notice to the company to conduct an investigation and report back. In the meantime, the CERT IN may also seek information about the data breach since it is mandatory to report such breaches to CERT In under the ITA 2000/8.
2. China unveiled draft guidelines seeking to limit the scope of mobile apps collection of personal data.
3. The controversy on WhatsApp privacy policy has now been referred to the competition commission since Government has taken a stand that WhatsApp may not be permitted to continue unless the Policy change is withdrawn.
4. US privacy laws are getting more complicated with the introduction of the California Privacy Rights Act (CPRA) to supplement CCPA and also a bill for Federal Privacy law. In the meantime some states like Virginia, Nevada, Maine etc.
5. EDPB adopted guidelines on Connected vehicles.
6. The passage of the PDB 2019 has been put off to the next session of the Parliament.
7. European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) have released a joint opinion with a proposal for Data Governance Act. This act aims at the promotion of reuse of public sector data and strengthening the data sharing mechanism.
8. Breach Clarity, which releases weekly report on data breaches has come up with an algorithm to assign a data breach score on a scale of 1 to 10 depending on the severity. This is similar to the Harm Audit scoring leading to DTS adopted by FDPPI in its PDPSI framework for assessment of data protection compliance.
9. According to Interbrand and Infosys study, the world's top brands across sectors might lose between $93 billion to $223 billion because of a data breach approximately 4 to 9.6 percent of their cumulative value.
10. Ubiquiti, a global IoT device provider announced a data breach that compromised the PII of its customers. The compromised resources include S3 data buckets, every application log and database, and every user database credential.
11. UK is considering forcing Facebook to implement a backdoor to allow security agencies and police to read the contents of messages sent across its messenger, WhatsApp and Instagram Chat services.
12. It has been reported that 533 million Facebook user's phone numbers and personal data have been leaked online. Data belongs to users of 106 countries including over 32 million records on US users, 6 million records of Indian Users.

(For more details, please refer to www.naavi.org or www.fdppi.in)

Knowledge Section

What is PDPSI?

PDPSI stands for “Personal Data Protection Standard of India” and has been in discussion for the last 2 plus years.



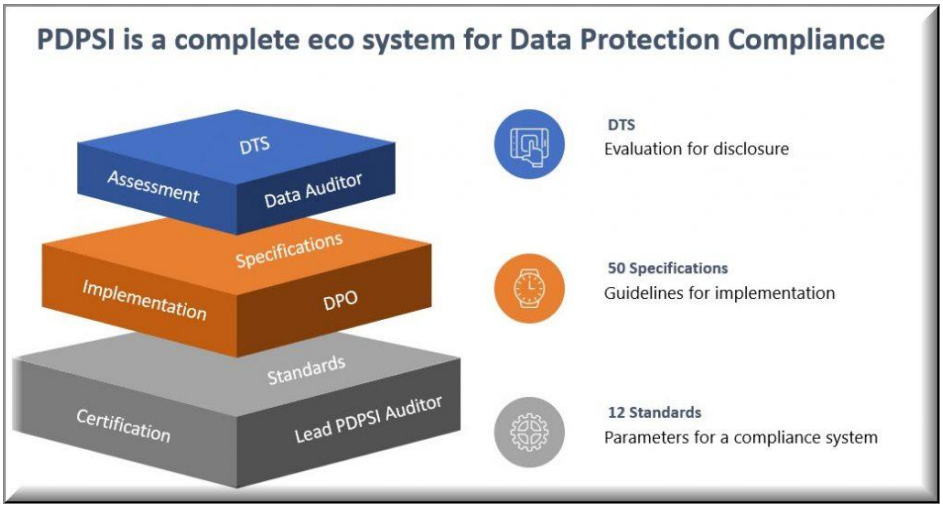
The Origin of PDPSI

At a time where the industry is already having an Internationally recognized Information Security standard in the form of ISO 27001 and an extension thereof in the form of BS10012 and ISO 27701 as Personal Information Management Standard (PIMS), it was found that India needs a “Made in India for the world” standard for Data Protection which is better and more focussed than the available standards which came into existence at a different point of time and for a different purpose.

PDPSI was therefore created to encompass all the best practices prevailing in the industry and to go several steps forward to add new thoughts and bring new focus to the concept of “Protecting Privacy of an individual as a constitutional right” through protecting a “Right of self determination of the individual on how his personal data is collected, used and disclosed”.

The PDPSI is therefore a new approach where the objective is clearly to protect the Privacy of an individual but within a framework of Personal Data Processing environment.

It will take time for the industry to absorb the ideals of PDPSI, understand and appreciate its principles and accept it as a better alternative to other more illustrious brethren who belong to a reputed dynasty.
FDPPI has adopted the **"Personal Data Protection Standard of India" or PDPSI** as a "Unified" framework for compliance of multiple Personal Data Protection laws by an organization.



The PDPSI consists of 12 standards and 50 implementation specifications that cover the entire gamut of PIMS as envisaged by other frameworks and goes further to address the needs of the need to be simultaneously in compliance of multiple global laws incorporating many futuristic thoughts on "Data Business".

This PDPSI framework is not only a "Certifiable Audit Framework" like the ISO 27701 but also an Assessment framework for the Data Trust Score (DTS) system which is a representation of the Personal Data Protection maturity of an organization as assessed by an auditor using the 50 implementation specifications of the PDPSI framework.

PDPSI is also a framework which is available for organizations for self implementation as an instrument of internal audit.

However the symbol shown along side is emerging as the symbol of Personal Data Protection and is the goal of every Data Fiduciary and Data Processor.

This is a symbol of protection for the Data Principal in the context of protection of his Privacy.

It also represents a framework for enabling Privacy Protection through Data Protection.

The accompanying symbol in future will represent an organization which has undergone an assessment of its DTS by a PDPSI accredited auditor.

This could be disclosed by organizations as required under the Indian laws.

The auditors and consultants who have undergone the rigorous training and passed through the Certification exams have been certified by FDPPI and certificates like the following have been issued to them.

These are sample certificates that only the privileged professionals who have gone through the rigorous evaluation process have been issued.

The “Certified Global Privacy & Data Protection Consultant” is a person with a reasonable knowledge of the Privacy laws and a reasonable skill to conduct data protection audits and provide consultancy to organizations in their Privacy Compliance program. The “Certified Global Privacy & Data Protection Auditor” is a person with an accreditation for conducting Audits and DTS assessment which will be registered with FDPPI and issue necessary “Certificate of Privacy and Data Protection Compliance” under the PDPSI framework.

FDPPI congratulates the professionals who have achieved this recognition in the first batch and hope that in future, we will have many more such professionals. They will form the backbone of the Data Protection Culture in India in the coming days.

ISO 27701 Vs PDPSI

An evaluation

"Privacy" is an obligation cast on companies handling Personal information either as part of their employee data or as data collected for business purpose. The Data Protection laws enforce protection of Privacy as an obligation of the corporate sector with a focus on "Collection", "Use", and "Disclosure" of "Personal Data".

The laws mandate that an opportunity should be given to the Data Principals (Data Subjects as they are called in some jurisdictions) to opt out of all collection by default and selectively opt in for collection and further use including disclosure and destruction. If the data principal agrees to provide his/her personal data, the collecting agency, namely the Data Fiduciary (also called Data Controller under some jurisdictions) is required to obtain the necessary consent and use the data accordingly. In certain cases, Consent may be excused or the use may be permitted under legitimate interest or public duty. The laws provide some clarifications on how the employee data or publicly available data may be handled and under what circumstances the data collecting company can presume that there is a consent for collection and processing.

Since there could be subjectivity involved in identifying what are the circumstances under which personal data can be collected and used and also in the interpretation of exemptions available, alternative measures, risk estimation etc., organizations try to look for guidance in the form of "Frameworks". They also would look for external certification of their implementation as an assurance of their implementation.

ISO has therefore come up with its own "Certifiable" frameworks to assist the organizations and these are quite popular in the industry circles. Some times the ISO "Standards" are even confused with "Legal Prescriptions" and companies feel that "If we are compliant with ISO 27701, then we are compliant with Privacy Laws".

The Data Fiduciaries need to realize that "Being in Compliance with law" is different from "Being Certified under a standard". Unless the law adopts a Certification framework as its deemed compliance, the frameworks are guidelines only and the organization should avoid being complacent with the perception that it has a certification and hence it need not do anything more.

All compliance certifications are a view on a particular date and if the organization does not have a continuing effort to maintain the compliance, the non-compliance can be an issue despite the certification.

In this context, if an organization adopts a framework which is different from what is required for a compliance, there would be a further risk of the compliance failing even the due diligence test.

For example, an argument can be extended that a Company compliant with ISO 27701 which is accompanied by ISO 27001 and supported by controls under ISO 27002 is PIMS compliant with any data protection law. The company may wrongly feel that they are compliant with Data Protection law while they are compliant only with an industry best practice.

Further, there is a question whether Certification of the PIMS of a company under ISO 27701 is an endorsement of the compliance of EU- GDPR or Indian PDPB 2019 (when it becomes a law, it will be called PDPA-India and we shall use this term here after).

If GDPR and PDPA-India are identical laws, then compliance of EU-GDPR may also be sufficient compliance of PDPA India. However, the two laws are totally different in terms of its applicability, obligations, some aspects of rights etc., and hence claiming compliance of PDPA-India on the strength of ISO 27701 would be unacceptable as a risk management for the organization.

Additionally, our familiarity with ISO 27001 tends to make it difficult to unlearn the concept of "Protecting Data" from "Protecting Privacy" . We often tend to think in terms of "Data Privacy" being the same as "Information Security" and fail to distinguish "Data Privacy" from "Data Principal's Privacy".

PDPSI (Personal Data Protection Standard of India) was developed to meet the objectives of getting a higher focus on the following:

- **Requirements of protection of the Right of a Data Principal to control the collection, use and disclosure of personal data**
- **Recognize the need for compliance of PDPA India in particular and incorporate the definitional differences with GDPR and differences in exemptions interpretation of legitimate interest, the rights of data principals and obligations of data fiduciaries.**
- **Recognize the possibility of multiple data protection regulations being applicable for a given Data Fiduciary**
- **Recognize the need for a framework that can be extended to computer the Data Trust Score assessment**

ISO 27701 lists 33 controls for use by organizations acting as PII Controllers and 18 controls for PII Data Processors, The guidelines provide that based on the statement of applicability (SOA),certain controls may be excluded if the risks are considered not necessary by the risk assessment.

This is similar to the Model Implementation Specifications in PDPSI out of which some may be excluded based on the "Variance Document" approved by the top management.

ISO 27701 addresses privacy related requirements under EU-GDPR and along with the application of ISO 27001/2 for the personal data as recognized under ISO 27701, PDPSI addresses the requirements of privacy in PDPA India along with the security controls required to protect the personal data as recognized under PDPA.

For example, definition of personal data under EU-GDPR and its applicability extends to

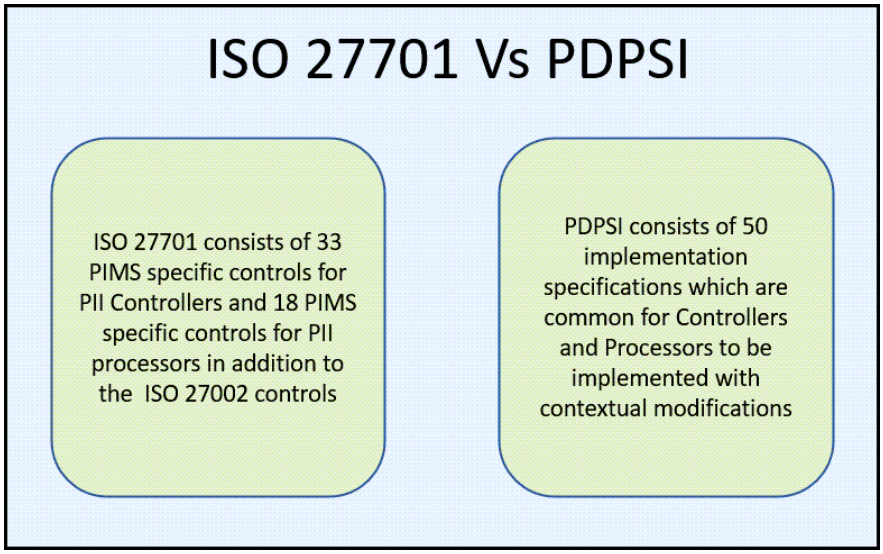
> "Data related to an identified or identifiable data subject and its processing in the course of activity falling inside the scope of the EU law or related to the offering of goods and services to the data subjects in the EU and monitoring their behaviour."

On the other hand, the Indian Data Protection Act applies to

> "Data about or related to a natural person collected disclosed, shared or otherwise processed within the territory of India and data processed outside India by Organizations established within the laws of India subject to exemption available and for processing involved in connection with business in India and profiling of data principals within the territory of India."

It is clear from the above that the applicability of the two laws namely EU-GDPR and Indian PDPA are different and hence ISO 27701 and PDPSI have to be considered different.

PDPSI is structured in a unique way where the application of the framework is "Data Oriented" and hence there is an inbuilt customization of PDPSI controls for different sets of data. Accordingly, PDPSI-IN controls apply to data which come under the provisions of PDPA India while PDPSI-GDPR controls apply to data which come under the provisions of EU-GDPR.



PDPSI has 50 implementation specifications that cover all the PIMS specific controls of ISO 27701 and the ISMS controls of ISO 27002 as applicable to the subject data.

PDPSI also incorporates the following controls which are not covered under the ISO 27701.

a) Augmented Whistle-blower
b) Data Valuation and Accounting
c) Senior Executive Development
d) Regulatory agency relationship
e) Business Acceptance

PDPSI is more management oriented than technology oriented and hence has controls distributed over multiple responsibility canters in the organization.

The PDPSI Certification audit is inclusive of a DTS (Data Trust Score Assessment) which requires an assessment on the entire 50 implementation specifications provided as a "Model" in the standards.

The Certification under PDPSI follows the principle of an option to be given to the organization for "Risk Absorption". To accommodate this "Risk Absorption" aspect, organization are required to create an implementation charter which could include a management decision to opt out of a few of the Model Implementation Specifications with a documentation of "Variance" explaining the logic for the omission.

The Certification would be based on the binary evaluation of the adopted implementation specifications but the DTS assessment is based on an evaluation of each of the model implementation over a sliding scale, followed by a grouping and group weightage system.

The Certification of an organization as "Privacy Compliant as per PDPSI framework" would be registered with the sponsoring organization namely FDPPI and the DTS score would be taken on record. The DTS of an organization as computed by the auditor would be published with the consent of the organization or when it is disclosed publicly by the Data Protection Authority. Before confirming the registration, a feedback is obtained from the auditee organization so that in case of a major variance of the auditor's evaluation and the Company's own assessment, a review audit can be organized.

As a result of the above, PDPSI based audit is several notches higher than an ISO 27701 though PDPSI is a relatively new introduction. Presently FDPPI has certified 21 professionals who may provide consultancy and/or audit based on the PDPSI.

It may be observed that PDPSI is comprehensive enough to cover ISO 27701 and 27002 and expands the scope of the compliance to all aspects of the enterprise activity from Management, DPO, Legal, HR and Technical. These groupings are also relevant for the DTS evaluation that PDPSI provides.

The detailed explanation of the specifications is out of scope of this article. The list of controls recommended in ISO 27701 Vis a Vis PDPSI is available in the annexure.

(P.S: Those who are interested in getting more details, may contact FDPPI)

Naavi

Annexure

PIMS specific controls for PII Controllers under ISO 27701

Conditions for Collection	
1	Identify and Document Purpose
2	Identify Lawful Basis
3	Determine when and how Consent is to be obtained
4	Obtain and Record Consent
5	Privacy Impact Assessment
6	Contracts with PII Processors
7	Join PII Controller
8	Records related to Processing PII
Obligations	
9	Determining and fulfilling obligations to the PII principals
10	Determining information for PII principals
11	Providing information to PII Principals
12	Providing mechanism to modify or withdraw consent
13	Providing mechanism to object to PII processing
14	Access, Correction and/or Erasure
15	PII Controller's obligations to inform third parties
16	Providing copy of PII processed
17	Handling requests
18	Automated decision making
Privacy By Design and Privacy by Default	
19	Limit Collection
20	Limit Processing
21	Accuracy and Quality
22	PII Minimization objectives
23	PII de-identification and deletion at the end of processing
24	Temporary files
25	Retention
26	Disposal
27	PII Transmission controls
PII Sharing, transfer and disclosure	
28	Identify basis for PII Transfer between Jurisdictions
29	Countries and international organizations to which II can be transferred
30	Records of transfer of PII
31	Records of PII disclosure to third parties
32	Records of Transfer of PII
33	Records of PII disclosure to third parties

PIMS specific controls for Processors under ISO 27701

Conditions for Collection and Processing	
1	Customer Agreement
2	Organizations purposes
3	Marketing and advertising use
4	Infringing instructions
5	Customer Obligations
6	Records related to processing PII

Obligations to PII principals	
7	Obligations to PII Principals
Privacy by design and default	
8	Temporary files
9	Return, transfer or disposal of PII
10	PII transmission controls
Sharing, transfer and disclosure	
11	Basis for PII transfer between jurisdictions
12	Countries and international orgnaizations to which PII can be transferred
13	Records of PII disclosure to third parties
14	Notification of PII disclosures to third parties
15	Legally binding PII disclosures
16	Disclosure of sub contractors used to process PII
17	Engagement of a sub contractor to process PII
18	Change of sub contractor to process PII

The PDPSI system is a common framework both to Controllers and Processors and has the following 50 implementation specifications.

Implementation Specifications under PDPSI

Management Specific

No	Description
1	Data Protection Committee Constitution
2	DPO Designation
3	Risk Mitigation Charter
4	Augmented Whistle-blower
5	Data Audits
6	Data Valuation and Accounting
7	Senior Executive Development
8	Communication Management
9	De-Identification, Pseudonymization and Anonymization
10	Distributed Responsibility
11	Data Disclosure
12	Privacy By Design
13	Business Acceptance
14	Business Associate Approval
15	Regulatory Agency Relationship

DPO Specific

No	Description
16	Organizational level Privacy Policy for Data Protection
17	Notice and Consent Form
18	Profiling
19	Legitimate Interest and Exemption Claim
20	Protection of Rights of the Data Principal/Subject
21	Data breach Audit and Notification
22	Cross Border Data Transfer
23	DPIA
24	Documentation and Record keeping

Legal Oriented

No	Description
25	Contract Control
26	Grievance Redressal

HR Oriented

No	Description
27	Employee Privacy Management
28	Augmented HR Policy with Incentivisation and Sanctions
29	Asset Responsibility
30	Work from home

Technology Oriented

No	Description
31	Record of Processing
32	Discovery, Consent tagging and Inventory of Personal Data
33	Classification of Personal Data from compliance perspective
34	Legacy and Publicly Available Personal Data Processing
35	Unstructured Personal Data Processing
36	Access Control
37	Data Storage and Security
38	Transmission Security
39	Processing Security
40	Malware Control
41	System Updation
42	BYOD
43	Data Destruction
44	DRP/BCP
45	Incident Management
46	Data Centralization
47	Data Leak Prevention
48	Hardware purchase/Sale and disposal
49	Application Sourcing
50	Physical Security

Data Protection Officer Required

While the legal community and the technical community are burning midnight oil to understand the personal data protection legislation in India, some companies have started recruiting "Data Protection Officers". Since HR professionals are involved in identifying and at least short listing the candidates, it is essential that they need to have a fair understanding of the requirements of a DPO.

Last year, one of the major Banks in India released a recruitment advertisement for appointing a DPO on a 2 year contract basis to be stationed in Mumbai.

The defined roles and Responsibilities were

- Ensuring Bank's compliance with the data protection & privacy legislation **in India** and other countries.
- Develop and manage Bank's **data protection strategy in India**, including the development and implementation of Bank's data protection policy and procedures
- Undertake periodic data protection audits or reviews, including all relevant manual filing systems, archived systems and back up data, in order to ascertain Bank's compliance with data protection legislation.
- Undertake necessary measures to rectify any deficiencies identified by the audit.
- Conduct data privacy impact assessment (DPIA)
- Submit reports on data privacy laws to the Board.
- Collaborate with supporting functions (Legal, IT & InfoSec, Compliance etc.) to stay up to date with new processes and policies.
- Maintain records of processing operations [Personally Identified Information (PII) & Data flow Diagram (DFD)].
- Provide education, training and awareness to all staff members on the requirements of data protection. legislations and care & handling of personal data to ensure that relevant business functions are made aware of both their legal responsibilities as well as steps to be taken for their compliance.

- Provide advice on development of new IT systems & procedures, drafting of data protection notices, obtaining consent from data subjects and operation of the HR function.
- Put in place processes & procedures to deal with data subject access requests and provide assistance & advice in respect of such requests.
- Provide advice and assistance for managing data breaches (if any), including liaising with the Supervisory Authority on behalf of the Bank.

The Key responsibility areas were defined as follows:

- Compliance to data privacy & related regulations in India & in its foreign offices at various jurisdictions.
- Relevant and timely updates on DP matters to senior management.
- Putting in place and communicating the policies and procedures.
- Deployment of relevant communications and training.
- Discuss with Operational Risk Department to ensure that risks are documented; controls are put in place; and monitoring/ testing is carried out.
- Data flows and data inventories are in place and are up to date.
- Complete the Privacy Impact Assessments, wherever required.
- Review and updating of documented risk assessment and plan as required.
- Timely, robust responses to authorities, data subjects etc.
- Delivery of prompt and accurate advice to the business.
- Interpreting and operationalizing regulatory directives.

The responsibilities rightly envisaged that the position reported to the top management and included multiple skills. The specific skills required were listed as

- Highly developed specialist knowledge in the General Data Privacy Regulation underpinned by theory and experience.
- Evidence of continuing professional and/ or personal self- development.
- Expert knowledge of data privacy laws and practices.
- Exposure to Data Privacy laws & regulations such as General Data Protection Regulation ("GDPR"), UK Data Protection Act 1998 etc.
- Knowledge of Information lifecycle, risk management & data security areas.
- Extensive knowledge of Information Governance disciplines.
- Skill of interpretation of national guidance and legislation and subsequent local implementation.
- Flair for managing staff and implementing budgets. Training Delivery.
- Capacity to work with cross functional teams, attention to detail, organizational skills and multitasking.
- Strong management, motivational & leadership skills with ability to drive large change management programs within organizations.
- Ability to maintain confidentiality and deal with situations in a sensitive manner.

- Ability to communicate across all organizational boundaries in an appropriate manner.

While the identification of the required skills and the role responsibilities were reasonably elaborate, the advertisement recognized the “UK Data Protection Act 1998” but failed to recognize the Indian “Information Technology Act 2000/8” (ITA 2000/8)or the proposed “Personal Data Protection Bill 2019”.

Accordingly the preferred professional certifications required were listed as

- Certified EU GDPR Foundation,
- CIPP (Certified Information Privacy Professional),
- CIPT (Certified Information Privacy Technologist),
- CIPM (Certified Information Privacy Manager) etc

While it is understandable that the recruiting institution was having international operations and hence it was necessary that knowledge of EU-GDPR was essential, the recruitment advertisement failed to recognize that there are privacy laws of different hue and colour in hundreds of other countries besides India itself.

If the DPO is an expert in EU GDPR, it does not mean that he would be a good DPO in the Indian scenario.

In order to frame the responsibilities of a DPO in India, we need to recognize that the most preferred qualification is some thing related to Indian data protection laws. At present there is no qualification other than the FDPPI’s Certifications in Module I, Module G and Module A that are designed exclusively to meet the requirements of organizations in India with international operations.

It is possible that who ever drafted the recruitment advertisement was not aware of the existence of FDPPI and knowledge of its activities.

But it is the duty of a good HR professional to understand the developments in India both in terms of the requirements of a DPO and also what kind of trainings and skill development programs are available in the given profession.

India already has ITA 2000/8 and any person who does not know ITA 2008 compliance and more particularly the impact of Section 43A, Section 72A, Section 79 and the Intermediary rules, Reasonable Security practices etc would not be fit to hold the place of a DPO.

Section 43 A of ITA 2000 which currently codifies the “Sensitive Personal Data Protection“ in India, and Section 79 with all the associated rules which codify the “Personal Data Collection and use restrictions” and the Justice Puttaswamy judgement are essential knowledge for a DPO. The PDPB 2019 is the due diligence under Section 43A and Section 79 and hence must be considered as currently effective guideline for Personal Data Protection in India.

Any recruitment advertisement for a DPO position which ignores the Indian laws is therefore indicative of the lack of understanding of the requirements. It is also an insult to the

professionals who have already upskilled themselves with the knowledge of the Indian laws in anticipation of the upcoming law.

The PDPB 2019, Section 30 speaks of the requirement of a DPO and states

Section 30. Data protection officer.

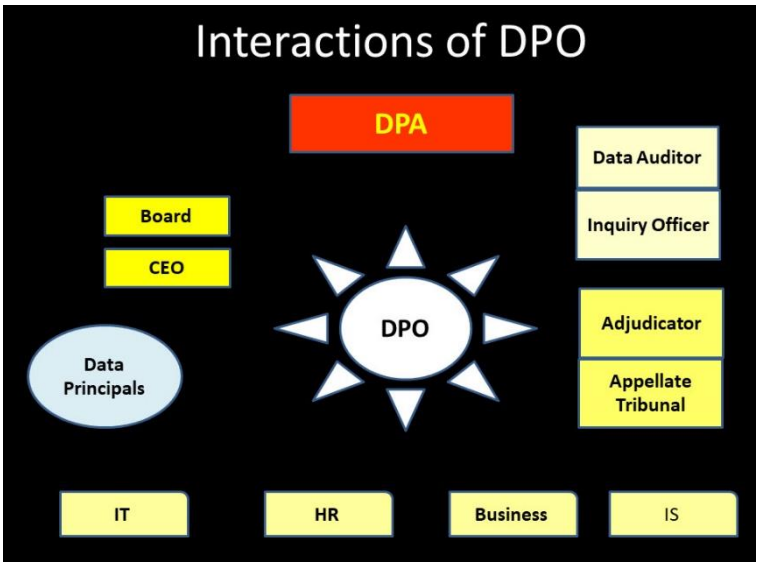
(1) Every significant data fiduciary shall appoint a data protection officer possessing such qualification and experience as may be specified by regulations for carrying out the following functions—

> (a) providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act;
> (b) monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act;
> (c) providing advice to the data fiduciary on carrying out the data protection impact assessments, and carry out its review under sub-section (4) of section 27;
> (d) providing advice to the data fiduciary on the development of internal mechanisms to satisfy the principles specified under section 22;
> (e) providing assistance to and co-operating with the Authority on matters of compliance of the data fiduciary with the provisions under this Act;
> (f) act as the point of contact for the data principal for the purpose of grievances redressal under section 32; and
> (g) maintaining an inventory of records to be maintained by the data fiduciary under section 28.
>
> (2) Nothing contained in sub-section (1) shall prevent the data fiduciary from assigning any other function to the data protection officer, which it may consider necessary.
>
> (3) The data protection officer appointed under sub-section (1) shall be based in India and shall represent the data fiduciary under this Act.

Accordingly, the DPO must be fully conversant with the Indian law. While the knowledge of GDPR etc is useful, lack of knowledge of Indian law cannot be excused. Often professionals trained in GDPR who does not recognize the differences with the Indian law commit grave errors of perception because they are not able unlearn certain concepts of GDPR which is essential to learn the Indian law. The role of a DPO in India has to take into account the types of interactions envisaged under the Act for the DPO.

The DPO will have three distinct types of interactions namely

1. Internal
2. External with regulatory agencies and Data Auditors
3. External with Data Principals



The Internal interactions involve working with multiple disciplines such as the CISO, CTO, CCO, HR, the Legal team etc. The DPO has to coordinate the activities and advise the different divisional heads.

The responsibility of a DPO includes assisting the regulatory agency or the external Data Auditor. and this involves taking up positions which should be independent of the CEO of the organization.

Dealing with Data Principals is another challenge involving dispute resolution skills.

Unless the recruitment specification captures the requirements including

a) Knowledge of Data Protection Laws
b) Understanding of Technological processes
c) Skills of negotiation with peers, superiors, regulatory agencies, and the public

The ideal candidate is difficult to find.

The Preferred Certifications need to be evaluated in this context and at present there is no challenge to FDPPI's certification programs in meeting these requirements. Particularly those professionals who have completed all the three certifications are the best suited professionals to don the role of DPO.

There are presently 23 professionals who have completed all the certifications they form the core of the Indian Data Protection Compliance system at present. Most of these professionals may not be available for recruitment since they may be already associated with some

companies. But soon this group of 23 will expand and more people should be available in the market.

More than 64 persons have been certified by FDPPI on Indian laws and more than 30 of them have also been certified for International Data Protection laws. Many of these will soon also complete the Audit module and join the Elite group of 23.

FDPPI has a scheme of "Talent Exchange" to assist organisations to identify DPO talents and also runs a mentoring program with a crash preparation for any body who are intending to take up a DPO interview shortly.

Hopefully the efforts of FDPPI will result in the availability of rightly qualified data protection professionals who can assist organizations towards better compliance.

The HR professionals need to take note of these developments before their next round of recruitments of DPOs. In the light of the above, a typical job specification may be as shown below:

FDPPI invites HR Professionals to get acquainted with the Personal Data Protection law so that they may be able to identify potential DPO candidates within their own organization who can be promoted to fit into the role or to recruit the appropriate candidates from outside.

Such a training would also be useful for HR professionals of large organizations where the number of employees themselves may be large enough to consider that the head of HR operations is a DPO himself for the employees including applicants of jobs.

Law?

For Me?

Knowledge of Data Protection Laws will be critical to the success of any professional in an organization and not limited to the Technology related professionals.

HR professionals, Legal Professionals can effectively compete with the CIOs, CTOs, CISOs or CROs to take up the important responsibility of a DPO

Knowledge is Power. Let us acquire it when there is an opportunity

A typical DPO Recruitment Advertisement

Job Description:

- DPO is the single point of contact in the organization for all external agencies including the regulatory agencies and data principals in relation to any matters concerning Personal Data Protection.
- Internally, DPO shall be responsible for the enterprise level Privacy and Data Protection in compliance with the applicable laws.
- DPO shall administratively report to the CEO but shall provide periodical feedback to the Board of Directors on the Data Protection status of the organization.
- DPO shall lead the development of short, medium and long term strategy to keep the organization compliant with the applicable data protection laws.

Responsibilities

- Ability to conduct a Risk Assessment at organizational level to identify exposure to different data protection laws in India and other countries.
- Ability to develop, review and maintain Privacy By Design Policy for the organization.
- Ability to analyze, identify and assess business processes, & business risks associated with lifecycle of data and taking pragmatic steps to address and mitigate such risks & liability proactively thereby protecting Company's interest or alternative approach as per company's policy
- Ability to monitor the activities of the organization and
    - Identify the need for and conduct harm audits as and when necessary
    - Identify the requirement for and supervise the conduct of the Data Protection Impact Assessment (DPIA).
    - Identify the requirement for and supervise the conduct of Data Breach Audits as and when necessary
    - Conduct periodical internal compliance audit and Data Trust Score assessments
- Ability to coordinate with external Data Auditors regarding annual or other regulatory audits
- Ability to coordinate with the Data Protection Authority for registration, submission of Privacy By design policy, DPIAs and any other exchange of information.
- Ability to receive and resolve complaints from Data principals
- Ability to develop necessary policy documents for different activities of the organization required for compliance with law covering the collection, use, storage, processing, disclosure and destruction of personal data.
- Ability to draft and develop necessary policies on mitigation of risks including strategies for anonymization, de-identification, pseudonymization etc

- Ability to maintain all records related to processes, risks, risk mitigation efforts, correspondence with regulatory agencies and the data principles, and any other matter required for compliance of data protection laws as applicable.
- Ability to ensure development of a necessary Privacy Protection culture in the organization in association with the HR department and ensure protection of privacy for all employees, including conduct of training programs, providing guidance on employee recruitment, management, and termination policies etc.
- Ability to guide the technology department to ensure that all necessary measures are undertaken to remain compliant of the applicable data protection laws.
- Ability to coordinate with the law department to monitor all contracts involving personal data processing and ensure they remain compliant of the applicable data protection laws.
- Ability to undertake any other activities that may be necessary to ensure that the organization always remains compliant of the applicable data protection laws.

Qualifications and Experience

- The preferred candidate shall possess Techno Legal qualifications and Professional qualifications that are commensurate with the requirements of the job responsibilities as above.
- Certifications focussed on skills and knowledge of data protection laws applicable in India would be preferred.
- Shall possess a minimum of 5 years of relevant experience including in the field of Privacy and Data Protection laws and related Technology.
- Knowledge of Information Technology Act 2000 and Personal Data Regulations in India critical.
- The ideal candidate will have knowledge of law and technology, skills of dealing with people possessing a high degree of communication skills and a self driven leader.

Finding a door when everybody sees a wall is the key quality required of the candidate.

Age no bar. Remuneration commensurate with the skills.

Reminiscences of a Privacy Aware Professional

Shalini Varanasi

Carrying my own privacy shield…

Data Privacy is the talk of the town among the users of services - for their privacy rights, and among the service providers - for their obligations under the respective data protection laws. The service providers seek to meet the compliance requirements in a cost effective manner, while the users want their rights protected.

Like everybody else, now before using a service or an App, I start going through the privacy policies and terms & conditions, examining them to ensure that all my rights are protected. Once while going through terms and conditions of a messaging app, I was shocked to read that the organization without mincing words was telling me that *I will be responsible* for maintaining confidentiality of my account credentials and other sensitive information.

At that time, I had just started exploring the privacy field and my focus was on deciphering the obligations *that organizations have to comply with*. Like, keeping the data secure from unauthorized access. Therefore my reaction was that this particular organization failed to understand their *responsibility* as per the data protection principles. But at the same time I had to revisit my understanding, as the organization in question has been in the field for more than a decade and quite well known for building communication and collaboration apps.

Allow me to share the above referred terms in little more detail, it said:

I will be responsible for keeping 'my device and my account' safe and secure. (Totally makes sense, thumps up!)

I will be responsible for all activities that occur in my user account and I needed to agree to inform the App immediately of any unauthorized use of my user account by email. (This too sounded absolutely reasonable.)

Now, comes the part, where I feel the App is not accepting its role in protecting my privacy as a user. *The terms mention that the app will not be responsible for any loss or damage to me or to any third party incurred as a result of any unauthorized access and/or use of my user account, or otherwise. Moreover, I did not find* any mention of data security provision by the App for user data.

Now, If I choose to go ahead and use this particular app then I will have to carry my own privacy shield, which I am sure will be a weak one without the provision of security infrastructure backing that a resourceful service provider could otherwise guarantee.

P.S: Most banks in their Terms state that the customer is responsible if the password is unauthorizedly used. This almost amounts to giving an indemnity for a Cyber Crime and it is doubtful if the law supports it….. Naavi

DATA PRIVACY LAWS | RIGHT TO BE FORGOTTEN

Sneha and Anupam Prasad

(Sneha is an intern and Anupam Prasad is the Founder, Partner, AP Law chambers)

In today's world of interest and convenience to its access, the six degrees of separation, as was once known, has now been reduced, perhaps not more than two / three degrees of separation. This is primarily due of so much of data being present in the cyber world and continuous data mining happening every single moment. Once a person's data is published on the web, it gets difficult to get that data removed in the absence of stringent laws. The data that has been published online becomes publicly available on the web and is potentially harmful for the person's reputation, his identity, his relationships and his status in society, especially, if the personal information is not authentic or is put on the Internet without the person's consent. With the concept of right to be forgotten, some succour may be sought to address this data dilemma highlighted above.

What is the right to be forgotten?

The right to privacy and protection of data and the right to be forgotten are the two sides of a coin. It is the right of a person to get his personal information removed from the Internet. The right to be forgotten allows a person to remove his name, pictures, contact details or any other personal information that might hamper his reputation or cause defamation from the search results.[1] It is also known the right of erasure which means that an individual has a right to get his personal information permanently erased or deleted from the Internet. However, there exists certain limitations to events under which the right to be forgotten can be exercised.

History and Origin

The right to be forgotten stems from the right to privacy. Its origin can be traced to the European nations that have strict policies and laws for personal data protection. Article 8 of the European Convention for Human Rights (ECHR) adopted in 1950 mentions the right to privacy.[2] The Article gives the right of respect to every person's private and family life, home life and correspondence life.[3] The International Covenant on Civil and Political Rights also talks about the right to privacy under Article 17. It states that there should neither be interference with an individual's privacy nor should there be any unlawful attacks on the person's honor or reputation.[4] Under these conventions, the right to be forgotten can be inferred from the right to privacy. In 1955, the European Parliament passed a data protection directive.[5] In Article 6(1)(e) of this directive, it was mentioned that personal data should be kept in such a form that allows the data to be identified only till the time it is necessary to achieve the purpose for which it was collected. Article 12(b) talks about the erasure or blocking of data that does not comply with the provisions of the directive.[6] However, people started acknowledging the right to be forgotten in 2014 when the Google Spain decision on the right to be forgotten was decided by the European Supreme Court. In 2016, a new data protection and privacy legislation, the General Data Protection Regulation (GDPR) was adopted by the European Parliament. It includes the right to be forgotten.

Right to be forgotten under GDPR

The right to be forgotten has been codified for the first time in the General Data Protection Regulation. Article 17 of the GDPR lays down provisions for the right to erasure or be forgotten.[7] As per the Article, the data subject or the person whose data has been collected has the right to demand the erasure of his person data from the data controller in any of the following conditions:

1. Where the data has already served the purpose for which it was collected and it is no longer necessary to keep the data intact.
2. If the data subject withdraws their consent to the processing of data.
3. When the data subject makes an objection to the processing of data and there is no reasonable or legitimate excuse to deny the objection.
4. If the data of the subject has been processed in an unlawful manner.
5. Data collection and processing of an individual who is below the age of 16 years is lawful only if the parent or the guardian of such person has provided the consent. When the person attains the age of 16 years, they can exercise their right of erasure.

If any of the above-mentioned conditions are met, the data controller will have to take necessary steps with the help of technology to erase such personal data for which the consent has been withdrawn or has been processed unlawfully. The controller will also inform other controllers that the data subject has withdrawn his content and wants his personal data to be erased.

However, the right to be forgotten under the GDPR is not absolute. It is subject to certain conditions. A data subject cannot exercise his right to erasure in the following cases:

1. When it is necessary to process personal data to uphold the freedom of expression and the right to information.
2. When such data is necessary to comply with the legal obligations for a task that is carried out to further public interest.
3. If it is necessary for public health.
4. If the data is necessary to conduct scientific, historical or statistical research.
5. To exercise, establish or defend any legal claims.

The Google Spain Case

The right to be forgotten was established in the landmark case of Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González.[8] In this case, the European Court of Justice interpreted the relevant provisions of the European Data Protection. Directive and held that the data subjects have the right to ask the Search engines to remove their personal information from appearing on the results when their name is typed. The suit was filed before the court by a Spanish national, Mario Costeja González. He claimed that whenever his name was typed on the Google search engine, a web page from a Spanish newspaper appeared in the results that connected his name with a case of recovery of a social

security debt. He filed a complaint with the Spanish Data Protection Agency requesting the removal of the webpage of the Spanish newspaper. Along with that, he also made a request to Google Spain to erase or delink his other personal information from appearing in the search results of the Spanish newspaper's webpage. The agency did not take an action on the complaint on the grounds that such information was necessary for public interest. However, the request made to Google Spain for hiding the name in the search results was accepted. Google then appealed before the court that data operators or search engines do not come within the ambit of data controllers as specified in the Data Protection Directive. The main question that arose before European National High Court was, whether the data operators can be considered as data processors under the Directive and whether they should be asked to remove or conceal information. The Court had held that the data operators are to be considered as controllers according to the relevant provisions of the directive. Along with that, the data subject also has the right to ask the data operators for removal or concealment of his personal data that obstructs his fundamental rights. The data operator will be obliged to remove the links associated with the data subject. However, while considering this request, it is pertinent that the freedom of expression and right to information are not infringed.[9]

The judgment received a lot of criticism on several grounds. People argued that the right the privacy was upheld over the right to information. The second point of criticism was the data operators are being given an uncensored right to publish and conceal information.[10]

Even though the judgment passed in this case was celebrated as the establishment of the right to be forgotten on a superficial level, the actual interpretation of the court was not concerned with the removal of information from the public domain but rather concealing the said information by removing the links that takes an internet user to that web page.

Justice B.N. Krishna Committee

While the GDPR governs the privacy laws in the European Union, there is no specific privacy law regime in India. The Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 govern the protection of data. To frame a specific legislation for data privacy and protection, a ten-member committee was appointed by the Government of India in July 2017 for the purpose of identifying key issues concerning data protection in India and the ways to tackle those issues.[11]

The Committee was headed by the retired judge of the Supreme Court, Justice B.N. Krishna, and was named as the Justice B.N. Krishna Committee. It prepared an exhaustive report on the same and submitted it in 2018. The Chapter 5 of this report lists down the purported rights of the data principal. Among other rights such as the right to access data, confirmation of processing, the right to object to the processing of data, the Committee also included a standalone right to be forgotten.

It stated that the right to be forgotten included the right to de-link, limit, correct or delete the data principal's personal information that is available on a public domain online. The information should be irrelevant, misleading or embarrassing. When the data principal's collected personal information becomes illegal or unwanted after a specific time frame, they

have the right to demand that the data should not be disclosed anymore. The data principal also has the liberty to withdraw his consent to publish personal information on a public domain at a later stage. The said information should then be removed from the Internet. The Committee also suggested that the right to be forgotten should be exercised in accordance with the freedom of expression and the right to information.

Right to be forgotten under the Personal Data Protection Bill.

The right to privacy and the right to be forgotten are the two sides of the same coin. The right to privacy was confirmed as a fundamental right under Article 21 of the Indian Constitution in the case of **K.S. Puttaswamy v. Union of India.**[12] The apex court states that, " One aspect of privacy is the right to control the dissemination of personal information. And that every individual should have a right to be able to control exercise over his/her own life and image as portrayed in the world and to control the commercial use of his/her identity." The Supreme Court said that Privacy is based on the autonomy of an individual. It means the reservation of a private space for the individual. It includes the right to be let alone.

The Justice B.N. Srikrishna Committee recommended the formation of a legislation for the protection of personal data. The Personal Data Protection Bill[13] was introduced in the Parliament in 2018. It is yet to become a law. Chapter VI of this Bill stipulates the rights of Data principals. The right to be forgotten is mentioned under Section 27. It states that a data principal shall have the right to restrict the disclosure of personal information by a data fiduciary or to prevent it entirely. The data principal can exercise his right to be forgotten in the following cases:

1. When the personal data collected has served its purpose and is no longer necessary.
2. When the data was collected through consent and the data fiduciary withdraws its consent
3. If the data violates any provisions of the Personal Data Protection Act, or any other law.

However, the right to be forgotten can only be exercised when an Adjudicating Officer appointed under the Act finds that the right to information and the freedom of expression of other people override the right to privacy. To arrive at this conclusion the officer would have to consider several factors such as the sensitivity of information, whether the data is relevant to the public, to what extent is the data disclosed, and the data principal's role in the public sphere. For this purpose, the data principal will have to file a request to the data fiduciary in writing explaining the identity of the data principal.[14]

Indian jurisprudence – Right to be forgotten

Despite the fact that the Right to be forgotten is not specifically mentioned under any existing law in India, the courts, at several occasions, have acknowledged the right to be forgotten and given judgments in the favour of the aggrieved person. In the recent case of **Subhranshu Rout @ Gugul**[15] **v. The State of Odisha,** the Odisha High Court refused to grant bail to an accused in a sexual assault case. The accused has recorded the sexual assault on the victim and posted it on social media platform. The Court recognized the right to be forgotten and

called for a debate on the same. It was stated objectionable photos and videos of victims of sexual assault on the Internet without any effective mechanism for its removal is a grave concern.

The Delhi High Court has also given a judgment recognising the right to be forgotten. In the case of **Zulfiqar Ahman Khan v. Quintillion Business Media and Ors.,**[16] respondents claimed that they had received harassment complaints during the #Metoo movement against the plaintiff (who is a renowned person in the media). As a result, they wrote two articles defaming the plaintiff. The plaintiff filed suit for a permanent and mandatory injunction against the respondents from publishing the articles online. The court recognised the plaintiff's right to privacy, and stated that the right to be forgotten and the right to be left alone are inherent aspects of the same. The court restrained the republication or circulation of the articles.

In the case of **Name Redacted v/s The Registrar General & Ors,**[17] a woman had filed a FIR against her husband on the grounds of forgery, forceful marriage and extortion and filed a suit for rendering the marriage void. A separate injunction suit was also filed against the husband. The father of the woman later approached the Karnataka High Court requesting the removal of her name from all the cases because on searching for her name on Google, several disputes will show up in her name thus tarnishing her reputation and will cause difficulty for a remarriage. The Karnataka High Court accepted the petition and recognized the right to be forgotten. The Court ordered that the name of the women would be redacted from all the cases filed by her.

However, the Gujarat High Court has posed a contrary opinion on the right to be forgotten. In the case of **Dharamraj Bhanushankar Dave v. State of Gujarat and Ors**.,[18] the petitioner was an accused for several offences in a case of culpable homicide amounting to murder. Even though he was acquitted and the judgement was made unreportable, it was published by an online Judgement repository. Therefore, the petitioner approached the Gujarat High Court for the restraint on publication of the judgment. The Court dismissed the petition on the grounds that publishing a judgement online does not amount to reporting and that the publication does not amount to the violation of his right to life and liberty. The court refused to acknowledge the right to be forgotten in the present case.

Difficulties in exercising the Right to be forgotten

While the right to be forgotten is enforced in the European Union under the GDPR and has also been acknowledged by the Indian courts, there still springs a debate now and then. There are several points on which the laws are silent.

1. **When the right to be forgotten can be exercised-** Does right to be forgotten only includes data that causes defamation or harms the reputation of a person or even in general cases where a person does not wish any of his information to remain in the public domain such as pictures or interviews of celebrities or pictures clicked at any public occasion. Even if the right to privacy is not infringed, whether the right to be forgotten can still be exercised remains unclear.

2. **Data can be traced-** Data leaves it traces somewhere or the other. Even if the information is de-linked from the search engines or restricted from disclosure, it is still present on the Internet and can be traced by professionals or hackers. This causes a grave concern for the data principals.

3. **Clash with freedom of expression and right to information-** There always lies a conflict between the right be forgotten and the right to information and freedom of expression. The right to be forgotten is not absolute. It can only be exercised to the extent that it does not violate the freedom of expression and right to information of the general public. Under GDPR, the right to be forgotten cannot be exercised if the data has been college for public interest. The Data Protection Bill, 2018 also states that the right to be forgotten will not be exercised if it infringes the freedom of expression or right to information. If the right to be forgotten is exercised, the other person's right to information will prevail over the former. It does not make the right to be forgotten an absolute right.

The importance of data and relevance on our individual lives, in today's day and age can certainly not be undermined, as it is often quoted that 'Data is the new oil'. Data is being used to influence and even determine our behavior, our social standing, our financial standing, etc.

The Data Protection Bill restricts or prevents the disclosure of personal data for which the consent has been revoked. However, in cases where consent has not been provided, there is no mechanism for the removal of personal information. The Bill also does not expressly state the removal of personal data from the Internet. Even if the bill is passed, there will be a lag in proper implementation of the right to be forgotten or removal of data from the public domain.

In the case of Name Redacted v Registrar General,[19] the order issued by the Karnataka High Court has not been implemented effectively because the name of the woman can be seen on several websites. The courts have time and again recognized the right to be forgotten and also acknowledged the need for a robust mechanism for removal of information from online platforms.

Therefore, while the right of privacy has been recognized as a fundamental right of the citizens, and extension of that also the right to be forgotten, for which the citizens should have unbridled right, subject to equitable and reasonable exceptions.

- *Sneha Chugh & Anupam Prasad*

Sneha is a third-year student of law at the New Law College, Bharati Vidyapeeth University, Pune and has recently interned at the Firm. The Firm acknowledges and expresses gratitude for the efforts put in by Sneha towards this AP Law Series write up.

[1] Guadamuz, Andrés. (2017). Developing a Right to be Forgotten. 10.1007/978-3-319-64955-9_3.

[2]https://www.indialawjournal.org/a-hustle-over-protecting-personal-data.php#:~:text=History%20of%20'Right%20to%20be,EC%20(%E2%80%9CDirectives%E2%80%9D)

[3] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available at: https://www.refworld.org/docid/3ae6b3b04.html [accessed 29 December 2020]

[4] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: https://www.refworld.org/docid/3ae6b3aa0.html [accessed 29 December 2020]

[5] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

[6] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

[7] https://gdpr-info.eu/art-17-gdpr/

[8] ECLI:EU:C:2014:317

[9] Guadamuz, Andrés. (2017). Developing a Right to be Forgotten. 10.1007/978-3-319-64955-9_3.

[10] https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/

[11] https://www.thehinducentre.com/resources/article24561713.ece

[12] (2017) 10 SCC 1

[13] Personal Data Protection Bill, 2018.

[14] Personal Data Protection Bill, 2018.

[15] BLAPL No. 4592 of 2020, High Court of Orissa.

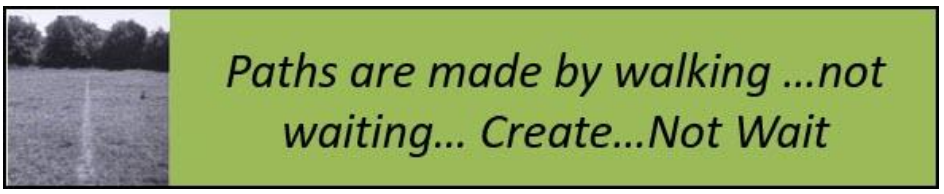
[16] (2019 (175) DRJ 660).

[17] Writ Petition Number 62038 of 2016 (GM-RES), Decided on January 23, 2017

[18] Dharamraj Bhanushankar Dave v. State of Gujarat, 2015 SCC OnLine Guj 2019, decided on 19-01-2017

[19] Writ Petition Number 62038 of 2016 (GM-RES), Decided on January 23, 2017.

Creating a Path Vs Waiting for others to develop a path



There are two kinds of organizations. One is a "Leader" and the other is a "Follower". A leader has a vision, a goal and fairly good idea of how to reach the goal. But often we are confronted with a situation where the goal is visible but the path has not been traversed earlier. In such situations, most people will wait for others to try out the path and then follow the path created by others. They donot mind waiting until the path is created.

On the other hand there are a few who are so confident of their vision that they donot mind traversing a path which no body else might have taken. They are the leaders who take the risk of uncertainties that they may face in being the pioneers of a journey. They do suffer initial bruises and hurdles but if their goal is right they succeed where others fail.

FDPPI is one such pioneer who has created its own path. When it was established in September 2018, the path was clear…to be the pioneer and an apex institution in the country dedicated towards the cause of creating a compliant Data Protection society in the country. The vision was to attain this status not by the designation of a Government body or by the financial strength of top corporates, but by building the institution brick by brick by the same people whose future depends on the Data Protection Eco system, namely the Data Protection Professionals.

FDPPI was therefore created as a Section 8 company limited by guarantee. In two years FDPPI has made significant strides of creating Certification Programs and the Personal Data Protection Standard of India. Soon it will add the third feather in its cap namely the DDMAC.

We have already left our footprints in the sands of time. But we have miles to go before we rest… FDPPI is a movement of the Data Protection Professionals and is set on a glorious journey ahead.

Naavi

Making PDPSI audits More reliable

If we analyse major data breaches, one thing common is that all such organizations where we have seen data breaches of significant proportions had been claiming that they were compliant to one standard or the other. In particular, almost all of them were ISO 27001 audited and PCI DSS audited.

FDPPI is now proposing a PDPSI audit and in the coming days, it is possible that even PDPSI audited organizations may face a data breach situation.

It is therefore essential for us to put in some systemic controls to ensure that the PDPSI audited organizations are subjected to some kind of monitoring on an ongoing basis to reduce if not eliminate the incidences of data breach of audited organizations.

One of the reasons why Certified Audits frequently gets discredited is that the audit certificates are often looked at as a Marketing tool" and nothing more than that. There is nothing wrong in using "Certification" for marketing but the auditee should realize that the core purpose of audit is ensuring that risks are properly assessed and bridged. No auditor is perfect and often new vulnerabilities emerge after audit and hence some element of failure of an audited organization is unavoidable. However, just as we expect "Due Diligence" or "Reasonable" security practices to be followed by an organization, organizations need to have a continued watch on the status of their certified status. Otherwise all audits are snapshots and auditors cannot keep watching the day to day operations of an organization to watch if the auditee has become complacent and ignoring the risk mitigation measures post audit certification.

Auditors and Certification systems also need to follow some due diligence measures to improve the reliability of the audit systems. Many organizations may not relish the audit certification agencies watching over their shoulders after an audit is closed and the auditor is paid off. But in order to protect the reputation of the Certification agency, some form of an attempt periodical interaction may be required.

FDPPI while using the PDPSI system has introduced the following controls to ensure a fair assessment during the audit.

1) After the completion of the PDPSI audit for Data protection Act compliance, the auditor will create a spread sheet for all the 50 model implementation specifications and make a DTS assessment based on certain group weightages.
2) The Auditor will send a copy of this worksheet leading to the DTS score to FDPPI along with a report that the audit has been successfully closed and a certificate issued to the auditee.
3) The auditee would be sending a feedback to FDPPI after the closure of the audit in a specified format essentially, accepting the assessment with or without permission for the disclosure of DTS.

These controls ensure that in case the auditor and the auditee are under a major disagreement on the assessment, FDPPI is kept aware of the disagreement and possible reasons. If necessary FDPPI may suggest a review audit besides taking the inputs for improvement of the system.

Once the audit is closed and registered with the FDPPI, the control to maintain the audit recommendations lies entirely with the auditee organization. To emphasize this aspect, the auditee organization will be required to send a quarterly report of continued compliance to FDPPI.

While FDPPI may not be able to enforce the submission of such a report, it gives an opportunity for FDPPI and the auditee to exchange a feedback such as when there is a substantial change in the business profile of the organization and there may be a need for an assurance of continued compliance from a PDPSI auditor. Towards this objective the quarterly report consists of a declaration that the organization continues to maintain the audit recommendations and to the best of its knowledge and good faith, there are no “incidents” that indicate a security alert nor there are any new risks that have arisen since the previous risk assessment.

With such a system FDPPI’s PDPSI system will remind the organization that audit of the PDPSI auditor cannot be considered as a permanent stamp of approval for the organization but is only an assessment of the risks and the remedial measures as observed on a specific date and the organization cannot remain complacent. Further in the event the organization does not utilize this

opportunity, then the auditor FDPPI as a sponsoring organization cannot be blamed for lack of due diligence.

The template of the audit feedback and quarterly feedback are being finalized and will be available in due course.

Naavi

Data Protection Emergency Response Team (DPERT)

PDPSI is addressing an important problem associated with Auditors and their reputation which is a unique proposition and perhaps the first time in the industry.

It is well known that whenever a major data breach occurs, everybody blames the organization stating that they had poor security. In their defence the organization will immediately try to shift the blame on to the auditor stating that they held a certificate from a reputed audit firm. The audit certification that we often hear is about ISO 27001 audit or PCI DSS audit. The fact that a data breach occurred even after a rigorous audit hurts the image of the audit system and more so the auditing firm.

In instances where the auditors have been reckless or conducted audit only for billing purpose without any commitment to the objective of the audit, there have been instances where auditors have been held “Negligent” and penal action is invoked on them.

In actual practice, there may be many genuine auditors who honestly try to assess an organization and leave valuable suggestions to them which if implemented would help the organization towards better information security. But the auditor has no control about what happens the day after the audit certificate is signed and delivered. Next time he hears is when he is called for a review audit or blamed for a bad audit.

As a result public normally has a low opinion of audits and consider it as a “Snapshot view” and has no relevance for a “Going Concern”

In order to find a solution to this problem. FDPPI has introduced a system of “Auditee Mentoring”. This is a service provided only to those organizations who undergo PDPSI based audit by the FDPPI accredited auditors so that such audit certificates have a value more than as a “Snapshot View”.

Presently the PDPSI auditor files a report with the FDPPI after conclusion of the audit and issue of his certificate to the client. The report will be accompanied by

the auditor's DTS worksheet. This would register the audit with FDPPI along with the assigned DTS. FDPPI will also get a direct feedback from the auditee organization about the audit in which consent would be sought for disclosing the DTS to the public from the FDPPI website. If the DTS is good, the organization may agree otherwise it may refuse and this choice would be honoured unless DTS is made public by the Company or the Data Protection Authority directly.

Having registered the audit, FDPPI will then offer an option to the auditee that a team of PDPSI consultants from FDPPI which is constituted as "Data Protection Emergency Response Team" (DPERT) would offer an audit mentoring service under which every quarter, the Company would be provided a quick high level review of any significant data breach which the organization would like to report to the mentor to seek his advice. Additionally, in case of any emergency also such quick check can be initiated.

In such references the DPERT would provide an instant guidance on how to proceed, without getting into an elaborate consultancy. It is a different matter if the organization then wants to seek advisory service when DPERT may assign the consultancy work to a suitable PDPSI consultant.

This arrangement means that FDPPI does not leave the auditee organization to simply fend for itself after the audit certification and tries to provide some minimal channel of communication.

In case of Corporate Members, FDPPI already has a continuous channel of communication and DPERT is part of such channel. Now FDPPI is extending this to the PDPSI auditees who may not have Corporate membership privileges.

PDPSI already offers consultancy to be availed prior to the audit and such consultancy is always available even after the DPERT intervention if the organization requires.

With this approach FDPPI is exhibiting its commitment to the Data Processing eco system to ensure that Privacy and Data Protection becomes a culture of the society and not simply look at PDPSI as an opportunity to introduce yet another audit system which is a cost on the system.

The concept is new and can be introduced only by an organization like FDPPI which is a Not for Profit organization with a commitment to the society. Hopefully organizations would make a good use of this unique proposition.

Naavi

Q & A

Here are a few questions that FDPPI has come across recently and some view points from FDPPI team:

Q1: What is the difference between Data Privacy and Data Protection?

Answer:

Certain terms have come to be used in the industry with a certain meaning in a context. Over a period the usage gets extended out of context and often leads to confusion. We as professionals need to understand the meaning and apply it appropriately based on the context. “Data Privacy” and “Data Protection” are such terms which may be used interchangeably. But at FDPPI, we would like to use them in the context specific manner and hence the following narrative needs to be noted.

“Privacy” is a term that is applied as a “Human Right”. It has come to be spoken in the context of Data Protection because the industry tries to protect the “Right to Privacy” of an individual by dealing with the “Data” in a particular manner. Industry cannot directly protect the “Right to Privacy” of a person. It can only protect “Information Privacy” or protection of Privacy through protecting data related to Privacy protection.

“Data Privacy” apparently means “Privacy of Data” and it can be better used in replacement of the term “Confidentiality” of data which is a component of Information Security. “Confidentiality” in the information security context is understood as “Allowing access only to authorized persons”.

“Data privacy” therefore appears more meaningful in the Information security context. Colloquially however Data Privacy has come to be used as “Protecting Privacy of an individual” by “using data about a person as per his choice on how it can be used and disclosed”.

The term “Data” and “Information” are also used interchangeably. However, as a norm, “Data” is used more in the context of “Privacy Protection of an individual” while “Information” is used more in the context of protection of the Confidentiality, Integrity and Availability of the data. In the context of Privacy Protection, “Data” contextually may mean “Personal Data”.

While the above provide justification for the use of the terms as interchangeable terms with understanding based on the context, at FDPPI we are trying to develop a distinct usage of the terms.

Hence, we understand that “Privacy Protection” is a human right concept and “Data Protection” is an Information Technology Concept. “Data Protection” means “Protecting the privacy of a person by providing the data subject, the choice of how his personal data is collected, used, disclosed or disposed”. “Personal Data” is data that is related to a natural person.

“Data” per se may mean both personal data and non personal data and as far as possible it is better to use the specific term “Personal Data” when we deal with Privacy Protection responsibilities.

As a standardisation at FDPPI we would like to use the term of “Data Protection” for protecting the Privacy of a Data Principal through protecting his Right of Choice on how his personal data may be used, disclosed and disposed by a third party (Data Fiduciary) to whom the personal data is given by way of consent for a specific purpose. In this sense, we would like to avoid the use of “Data Privacy” and leave it to describe the security of the inanimate object called “Data” which may include non personal data also unless the context exludes.

Since in the larger market people continue to use the word “Data Privacy” for all measures taken to protect the privacy of a data subject, we cannot discontinue the use of the term from time to time.

Similarly, we need to put up the alternate uses of the term “Data Subject” and “Data Principal” as interchangeable and “Data Controller” and “Data Fiduciary” as interchangeable. As far as possible we use the terms Data Fiduciary and Data Principal in the Indian context while using the terms Data Controller and Data Subject in the context of GDPR or other laws.

For the same reason we are using the term “Certified Data Protection Professional” for our courses instead of “Certified Privacy Professional”. In the Consultant/Auditor certificate we have used the term “Certified Global Privacy and Data Protection Professional” so that the industry understands that this certification is related to what others call as “Privacy Protection”.

Q2: What is the difference between GDPR and earlier European Data Protection Directive

Answer:

The European Data Protection Directive was an instruction to all EU member states to follow measures mentioned there in as a “Model law” to protect the privacy of individuals in the EU. Each member states were therefore required to

pass their own data protection laws applicable within their jurisdiction on the lines of the directive.

The GDPR is however a General Data Protection Regulation applicable to all member stated of EU without the need for a country specific law to be passed. This was meant to bring more uniformity in the laws.

However, presence of the earlier laws and some flexibility built into GDPR to accommodate local laws related to employment and minority etc continue to present a local version of GDPR which outsiders need to take note for compliance.

Q3: What is the difference between PI and PII?

Answer:

PI refers to Personal Information while PII refers to Personal Identifiable Information. They may often be used interchangeably. If we need to make a finer distinction, PII contains elements which can be used to identify a natural person to whom the information belongs to. On the other hand PI may relate to information about human beings but may not contain personal identity of any person.

The distinction is not very significant since if an information cannot be identified directly or indirectly as belonging to an identifiable natural person, it may be more aptly called “Non Personal Information”.

Further in this context we may note that “Information” is used as an alternative to the term “Data”.

In laws such as HIPAA certain elements have been listed in the law itself and are called “Identity Parameters”. There is one school of thought that considers these identity parameters as PII.

However unless the identity parameter is associated with another identifiable parameter often it cannot be used to identify the natural person to whom the information belongs to. Hence such information may remain non personal information until in the life cycle of processing it becomes identifiable with an individual and there after it attains the status of a PII.

Using the analogy of Physics, we can take the example of a wandering Proton which is just a proton. But if it can capture an electron into its orbit and become

a “Hydrogen Atom”. The properties of an “Atom” is different from the properties of the “Hydrogen atom”. Similarly one single element of information may be a PI. It may become PII when it is associated with another element with which the identity of a person develops. The two together can be called a PII.

Hence an IP address is recognized as a PI under HIPAA. But only if the IP address is associated with some thing else, it has the characteristic of a PII. The e-mail address is another such enigma. As long as the system of e-mail system exists where any person can register an e-mail ID without any identification, the e-mail ID itself is nothing more than a PI but is less than a PII.

For example if there is an email ID narendramodi2021@gmail.com, it cannot be presumed that it is a personal ID of PM of India or even that it is the ID of a person whose name is Narendra modi even if he is not the PM of India. A Rahul Saxena can also register the email Id of narendramodi2021@gmail.com. Hence the e-mail ID is per-se a Pseudonymous ID. But when this ID is associated with another parameter say a PAN card or Aadhar card or even a content from which some indication can be obtained whether the person is the PM of India or not, then the character of the e-mail ID changes into a PII.

Similarly even the name “Narendra Modi” is not a fully identifiable personal information since there is no rule in the world that two persons cannot have the same name.

We should therefore use the term PI and PII with the distinction they deserve.

Q 4: What is the difference between Privacy policy and Privacy Notice

Answer:

The terms “Privacy Policy” and “Privacy Notice” are also used interchangeably. However, it would be good o make a distinction under the following principles.

“Privacy Policy” is a declaration of intent. “Privacy Notice” is however a more direct communication to an individual.

When we need to take a “Consent” of an individual to collect his personal information, and want to treat the “Consent” as a “Contact”, it is preferable to use the term “Privacy Notice” since it becomes an “Offer” in a contract which the individual can “Accept” and a “Consent Contract” emerges.

The use of the term “Privacy Policy” has come since many organizations prefer to declare “ I respect privacy of individuals and follow the following principles…”.

At the end of such “Declaration” it is more appropriate to ask the individual, “Are you satisfied with my Privacy policy? If so you can give your consent to avail this service”.

The use of the terms should also be seen in the context of what does the individual do at the end of reading the “Privacy Policy/Notice”.

If he says “I Accept”, the wordings of the document should be construed as a “Privacy Notice”. If it says “Submit”, the wordings of the document may be construed as an “Invitation to offer” and not “Offer”. If a document is an “Invitation to offer”, then based on the “Declared Privacy Policy”, the individual will submit his “Offer” which states “I apply for your service as per the privacy policy you have declared. Please accept to complete the contract”.

Indian PDPB 2019 is clear that the “Consent” need to be treated as a contract as defined under the Indian Contract Act. Hence the term “Privacy Notice” followed by “I Accept” appear more appropriate.

However, since the clicking of the button “I Accept” is a “Click Wrap” Contract, the contract may be construed as a “Deemed Contract”.

Question 5: Is 'disclaimer of warranties' an appropriate clause to include in a privacy notice? If yes, then to what extent.

Answer:

A Privacy Notice is different from “Terms of Service” unless it is drafted as a “Privacy Notice cum Terms of Service”.

If “Privacy Notice” is distinct, it should confine itself to the information required to be given to the data principal from whom personal information is collected, such as what information is being collected, for what purpose, how is it going to be used, how long it will be retained, with whom it will be shared etc. In terms of the recent data protection laws, it is necessary to inform the data principal at the time of collection itself information about his rights of access, correction, portability, deletion, grievance redressal etc. Indian PDPB also requires the DTS disclosure at this stage itself.

The Warranty related information my be more appropriate for the “Terms of Service”.

It must be remembered that the nature of a document whether it is only a Privacy Notice or also a EULA, depends on the content and not the title.

Question 6: Shouldn't user's part of responsibility be mentioned in the privacy policy to make them aware about their own role in protecting their Privacy?

Answer:

“Privacy Policy” as explained above is a term more suitable for “Self Declaration”. If any user responsibility has to be added here, it would be more like expression of “Limitations”. As long as we realize the principle of what is a “Policy” or a “Notice” or What is a “Privacy Notice” and what is a “Terms of Service”, the intentions of the parties can be captured adequately.

It is for this reason that we often make a reference to the Privacy Notice in the terms of service and vice versa with hyper links as if one is an extension of the other.

Question 7: Is biometric data theft really permanent?

Most biometrics may be considered “Unique” and hence biometric data theft is permanent. There could be exceptions such as “Voice Biometrics” which may be altered by a surgery as much as the features of ear or nose being altered in facial recognition. Finger print is perhaps more permanent though it can get erased rather than modified by surgery like interventions.

The dental structure or skull structure or DNA also provide permanent identity of an individual and hence the “Theft” of such data cannot be corrected like re-setting of a password.