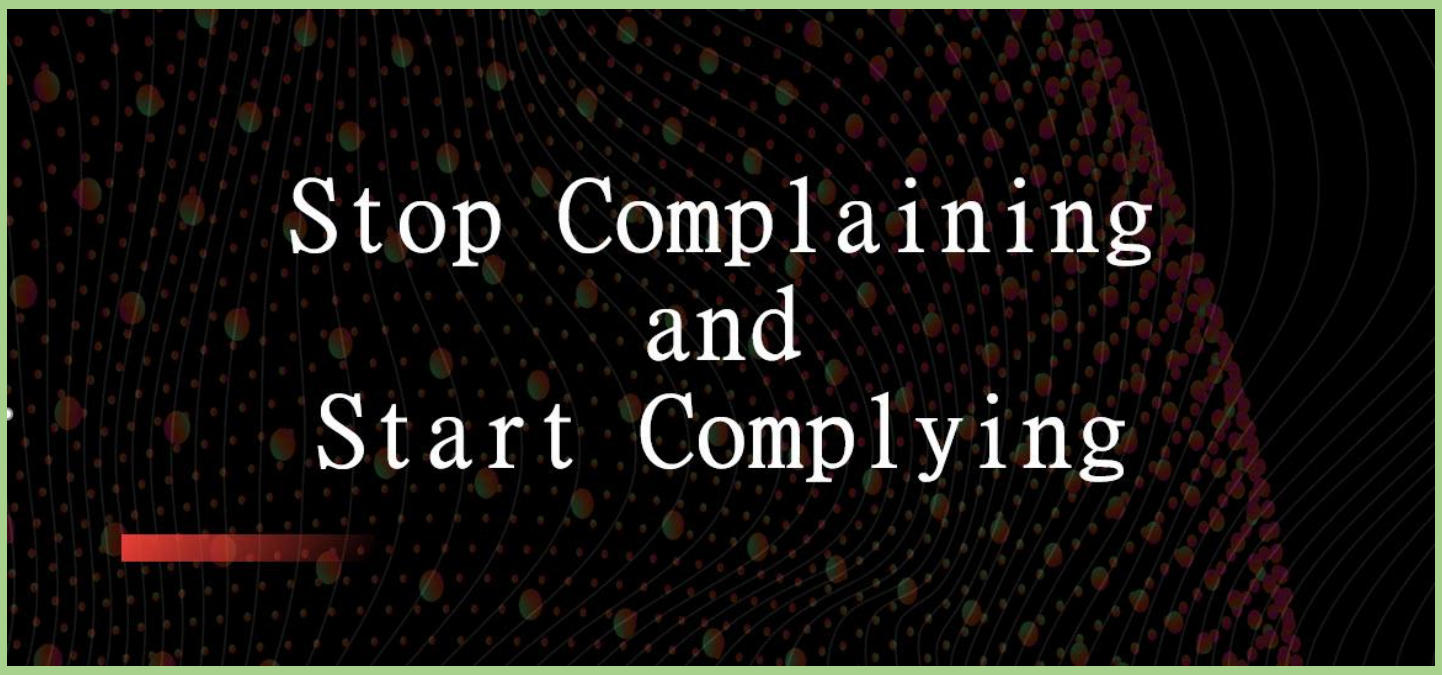
.

Data Protection Journal of India

Volume 2: No: 2/2022: 30th April **2022**



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

Previous versions of the Journal are available at www.dpji.in

The Budget Session of the Parliament is over and there is no news about the passage of the Data Protection Act 2021, the updated Personal Data Protection Bill 2019.

In the meantime, the Government issued the draft "India Data Access Policy" for the Governance of Data at the Central Government level and also advised States to pass similar policy documents. Tamil Nadu was one of the first State Governments to pass a "Data Access Policy".

Further on 28th April 2022, the Ministry of Electronics and Information Technology (MeitY) issued a fresh "Data Breach Notification" order to replace the earlier order of 2017 with a greater clarity on notification of data breach under ITA 2000 to the CERT-IN.

These moves indicate that the Government is working in the background to ensure that they are first of all ready for the implementation of the DPA 2021 (or DPA 2022 as it may finally be named).

It is therefore necessary for the private sector to start reflecting if they also have to start their compliance program assuming that the Data Protection Law will be passed at least in the next session.

At FDPPI, we believe in starting the journey towards Data Protection early and recommend that Corporates should not be complacent that the law may not come now or will come with many changes etc and they can take note when the law is finally passed.

FDPPI therefore is continuing its efforts to educate the industry in different forms. Towards this end, FDPPI organized a one day symposium in Chennai on "DPA 2021-Compliance View" jointly with Madras Management Association, in the MMA Auditorium in Chennai. The program were partnered by ISACA Chennai and Cyber Society of India, Chennai. Over 150 participants attended the symposium, details of which are provided elsewhere in the journal.

FDPPI has also launched a National initiative titled "National Privacy and Data Protection Compliance Movement" and will undertake more activities like the Chennai symposium in other parts of the country in due course.

Additionally FDPPI has launched a special Corporate initiative of developing sector wise code of practice for different sectors based on the Data Protection compliance standard of India (DPCSI), which is the upgraded version of PDPSI which we have discussed in earlier DPJI issues.

At the same time, the core DPCSI is also being updated with the changes such as the new Data Breach Notification Requirements notified by the Government.

Even if the Government is taking its time to pass the Bill, FDPPI will continue to push the industry towards early adoption so that the delay in passage of the Act would be mitigated by a quicker adoption after the Bill is passed.

In view of the delay in publishing this edition, some information of April 2022 has also been added.

Naavi

News Section

From the Newsroom

1. According to survey of Market Research Future, in US, Data Protection as a Service (DPaaS)market may touch USD63 million by 2027. DPaaS is deployed on IoT enabled devices to encrypt, secure and store enormous amounts of data generated by individuals and businesses. BYOD and Chose your own Device (CYOD) is boosting the security requirements. This survey may cover only the technical aspects of Data Protection and not the compliance related activities.
2. Bangladesh has published a draft of the proposed Data Protection Act 2022
3. Sri Lanka has also passed the Data Protection Law has passed Personal Data Protection Act 2022.
4. Lakeview Loan Servicing, a mortgage servicer in USA, revealed a data breach of over 2.5 million loan customers.
5. US-EU entered into a new arrangement to replace the Privacy Shield on March 25, titled Trans-Atlantic Data Privacy framework. A final agreement is expected to in place in due course.
6. The Dutch Data Protection Authority imposed its highest ever fine of 3.7 Euros on the Tax authorities for illegal processing of personal data in the Fraud Signalling facility. (Expected to be challenged)
7. True caller headquartered in Stockholm is said to have built up a data base of over 5.7 billion unique phone identities., made possible by the lack of adequate privacy laws in India.
8. Utah passed a comprehensive Privacy Law similar to CCPA.
9. EU is working on a proposal for a Data Act to supplement the Data Governance Act which was adopted last year. This act may define obligations of data sharing by manufacturers of connected devices.
10. ENISA (European Union Agency for Cyber Security) has published on 24th March 2022, a report on deployment of pseudonymisation techniques to be used by the Health Care Sector.

Knowledge Section

Report on Conference at Chennai

By

Naavi

On April 23rd 2022, FDPPI Conducted a day long symposium on "DPA-2021-Compliance View", in association with the Madras Management Association (MMA). ISACA Chennai, CySi and Paramount Data Products partnered with a large number of their members attending as delegates . Mr Vaidyanathan Chandramouli, Mr Sridhar Ramakrishnan and Mr Govind Srinivasan represented these organizations respectively and along with over 50 members of MMA ensured that the well equipped MMA Auditorium at Pathari Road, Thousand Lights, Chennai was overflowing with delegates.

The theme of the seminar was "**Compliance and not Complacency is the Choice of Wisemen"** and urged the professionals and the Companies to be leaders and start the journey to compliance and not be satisfied as followers with excuses that the Act is not yet passed and waiting for others to take the lead in compliance.

After a formal Virtual inauguration by Sri R Ravichandran, IRS, Commissioner of Income Tax, FDPPI conducted one introductory key note session by Naavi followed by four different panel discussions on different topics, anchored by Naavi.

During his key note address, Naavi introduced FDPPI and gave an overview of DPA 2021. He highlighted the complexities of complying with DPA 2021 in view of the inclusion of Non Personal Data in the Bill as well as the need for Indian companies to be compliant with other data protection laws such as GDPR if they handle relevant data. He also highlighted that ITA 2000 continues to be effective today as the Data Protection Act and gets augmented by the new bill as "Due Diligence" even before the Act is passed. He pointed out that ITA 2000 will continue to be relevant particularly for "Criminal Offences" while DPA 2021 will essentially focus on Civil Penalties to promote compliance.

The session was followed by a panel discussion where Advocate Rohan K George of Samvad Partners and Ms Geetha Jayaraman of Capgemini in which several key legal aspects of DPA 2021 was discussed.

The session focussed on the definition of Privacy as per the Puttaswamy Judgement and how it gets converted into Data Protection in the data processing environment.

Naavi also drew the attention to the definition of harm in DPA 2021 which includes psychological impact that impairs the judgement of an individual and how it brings in the concept of "Neuro Rights" into the discussion of Privacy.

This session was followed by the second session on "Critical Technology Challenges before the industry" in which Dr Mahesh Kalyanaraman, of HP, Nagendra Javagal, a Governance consultant and Ms Suhasini of Karkinos health care participated. During the discussions technology aspects such as Anonymization, Centralized Data Storing and Classification of Data. A brief discussion on the Sandbox system as proposed in the Act and how it could help start ups to conduct controlled testing in a sand box so that "Innovation" is not curtailed by the operation of the Privacy regime.

In the first post lunch session, a panel consisting of Mr R Vittal Raj, a well known Information Security consultant, Mr Ramesh Venkataraman of Carl Zeiss and Mr Nagendra Javagal discussed the two key career opportunities presented by the proposed DPA 2021 in the form of Data Protection Officers (DPO) and Data Auditors.

The panellists discussed the impact of the Act equating the position of a DPO to a Key Managerial Personnel. The panel also discussed the skills requirements and the sources of from which appropriate training and certifications could be obtained.

It was also highlighted that the work of an "Independent Data Auditor" who has to conduct a mandatory annual data audit would also give raise to new opportunities and a career.
In the fourth and final panel discussion, a team consisting of Mr Rupak Nagarajan of KPMG, Govind Srinivasan of Paramount Dataware and Ramesh Krishnan discussed the compliance frameworks now available and the framework which

FDPPI has developed as Data Protection Compliance Standard of India or (DPCSI). The need to update the current frameworks such as ISO 27701 which have been designed for a different purpose and different law to meet the compliance of the Indian law and how a Compliance oriented framework such as DPCSI could be more useful to the organizations.

Naavi also highlighted that taking advantage of the provision of Section 50 of DPA 2021, FDPPI would we working on developing codes of practice to different sectors so that a good self regulatory system can be developed and presented to the Data Protection Authority at the appropriate time seeking their approval and softening the hardships of compliance.

Each of the sessions were followed by question and answer sessions and the program was very well received by the audience

Some views about the conference

After over a yearlong zooming and teaming to get precious knowledge basics on the emerging data protection law in India, the chance to be part of the in-person event hosted by the Foundation of Privacy Professionals of India (FDPPI) on 23rd of April, 2022, was like a refreshing cool breeze in the sweltering Chennai heat.

The mega-event, first of its kind by FDPPI, since Covid-19 restrictions have been relaxed. was a day long affair, co-hosted by ISACA at Madras Management Association (MMA). I must admit, I am usually a tad sceptical of panel-based discussions; so, I went expecting the usual round of question answer sessions.

The first thing that struck me was the level of professionalism in the organization of this event. Starting with the registration, where I normally must search for my name in a long list of participants. Here, the organizers, had separated all participants into different categories, members of professional body, panel participants, others. So, it took only a few seconds to find my name, take my programme folder and find a front row seat in the auditorium.

The highlight of the day, for me, was meeting Mr. N Vijayashankar (Naavi) and Mr. Ramesh Venkat. I had attended the online training programs led by Naavi and Ramesh Venkat, early last year. Their knowledge of the privacy bill and privacy laws of other countries is just phenomenal. After attending those training sessions, I have been waiting to see and interact with them in person, and this conference did that! Despite being a summer weekend, there were a large number of participants eager to hear from the panellists.

The uniqueness of the whole session was that Naavi gave an informative prelude to each panel session, highlighting the bill requirements and the challenges, also providing interesting references to litigations pertaining to the topics discussed. Panel members were well prepared, and each session gave food for thought. Despite his busy schedule and challenges that prevented him from being in Chennai, Mr. R Ravichandran, Chief Commissioner of Income Tax, logged in from Bangalore and gave a very insightful introduction to the need for privacy legislation in the Indian context.

The sessions covered i) Key legal issues emerging out of DPA 2021, ii) Critical technology challenges, iii) Professional opportunities and disruptions, iv) Existing compliance frameworks and new codes of practice. Each panellist shared has/her knowledge on the topics discussed and the moderation by Naavi, kept the conversation flowing seamlessly.

This was one fantastic conference.

MANJULA SUBRAMANIAN

New Data Breach Notification Policy and impact on Data Protection

Naavi

When the Joint Parliamentary Committee (JPC) on Personal Data Protection Bill 2019 re-named the Bill as "Data Protection Bill" instead of "Personal Data Protection Bill", the section on reporting of data breaches (section 25) was modified in the title as "Reporting of Data Breach". However in the sub sections (1) to (5) , the section indicates how the data breach has to be reported, what should be the remedial actions to be taken etc related to the breach of personal data. Subsection (6) alone states that "The authority shall in case of breach of non-personal data, take such necessary steps as may be prescribed".

Hence at this stage of this Data Protection Bill/Act there is no specific guideline on post-breach action in respect of non personal data.

Additionally, it should be noted that DPA 2021 (current version of the Bill) replaces only Section 43A of Information Technology act 2000 (ITA 2000) and does not affect Section 70B of the Act which creates an agency by the name "Indian Computer Emergency Response Team" which shall serve as the national agency for performing functions related to Cyber Security such as collection, analysis and dissemination of information on Cyber incidents.

It is to be also noted that the powers of CERT-IN are not restricted to monitoring of Critical Information Technology Infrastructure for which it is the national nodal agency. The role of CERT-In is linked to the definition of "Cyber Security Incident" and "Cyber Security Breaches" which are contained in the notification of 16th January 2014 which is supplemented by the new Data Breach Notification Direction (DBND) of 28th April 2022 which will come into effect from 28th October 2022.

Hence Section 70B of the ITA 2000 and the powers of CERT-IN under ITA 2000 will survive the passing of Data Protection Act 2021/22 and the creation of the Data Protection Authority. CERT-IN will have its defined role in the "Cyber Security" area and will have to work along with the Data Protection Authority of India (DPAI) as envisaged under DPA 2021. This would be as much a responsibility of CERT-IN as that of the DPAI though DPAI would be a much larger body as compared to CERT-IN which will appear to be part of the MeitY.

Though it appears to public perception that the CERT-IN is a department of MeitY, CERT-IN will like the Controller of Certifying Authorities enjoy an independent status as a statutory body. I have often referred to CERT IN as the proverbial Hanuman who through a curse was unaware of his powers until he was reminded by the wise Jambavanta, CERT IN has never exercised its powers and has humbly remained a back office of MeitY manned by some scientists who try to send out advisories from time to time and remain quiet thereafter.

The possibility of the DPAI becoming an all powerful body for regulation of both personal and non personal data once the DPA 2021 is passed, has now woken up the Jambavanta in the MeitY which has reminded the CERT-IN that it has the power that will survive the DPA 2021 and would not be irrelevant when DPAI becomes a "Regulator of both Personal Data and Non Personal Data". This notification is meant to announce this newly discovered role for the CERT IN and was one of the pre-emptive actions that MeitY perhaps wanted to complete before the passage of the DPA 2021.

CERT-IN is created by a statute and is a Quasi Judicial authority which provides it the powers under Section 70(B)(7) to impose punishments of imprisonment for a term that may extend to one year or fine which may extend to one lakh rupees or with both. This power is like the power of the UIDAI in the UIDAI act for prosecution and the offence shall be cognizable only on a complaint by CERT-IN and not otherwise.

Once the CERT-IN (i.e., Director General who exercises the powers of CERT-IN) decides that an organization (Which could be any Government or a Non Government agency or individual) is guilty under Section 70B, it could mean either that a data breach was not reported or any of the guidelines of CERT-IN was not followed, it automatically fixes the "negligence" on the part of an organization in maintaining "Reasonable Security" and hence confirm the operation of Section 43A and Section 43(g) of ITA 2000 along with Section 66 of ITA 2000.

The powers of CERT-IN are therefore larger than that of DPAI since DPAI cannot order "Imprisonment" of any of the executives of a company where as the Director General CERT-IN can do so under Section 85 of ITA 2000.

The question will therefore arise whether the powers of the Director General of CERT-IN are excessive and curtail any provision of the Constitution of India. As has been the habit of some activists, any regulation being passed by the Government will be questioned in the Supreme Court and our honourable Supreme Court is always obliging the activist lawyers and sit in judgement of every decision of the Government brought to its knowledge.

Recognizing this possibility the data breach notification directive has taken care to be a comprehensive code by itself. It has the preamble reference to Section 70B of ITA 2000, the notification of 16th January 2014, the need to control increasing threat of Cyber Security breaches and more importantly the constitutional exceptions such as "in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence".

Further a time of 6 months has been provided for implementation of the order though this notification being an order related to the law which came into existence on 27th October 2009 did not require such a notice. This means that the argument of "Sudden imposition of a draconian order" could not be raised in the Supreme Court.

In view of these precautions taken by the MeitY, the potential threat of a judicial suppression of executive powers has been mitigated to some extent. Despite this, it is a reasonable expectation that the matter would be referred to the Supreme Court and like the "Intermediary Guidelines of 25th February 2021", Supreme Court would be obliged to take up the petition and issue notice to the MeitY so that for as long as the Court wishes and continues to oblige influential advocates, the matter can be kept as "Sub-judice" and not implemented.

FDPPI however does not believe in complacency in complying with any law and would consider that once a notification is issued, it determines the legislative intent of the state and the Courts are at liberty to accept the provisions as "Due Diligence" even during the period of cooling time provided in the law itself or with the "Sub-Judice" status. Just as many Courts have started quoting PDPB 2019 to justify "Right to Forget" as a recognized privacy right, it

is open to Courts to consider that the notification and the contents thereof constitutes "Best Practice" and "Due Diligence" as of today. Hence unless it is over turned subsequently, it would remain the "Best Practice" for prudent Corporates to assimilate and absorb these regulations into their Cyber Security practice.

FDPPI has already taken a decision to make necessary updation to its Data Protection Compliance Standard of India (DPCSI) and revise its Data breach notification policy expectations under the standard.

Now that the logic is set for Companies to consider this notification seriously and not ignore it as many may suggest, let us look at those prudent companies who know that their business is not to challenge the law but try to follow it in good faith. If some activists take steps and reduce the burden of law, it would be welcome since it can help in reducing the risk further.

Essence of the Action to be taken by Companies

1. The notification applies to all Service Providers, Intermediaries, Data Centers, Body Corporate and Government organizations.
2. All system clocks shall be synchronised with NTP server of NIC or NPL or traceable to these servers. Even entities having ICT infrastructure spanning multiple geographies shall ensure that they use accurate and standard time source not deviating from the NIC/NPL time source.
3. Cyber Incidents shall be reported mandatorily (may within 6 hours of an organization coming to know of the incident through e-mail
4. CERT-IN may issue directions for the purpose of protective and preventive actions related to cyber incidents which shall be adhered to.
5. Point of Contact shall be designated and informed to CERT-In
6. Logs of all ICT systems shall be maintained on a roll over basis for 180 days and stored within Indian jurisdiction, to be made available to CERT-IN as required
7. Organizations handling customers, need to keep customer data such as "Validated Names", IP addresses used for registration, ownership of subscribers, validated address and contact numbers, etc for a period of 5 years.

A list of incidents that may be considered as Cyber incidents include targeted scanning of systems, unauthorized access, defacement of websites, attack on data base, mail servers, DNS network, Identity theft, spoofing and phishing attacks, data breach, Data leak, Fake mobile apps, unauthorised access to social media accounts, etc.

All together, the guidelines will shake up the industry which so far was not even recognizing the existence of CERT-IN.

Interesting days are ahead for compliance managers. Organizations which were short changing security and declaring "We shall introduce commercially viable security measures" will now have to revamp their systems to meet the stringent demands that CERT-IN may make.

Whether the Director General will actually implement the guideline or go back to the Kumbhakarna sleep, only time will tell. If however, CERT IN decides to follow the intent behind the directive, it would be better for them to also present a strong organization to take measures such as penalizing the contraventions.

Creating an Advisory Council for CERT-IN

CERT-IN presently has two distinct activities.

Firstly, it provides guidelines and advisories for mitigating Cyber Security risks. This requires a developmental attitude and technical knowledge and skills. At present this is being provided by the Director General and the team of scientists working under the MeitY.

Secondly it has to take action post a data breach report or disciplinary action when a data breach is not reported to it or when its directives are not complied with by an organization.

The Director General CERT IN will not be able to enforce his powers effectively because the organization that needs to be disciplined will be more powerful than the individual who works as the Director General. However good the person can be, he needs the support of a team of experts to led weight to his actions.

Since in due course the Director General, CERT-IN will have to deal with both personal data and non personal data protection, there could be directions given by CERT IN which may have to be coordinated with the DPAI which is a 7 member powerful body with experts of all kind. Further the penalties if any would be decided by DPAI through a quasi judicial person namely the adjudicator whose decision is subject to the appeal to an appellate Tribunal.

In comparison, CERT IN decisions will be the decisions of an individual and he can only invoke a complaint under Section 70B(7) which has to go to a Court. CERT IN may not impose financial penalties but his decision may be taken cognizance of by an Adjudicator under ITA 2000 and penalties imposed.

The Director General CERT IN, as an individual, may find himself inadequate to confront the might of the DPAI despite his statutory powers. In order to render weight to the decisions it is therefore suggested that the MeitY/CERT-IN should create a CERT-IN advisory Group to assist the Director General. This group should be comparable in expertise to the DPAI though it may be an adhoc group which may meet once in 3 months under the chairmanship of the Director General CERT-IN. The group should be constituted with care that matches the intellectual might of DPAI. It should include atleast 6 experts matching the requirements of DPAI members. With the power of such a body behind him, any decision taken by the CERT IN Director would be respected by the companies or even the DPAI.

At present such a body can only be constituted as an advisory body and not a legally empowered body like DPAI. But the creation of such an advisory body would strengthen the office of CERT IN and reduce its hesitancy to take decisions. If the advisory body has its own technical experts, the members can even assist the CERT In in it's other activities presently handled only by the employees of MeitY.

According to the Minister of IT, Government is working on amendment of the ITA 2000/8 and a draft for public comments would be released within a month. Probably this will be released before the DPA 2021 is passed. May be some of the changes that the Government thinks it needs to pass before DPA 2021 is passed may be included in this amendment. If required, the suggestions for the "Advisory Committee" indicated above may also be formally included in the amendment.

Commercial Interests taking over Privacy Rights?

By M.G.Kodandaram, IRS.,

Assistant Director (Retd),

ADVOCATE and CONSULTANT

Privacy in Cyber Space

Every human being knows that the current explosion happening in cyber space have shattered the privacy of the netizens / users across the globe with no shelter for the victims to seek relief. In any civilised society, restoring a dignified living of an individual is of paramount importance for any administration or government. It is a necessary endeavour of every person to respect the privacy of others so that every resident can lead of dignity. Majority of the countries in the world (Approximately 132 countries) have provided the much-aspired legal protection, from the harms caused by abuse of digital information by the Data Fiduciaries and Data Processors involved in personal data collection and processing for commercial gains. It is distressing to write here that India, with a huge population being targeted by the evils of personal data abuse, has continued to deprive their citizens, the much-desired legal protection. Even though this is part of a fundamental right under Article 21 of our Constitution, as has been held by the highest court of the land, has not been treated with necessary attention it should deserve. However, there is ray of hope as the IT minster in a recent press meet stated, 'extensive deliberations are on over various aspects and suggestions related to the draft data protection Bill, and the government hopes to resolve certain complex issues soon and get Parliament's approval on the legislation latest by the monsoon session'.

This further indicates that the privacy law as per the recommendations of justice Srikrishna commission is not going to happen as it is deliberately diluted. The law-making process is being throttled by the commercial interests to cut down the privacy rights proposed in the bill which is matter of greater concern. The law-making machinery yielding to such pressures, which is against the interests of individual, is deplorable. An attempt, through this article, is made to note the historical developments leading to the current situation, with a view to find out the reasons for the delayed law-making process and the dilution occurring in the making of a fair privacy law. Also, standard measures that could be initiated / equipped by the fiduciaries to be ready for the new compliance regime are deliberated.

Privacy law making Crippled

It is a fact that there is digital revolution taking place all over the world and India, without an exception, is very much in the race, thanks to the massive population who are using ICT tools in all walks of life. India, according to reliable reports, with approximately 4.66 billion internet users and new data being added at the rate of 2.5 quintillion bytes per day, stands amongst the fastest growing data generating nations in the world. The growth of the e-commerce markets in India are guesstimated to be of the order of US$ 188 billion by 2025. As on date around 132 countries are administering the legislation to secure the protection of personal data and privacy of their populations. It is also pertinent to mention here that the multinational business entities,

including Indian companies are, in their day-to-day operations, sincerely adhering to privacy norms as mandated by the respective jurisdictional country, but when it comes to Indian jurisdiction, they are not showing much interest to the Indian privacy proposals.

Though the Apex Court during the hearing of the justice Puttaswamy case, over four years ago, has been assured by the Indian Government, to make appropriate laws for protection of the privacy of individuals, there is no fair legislative framework in place. Whereas the ICT tools continue to flourish and harm the privacy of the innocent citizens, the legislators have remained a mute spectator to the crisis faced by the people. There appears to be little urgency shown by the law makers to provide suitable regulatory mechanism to protect the most essential fundamental right.

Privacy – Why it matters?

In any democracy the 'Right to Privacy of an individual' is a much-cherished right. The protection of the personal information of an individual has become common factor in these days, as all the entities, including Public Authorities, are using digital means to conduct their activities and services. As an essential part of their activity, they gather personal data of individuals who come in contact, may be as customers, as vendors, as employees etc., for multiple purposes without providing any security for the data so collected. Such personal information aggregated, with or without the knowledge for the subject concerned, could be exploited by fraudsters through illegitimate means. If there are no fair law in place to regulate the personal data, it leads for exploitation of personal data by the entities or by the hackers, who illegally access such data to commit crimes on such individuals. When personal information reaches the wrong hands, the individual is made to undergo severe harm to his privacy, finance, dignity, and the very existence. The rampant and unregulated deployment of digital technology tools to collect such personal data, without the consent or knowledge of the subject, has created a scary situation for the privacy rights of all such individuals. In cases of such personal data reaching the hands of the Dark Webs, dominated by outlawed criminals, the injury it could cause to the personal life and liberty of individual cannot imagined. Despite such crimes happening unabated and the citizens continue to be the victims, the legislators have remained complacent, which is a matter of greater concern.

Injuries caused to the dignity of an individual by breach of Personally Identifiable Information (PII) are as old as the mankind, but that was not as scary then as there were no faster modes of communication. Most of the times, the information could be passed on to others only by word of mouth and in some critical situations, through runners for urgent communications. In the past, the flow of information was slower in pace and limited to restricted groups.

As days passed, the various inventions and means of improved ways of communication, brought more pace to such activities, but still, certain barriers could be laid down in law and practice, to prevent the flow of information to the Criminals. But the current explosion in Information Communication Technology (ICT) enables speedier communication of digital data, including the PII, to entire global space, which has turned out to be disastrous. The use of mobile technology and the increase in the density of smart phone users in India has further aggravated the criminal activities in the cyber world. The digital 'global common' accessible to the entire population, with no respect for territorial or political sovereignty, and with little

restrictions in place has become a dangerous tool to damage the privacy fabric of the society. This technological explosion, giving raise for unregulated rampant information flow and the related activities have resulted in higher cybercrimes also. These changed circumstances have created a situation where the personal data of an individual could be gathered remotely and exploited for meeting the ulterior motives by the cybercriminal within fraction of time. As the growth in use of digital devices have enabled accelerated information communication without any barriers, the present times have caused huge embarrassments and harms to the privacy of persons around the globe.

The laws made by the Nations are territorial in nature, but the crimes committed are universal. The usage of digital technology, open for participation by all and accessible to the entire population, without any obstruction or restriction, has driven the society to a weird situation. The personal information, as of now, require a different standard of protection to avoid damages at the hands of fraudsters. As on date, any information could be shared with the whole world in a flash and this has caused a huge discomfiture for individuals in respect of protecting their personal information, which are essential for a peaceful living. By showing complete disregard and disrespect for the moral, cultural and national values, with scope for anonymous and pseudonymous application possible, the world's biggest information network has turned out to be a paradise for the criminals. The perpetrators of crime, residing in any part of the globe could cause huge harm and damage to an individual's reputation, wealth and mental health exploiting the current technology. The victim may not be able to know who the criminal is and from where such wrongs are being carried out, which further adds to the woes of law enforcing authorities.

The law enforcing authorities are in a state of worry as the existing laws and the international situation do not assist them even a bit to safeguard the interests of the victim and of the society in general. It has equally become a cause of serious concern to every user, to find effective ways and means to prevent and combat the unregulated illegal flow of data worldwide. In view of the changed circumstances and free flow of information in a breakneck speed, there is phenomenal increase in Cyber-Crime followed by Cyber-Terrorism and Cyber- War in the present society. There are state players encouraging and backing such criminal activities which cause a huge threat to the entire mankind. Therefore, there is urgent need for suitable privacy protection laws to enforce fairness, transparency and accountability for aggregation and usage of personal data in India and across the world, so that such cyber-crimes could be identified, contained and the victims could be sufficiently protected and safeguarded.

Privacy protection in India

As on date, in India, there is no standalone and comprehensive privacy law for the protection of personal data of an individual. The Information Technology Act 2000, (IT Act) as amended, has limited scope for protection of Personal information of individuals by the corporate engaged in the data related activities. The IT Act, in addition to regulation of the electronic applications, storage, processing, authentication as well as electronic contracts, e-commerce, cyber offences and liability of network service providers, provides protection in respect of digital data or information concerning the privacy of an individual. The Sections 43, 43A, 72 and 72A of the IT Act read with "The Information Technology (Reasonable Security Practices and procedures and Sensitive Personal Data or Information) (SPDI) Rules 2011 are the

provisions that cover the matters relating to ‘sensitive personal data’ protection. The IT Rules define personal information which consists of information relating to: ‘Passwords; Financial information such as bank account or credit card or debit card or other payment instrument details; Physical, physiological and mental health condition; Sexual orientation; Medical records and history; Biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise’. The Section 43A and the SPDI Rules apply to 'body corporate', requiring them to maintain reasonable security practices and to follow the due diligence principles while possessing, dealing, or handling data in a computer resource. In view of the general protection provided, one can conclude that the IT Act does not exclusively deal with the ‘right to privacy’.

The adjudication mechanism for redressal of privacy violations under the said provisions have also failed miserably as the commercial interests blocked the quasi-judicial justice delivery mechanism pertaining to individual rights. The adjudicating authorities are busy attending to various other functions under the Ministry, except sparing time for deciding matters relating to protection of privacy of a citizen as stipulated under IT laws. The adjudicating officers have remained non-performers, with no inclination to attend to the complaints of the individuals on privacy rights violations. The victims have stopped complaining to the authorities as no outcome could be expected from such exercise. There are no one to listen to individual privacy rights violation and redress as per law in force. The Author earnestly feels that similar situation is going to happen on the proposed combined data regime, as nothing different could be expected by the newly formed joint authorities as they, as usual, prioritize and attend to commercial needs, rather than to attend to restoring the individual’s right.

Speaking on the precarious situation created due to non-performance of information secretaries, Naavi, the cyber law expert observes, “It now appears that all adjudicators have lost interest in such cases, and it is very difficult to suggest cybercrime victims to approach the Adjudication. The Cyber Judicial system has irrevocably failed.” There is little hope for the citizen to seek protection from the combined data authority proposed in the combined regime in the delivery.

Post- Puttaswamy developments

The voyage for an exclusive privacy law in India started in 2012, when a case was instituted by Justice K.S. Puttaswamy, (petitioner) a retired judge from Karnataka, in relation to the Aadhaar Project, of the Unique Identification Authority of India (UIDAI). The Aadhaar scheme is linked with several welfare measures, with a view to streamline the process of service delivery and to get rid of false beneficiaries. The Aadhaar data, among others, involved privacy information of all Indian citizens, which could be misused by any person who has access to such crucial information. The petitioner challenged the constitutionality of ‘Aadhaar project’ on the ground that it violates the right to privacy of an individual. Over the time, other petitions challenging different aspects of Aadhaar by others were also referred to the Supreme Court. As it was a question of law having impact on life and liberty, it got referred to a larger bench of nine judges.

The Supreme Court, after due process, passed the historic judgment on 24th August 2017 [Justice K.S. Puttaswamy v/s Union of India [(2015) 8 S.C.C. 735 (India)], affirming the constitutional right of a citizen to protect her / his privacy. The Court held that the privacy of

a person is a fundamental right flowing from the right to life and personal liberty as well as other fundamental rights securing individual's liberty. Further the individual's dignity is cited as the basis for extending it the status for it as a fundamental right. The Article 21 mandates that, "No person shall be deprived of his life or personal liberty except in according to procedure established by law". Such fundamental right cannot be taken away from the citizen by any private entity or government as doing so will be in violation of fundamental rights guaranteed under the Constitution. The judicial remedies are available to the victim through writs under article 32 and 226 of the constitution.

Further, the Supreme Court clarified that the right to privacy is not an "absolute right" but may be subjected to reasonable restrictions in certain situations. For using such restrictions (i) there must be existence of a genuine state interest ;(ii) such restriction should be proportionate to the interest;(iii) and it shall be through valid legislations.

Justice (Rtd) B N Srikrishna report

During the proceedings of the said case, the Government of India set up an expert committee, headed by Justice (Rtd) B N Srikrishna, in August 2017 to examine issues relating to data protection, recommend methods to address them, and draft a data protection Bill. After due public consultations, the committee submitted its report along with a draft Personal Data Protection Bill 2018 on July 27, 2018.

The Committee observed that the regulatory framework must balance the interests of the individual with his personal data and the interests of the entity such as a service provider who has access to this data. It further noted that the relationship between the individual and the service provider must be viewed as a fiduciary relationship. This is due to the dependence of the individual on the service provider to obtain a service. Therefore, the service provider processing the data is under an obligation to deal fairly with the individual's personal data and use it for the authorized purposes only.

The opening remark of the report captures the purpose of the protection of personal data as follows: "This report is based on the fundamental belief shared by the entire Committee that if India is to shape the global digital landscape in the 21st Century, it must formulate a legal framework relating to personal data that can work as a template for the developing world. Implicit in such a belief is the recognition that the protection of personal data holds the key to empowerment, progress, and innovation. Equally implicit is the need to devise a legal framework relating to personal data not only for India, but for Indians." The committee's recommendations included, "set up a Data Protection Authority (DPA) which will be an independent regulatory body responsible for the enforcement and effective implementation of the law. Broadly, the DPA shall perform the following primary functions: (i) monitoring and enforcement; (ii) legal affairs, policy and standard setting; (iii) research and awareness; (iv) inquiry, grievance handling and adjudication. The DPA 's Adjudication Wing shall be responsible for adjudication of complaints between data principals and data fiduciaries" [Section 68 of the Bill].

Formation of PDP Bill, 2019

The Union Government, after certain modifications, introduced the 'Personal Data Protection (PDP) Bill, 2019' in the Lok Sabha on 11th December 2019. This Bill proposes to provide a legitimate structure for protection of personal data of individuals and regulatory framework for

collection and processing of such data by various agencies, through an establishment of a Data Protection Authority (DPA).

The PDP bill 2019 consists of 98 clauses and one schedule, distributed among 14 chapters. In the preamble, the objectives of the bill stated as: "A BILL to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organizational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorized and harmful processing, and to establish a Data Protection Authority of India for the said purposes..." It further asserts that, "the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy. The growth of the digital economy has expanded the use of data as a critical means of communication between persons and therefore it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion ….".

Personal data under PDP Bill

The term "data" includes a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means. The personal data collected in the traditional way, using non-digital mode [paper pen method] are also covered under the scope of the bill, as above definitions indicate. The clause 4 of the PDP bill states that, 'no personal data shall be processed by any person, except for any specific, clear, and lawful purpose'.

The "personal data" has been defined as data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute, or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling [clause 3 (28)]. The '(i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorized as sensitive personal data under section 15 by the authority and the sectoral regulator concerned' are treated as "sensitive personal data"[clause 2 (36)].

Rights of the Data Principal

One more important factor to be noted is that the protection under this proposed legislation is limited to the personal data. The definition of personal data covers any inference drawn from personal data for the purpose of profiling since such inference typically leads to indirect identification of a natural person. The natural person to whom the 'personal data' relates is termed as "data principal"[clause 3 (14)].

The entities that collect and / or process a data relating to a principal are called as "data fiduciary, which include the State, a company, any juristic entity, or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.

The "data processor" means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary.

The primary objective of the bill is to safeguard the right to privacy of the citizen / Data Principal. The Data Principal, in respect of the personal data pertaining to him / her, has the following rights:

- Right to confirmation and access to the personal data with the fiduciary;
- Right to seek correction of inaccurate, incomplete, or out-of-date personal data;
- Right to have personal data transferred to any other data fiduciary in certain circumstances. [Data portability];
- Right to restrict continuing disclosure of their personal data by a fiduciary if it is no longer necessary or consent is withdrawn;
- Right to receive the data from the fiduciary in a machine-readable format.

The Bill proposes for setting up of a Data Protection Authority (DPA) who may, (a) take steps to protect interests of individuals, (b) prevent misuse of personal data, and (c) ensure compliance of concerned with the Bill.

Obligations of Data Fiduciary

The Bill allows the processing of data by Data Fiduciaries / Data Processors only after consent is obtained from the individual / principal for which there is need of issue of a notice by the fiduciary to such person, stating the reasons in clear, concise, and easily comprehensible terms. Further such activities should be carried out, restricted to such purposes as consented, in a fair and reasonable manner, to ensure the privacy of the data principal. A personal data can be processed only for specific, clear, and lawful purposes only. The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it was processed and shall delete the personal data at the end of processing. In addition to the above stipulations, all fiduciaries should undertake certain transparency and accountability measures such as: (i) implement data security safeguards, such as data encryption and preventing misuse of data. (ii) Set up grievance redressal mechanisms to address complaints of individuals. The sensitive personal data may be transferred outside India for processing on explicit consent by the individual, and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India. Certain personal data notified as 'critical personal data' by the government can only be processed in India.

The Bill mandates that a data fiduciary is required to formulate a privacy by design policy. The data fiduciary should submit its Policy to the Authority for certification in the prescribed manner and display the certified Privacy Policy on their websites. Each company classified as significant data fiduciaries will have appoint a Data Protection Officer (DPO) who will liaison with the DPA for auditing, grievance redressal, recording, maintenance etc.,

Processing of personal data is also exempted from provisions of the Bill for certain specific purposes such as: (i) prevention, investigation, or prosecution of any offence, or (ii) personal, domestic, or (iii) journalistic purposes. However, such processing must be for a specific, clear, and lawful purpose, with proper safeguards. Offences under the Bill include, (i) processing or transferring personal data in violation of the stated law and (ii) failure to conduct a data audit.

The Processing or transferring personal data in violation of the Bill is punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher. The failure to conduct a data audit is punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher.

The Officers in the DPA are vested with the power to call persons concerned for inquiry into fiduciaries, assess compliance, and determine penalties on the fiduciary or compensation to the principal. The Adjudication decisions, which are quasi-judicial in nature, can be appealed in the appellate tribunal and appeals from the Tribunal will go to the Supreme Court.

The provisions relating to obtaining consent of the principal to collect personal data may have to be followed in a scrupulous manner so that the strict compliance to the privacy law is followed. The entities classified as data fiduciaries should determine the purpose and means of processing personal data in a fair manner as stipulated in the law. Organizations will have to undertake a great deal of technical changes in engineering the existing architecture to modify business processes to meet the requirement of the proposed law. They need to place limits on data collection, processing and storage and similar responsibility they owe to the principal. There is need of proper encryption of personal data along with technical security safeguards, including de-identification i.e.., preventing an individual's identity to be inadvertently revealed to prevent instances of data breach. All personal data (characteristic, trait, attribute, or other feature of the person) online or offline, shall require the explicit and informed consent of the individual to whom it belongs to before such data can be collected or subjected to any form of analysis. This may cause huge disruption in the businesses and organizations that thrive on processing and monetizing data collected from the individuals.

The bill was referred to a joint parliamentary select committee for scrutiny and report, after suitable consultation with all stake holders.

Influence of Kris Gopalakrishna Report

Any data which is not a personal data (data pertaining to characteristics, traits, or attributes of identity, which can be used to identify an individual) has been categorized as non-personal data (NPD). In terms of origin, non-personal data can be data which never related to natural persons (such as data on weather or supply chains), or data which was initially personal data, but has been anonymized (through use of certain techniques to ensure that individuals to whom the data relates to cannot be identified). The Ministry of Electronics and Information Technology (MeitY) had set up the committee headed by Mr. Kris Gopalakrishnan to regulate and to set up a framework to unlock the economic value of such NPD and to address the concerns arising thereon. The constituted Expert Committee submitted its report in July 2020 and further revised as required. The Committee observed that NPD should be regulated to: (i) enable a data sharing framework to tap the economic, social, and public value of such data, and (ii) address concerns of harm arising from the use of such data.

The Committee observed that even when personal data has been anonymized, the possibility of harm to the original data principal exists as no anonymization technique is perfect. In view of such a situation, the report viewed that it is necessary to address privacy concerns arising from possible re-identification of anonymized personal data, to ensure no harm is caused due to such processing. The Committee recommended certain categories of data to be considered as sensitive based on the risks: (i) NPD which is derived from sensitive personal data (such as

health, caste, or tribe) which bears a risk of re-identification, (ii) data which bears risk of collective harm to a group, and (iii) data related to national security or strategic interests. The committee recommended for formation of a regulatory authority called NPD Authority for putting in place the framework for governance of non-personal data. The Authority will be responsible for framing guidelines with respect to data sharing and risks associated with non-personal data.

The expert committee on 'non-personal data governance (NPDG) framework' has suggested harmonization of authorities for data protection, and having one authority, if need be, for personal and non-personal data, as they opined, "we said (in the report that we can have), separate authority, but look at all (data) authorities and make sure that you harmonize them. If need be, have just one authority for all data."

Delay by JPC recommendations

The PDP Bill referred to a Joint Parliamentary Committee ("JPC") on December 12, 2019, after nearly 2 years of deliberations, tabled its report on December 16, 2021. The JPC Report lays down various recommendations and modifications to the PDP Bill. The revised version now referred to as DPA 2021 (could also be renamed as DPA 2022) is said to be ready for final debate in the Parliament and for being passed into a law, which is awaited since then. The joint parliamentary committee also set deadlines for implementation: 'the Data Protection Authority should be active within six months, registration of "data fiduciaries" within nine months, and all provisions of the Bill to be implemented within 24 months', which appears to be impossible by viewing the pace of activities of the administration at the backend.

Like all laws that have a significant impact on the society, the PDPA 2019 (now renamed as DPA 2021), has been facing uncertainty due to many reasons among which the data exploitation for commercial interest are in the forefront. The proposed merger PDPA with NPD has been presented in a distorted way, creating hesitation in the minds of the industry professionals as to whether such amalgamation is desirable or not. This has resulted in many organizations delaying the planned implementation of the privacy compliance regime.

Weakening of the Privacy Law

As stated, the JPC has recommended inclusion of NPD within the scope of the recommended Bill and there is lack of clarity on the interplay of NPD with personal data and privacy protection in the New Bill. Section 2 (d) has been added mandating that 'the provisions of this act shall apply to the processing of non-personal data including anonymized personal data'. However, the actual changes made in different operating sections are limited to Section 25 related to the reporting of data breach of non-personal data to the Data Protection Authority of India (DPAI) along with the breach of personal data. It is proposed that the regulations on NPD will be drafted in due course.

Combining the privacy data protection measure with the NPD regulation made for commercial purposes is a disastrous event as the objective of both the frameworks are farthest. Further as the governing measures of NPD are yet to be formulated will need more time, which is going to add to the delay of the privacy law-making process.

The principal objective of the legislation of protection of personal data is to restore the fundamental rights of a citizen whereas the intention of governance of NPD is to exploit the

data, including anonymized personal data for pecuniary benefits. The privacy protections laws are citizen centric whereas the NPD governance is fiduciary centric profit-oriented regulation. As the purpose of the legislation are meant for serving different category of persons, bringing them together to usher a uniform legislative remedy puts the personal data in a dangerous position of dilution and diversion. The concerns of an individual are going to be neglected, as the interests of the commercial organizations are going to occupy the full space of the DPAs. This will once again lead to a suffocating situation which is existing, at present, in respect of adjudication process of personal information breaches. This is totally unfair as it fails in timely restoration of the fundamental rights of a citizen, which is the main purpose of the privacy legal framework planned as per the recommendations of the Srikrishna commission. Such an unholy fusion deprives the individual a means of fair justice in cases of privacy violations. This is not in line with the decision of the Apex court. The legislators' silence in not rescuing the citizen from the diabolic blending is deplorable.

Where a data breach incident involves either the personal and NPD, the data fiduciaries and processors need to report such an incident to the common DPAI. The DPAI reserves the right to give appropriate directions to the reporting company/organization on the action to be taken. The inclusion of non-personal data at this stage is premature, especially for the business ecosystem in India. Businesses are grappling to understand the nuances of this new experiment, where personal data and NPD are treated to similar process even though they are intended to serve different purposes. Personal data needs to be protected through a unique contractual obligation of an individual with the fiduciary and processors for collecting and processing, wherein the protection of fundamental rights of the principal is of utmost importance. As against this, the governance and commercial exploitation of all NPD, is between the authorities and the fiduciaries, and participation of the individuals in this framework may not arise, except in rare cases of such issue arising out of use of personal data at certain situations. The goal of governance of NPD is mostly for unlocking economic benefit from non-personal data, creating a data sharing framework, establishing community-based rights over NPD and addressing potential harms to privacy due to misuse of data (3.5, Revised Report). A better solution in this regard could be to have a regulator i.e., the Data Protection Authority, who shall primarily enforce the personal data protection law, which is ready for legislation. Subsequently, the regulator could also be nominated for governance of data in respect of NPD, once it is gets evolved.

Preparing for the combined data regime

In such an ambiguous environment, it is natural for organizations to be uncomfortable with a regulation and more so when the regulation requires a re-structuring of some of the existing business architecture. The privacy regulations which are the global norm, are inevitable and they should not be either delayed or avoided for the sake of evolving scheme of commercial exploitation of the NPD. Most of the multinational companies are already adhering to privacy protocols of various other countries. If NPD is included in the New Bill as recommended by the JPC, foreign businesses may have to re-structure their data architectures for India, which will spoil the business opportunities of Indian entities further.

In case the government accepts the recommendations of JPC the challenge to the fiduciary will be to design a Unified Framework for entities in the Indian jurisdiction to be compliant with

all Personal Data Protection laws and include some aspects of compliance of Non-Personal Data protection which is part of DPA 2021. As many countries around the globe start to enact and implement personal data governance regimes, this bill will have an important role in shaping the regulation governing today's increasingly data-driven geopolitical landscape. So, irrespective of the media campaign against the immediate introduction of the bill DPB 2021 in the Parliament, industries need to look for ways to build the path towards compliance.

The Foundation of Data Protection Professionals in India (FDPPI) is an organization dedicated to the cause of "Data Protection" in India and building a Data Protection compliant environment through the "Data Protection Compliance Management Systems". The "Data Protection Compliance Management Standard of India (DPCMS)" focusses on the compliance of DPA 2021 incorporating the best principles of other international frameworks have been developed by professionals of FDPPI. It is time for business entities to start equipping themselves with the standards evolved by FDPPI so that the organizations are ready to comply with the DPA legal regime.

Governments move towards Building a Data Governance Structure

By Naavi

The Government of India is well aware that when the Data Protection Act is passed, more than the corporate sector, it would be the Government sector which would be facing the biggest hurdles in compliance. Government is the largest repository of personal data of citizens and it will continue to be so in the future also.

Despite the exemptions made available in the Act for consent under Section 12 of the DPA 2021 (The version of the personal Data Protection Bill approved by JPC), Government is aware that as soon as the law is passed, a battery of advocates would mount attacks on different departments of the Governments both at the Center and the States as well as the public sector organizations with all sorts of complaints on infringement of Privacy. More than any body else, the Government needs the two year time for implementation of data protection policies in its establishments.

Recognizing the risk therefore, the Government is taking steps to introduce some measures to ensure that it can move towards preparing itself for the Data Protection era. As a step in this direction, Government of India has published a "Draft India Data Accessibility and Use Policy" which is a "Data Governance Policy" for the Central Government undertakings. The Government has also suggested that every state should independently start developing their own policies for Data Governance so that developing Data Protection policies becomes easier.

The draft policy now released for public comments has indicated the following objectives.

1.Maximising access to and use of quality public sector data

2. Improving policy making, evaluation and monitoring

3.Enhancing the efficiency of service delivery

4. Facilitating the creation of public digital platforms

5. **Protecting the privacy and security of Citizens**

6. Streamlining inter-government data sharing

7. Promoting transparency, accountability and ownership in data sharing and release

8. Building digital & data capacity, knowledge & competency of Government officials

9. Promoting data interoperability & Integration to enhance data quality and usability

10. Ensuring greater citizen awareness, participation, and engagement with open data

11. Enabling secure pathways to share detailed data sets for research and development

12. Increasing the availability of high value data sets of national importance

13. Improving overall compliance to data sharing policies and standards.

The objectives indicate that the Government is focussing on using data efficiently for enhancing its Governance, prepare itself for regulated disclosure of data, and also start working on protecting the Privacy of citizens.

The policy recognizes the need for greater citizen awareness, participation and engagement with open data and build , knowledge & competency of Government officials.

For implementing the Data Governance plan at the Central Government/Ministries level, a new entity called "India Data Office" would be set up and every Ministry/Department will have Data Management Units headed by Chief Data Officers (CDO) which will work closely with the IDO.

While there is no mention of a "Data Protection Officer" as such, it is likely that each of the Chief Data Officer would like to entrust the responsibility of Data Protection to a suitable officer so that there is greater accountability and efficiency.

The India Data Officer and the Chief Data Officers will function as a "India Data Council" and manage the Data Governance in a collaborative spirit.

Simultaneously the State Governments are expected to take similar steps so that a State Data Officer with State department level Data Officers forming a State Data Council.

The concept is very innovative though the implementation requires lot of effort.

It is noted that one of the first states to respond with a similar policy is the State of Tamil Nadu which released a final approved policy called Tamil Nadu Data Policy 2022.

The Tamil Nadu Data Policy (TNDP) is built on 13 key principles such as

1. Openness,
2. Privacy, Ethics and Equity,
3. Flexibility,
4. Transparency,
5. Legal Conformity,
6. IPR protection,
7. Interoperability and Standards,
8. Quality,
9. Security,
10. Accountability and formal responsibility,
11. Sustainability and Usability

The policy would be applicable to all the public authorities under the RTI act within the State of Tamil Nadu. TN e Governance Agency (TNeGA) will be the nodal agency to monitor the policy. A state level Empowered Data Governance Committee chaired by the Chief Secretary will provide the strategic guidance. The CEO, TNeGA will be the State's Chief Data Officer

(CDO) and there will be a Data Inter-Departmental Committee to take operational level decisions.

The Central Government and TN Government have shown that the concepts of being "Data Driven" for decision making is not the preserve only of the private sector. They have also shown that they are not bogged down by "Complacency" and are ready to start working towards the onerous task of Data Governance and Protection at the Government level even as parts of the private sector is still dithering on whether they should start their compliance activity or wait for the Act to become effective.

We need to see how other States including Karnataka, Maharashtra, Telengana etc. respond to these developments.

Sectoral Codes of Practice

By Naavi

Compliance to any law is an effort for a business entity. It is natural that any business entity will consider forced compliance as a pain and a disruption of their day to day activity. It does also involve additional cost. Hence a resistance to change is a natural reaction of the industry when a major law like DPA 2021 is proposed.

Some laws like DPA 2021 directly affects the technology architecture and the Governance structure of a company. It is not a simple change of law that the legal department can manage with a few internal policy communications being issued. It requires finding of a senior employee to be designated as a DPO, making changes in the data collection, processing and retention mechanism, introducing new training measures for the employees, introducing measures to conduct background verification on vendors, pre-purchase audit for hardware and software etc. Obviously the companies have a resistance to the introduction of the new law and would wish it does not come for some more time.

When framing such laws the law makers have a challenge that the law should be uniform for all segments of the stakeholders but have no option to frame one law for all and provide for a few exceptions for small entities or law enforcement etc. But the impact of the law would vary depending upon the capacity of the stakeholder to bring the necessary changes in their business systems. Hence a law meant for SBI would be a huge burden for a smaller Bank. Law that can be implemented by Taj Hotels would be a burden for the local hotel. Law which Fortis can implement is an impossible burden for a small nursing home.

Presently one of the exemptions provided under the Act is a limited exemption under Section 39 which exempts non automated processing by "Small" entities from the provisions of issuing a notice, about updation, retention, the rights and transparency measures. However the exemption is not available for "automated processing" .

A "small" entity could be defined through notification and may take into consideration not only the turnover of an organization but also other aspects such as the sensitivity and volume of data processed.

"Automation" in this context is related to "automated decision making" and hence care should be taken by "small" entities to ensure that they donot mindlessly grab an AI tool because it appears fancy as it would open up their compliance obligations.

DPA 2021 has however provided an opportunity for the industry to soften the impact of the law by proposing that the industry may develop their own "Codes of Practice" under the broad guidelines provided under Section 50 which may be approved by the Data Protection Authority if found acceptable.

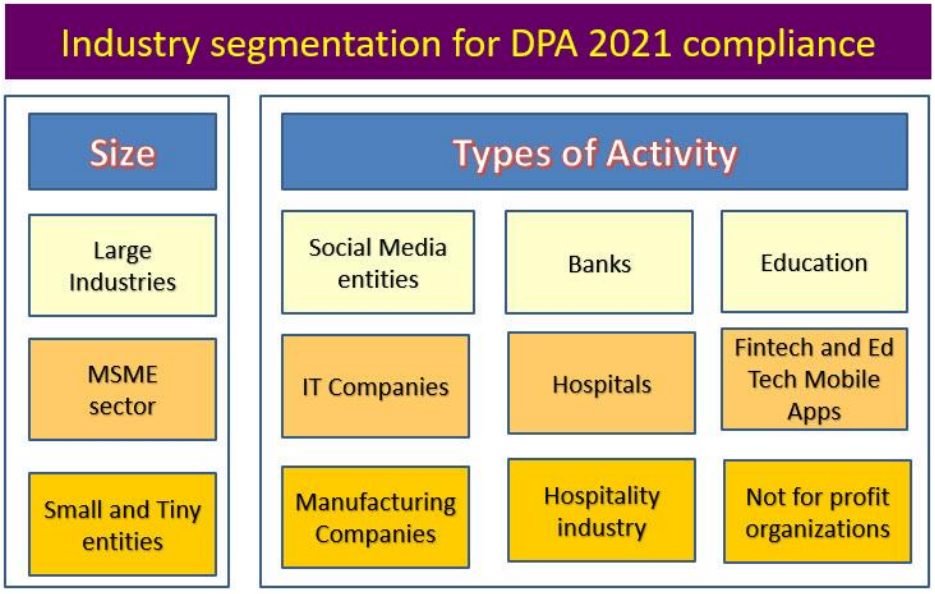
Under Section 50, associations representing industry or trade or the interest of data principals or technical service organizations may submit codes of practice to promote good practices of data protection and facilitate compliance with the obligations under this act. Even the sectoral

regulators or any department or ministries of the Central or State Government can develop and submit such codes of practice for approval.

FDPPI as an organisation of the Data Protection Professionals formed as a Not for profit Company intends to lead the initiatives from the industry to develop such codes of practice and make an attempt to get it approved at the appropriate time by the Data Protection Authority.

In this context, FDPPI is encouraging the industry to join hands with FDPPI by setting up Special Interest Groups for different sectors to work on the development of codes of practice for a given segment of the industry. FDPPI will work with its corporate members to identify some sectors relevant to the corporate member so that their industry experience can be factored into the development of the sectoral code of practice. At the same time, this will provide an opportunity for the industry partner to engage himself in an activity which will project him as a leader in the given segment for Privacy and Data Protection initiatives.

For the purpose of this project industry may be segmented based on different types of activity and different sizes of activity.



FDPPI already has an umbrella compliance model called “Data Protection Compliance Standard of India” (DPCSI), which looks at compliance of a “Data Protection Compliance Management System” (DPCMS) based on the applicable laws. In India “Applicable law” is focussed on DPA 2021 and includes ITA 2000. In the event an organization handles data coming under laws such as GDPR or HIPAA, the DPCMS should accommodate the requirements of such laws also so that there is a “Unified system of compliance” that the organization may pursue.

The process of identifying interested industry partners in different industry segments has started and the SIGs will soon be formed in “Insurance Broking”, “Retail Fashion industry”, “Housing Societies”. We hope that within the next six months when the DPA is likely to come into existence, FDPPI will have a few COP s ready.

Neuro Rights..opening a new debate

By Naavi

India entered the domain of Cyber Laws on 17th October 2000 with the notification of the Information Technology act 2000 (ITA 2000). Several amendments were passed on this act in 2008 effective from 27th October 2009. These amendments gave a strong "Information Security and Data Security" posture to ITA 2000. Concepts of "Reasonable Security" and "Due Diligence" became part of the law and gave a compliance direction to the law.

With the concept of "Due Diligence", the compliance goal post became a moving target with every advancement in technology and global laws. It was therefore possible for Courts to start picking ideas from PDPB 2019, a bill pending in the Parliament and discuss the "Right to forget" in some judgements. For the same reason, even though DPA 2021 is still a bill to be passed, it is considered as a due diligence guideline to be incorporated in the compliance framework for a company.

Despite this flexibility with which we can interpret ITA 2000 for new scenarios arising out of technological advancement, there is always a demand for law to be more specific. Hence there is a need to replace Section 43A and its notification with a whole new act-DPA 2021. There is also a demand now for a major amendment to the ITA 2000 itself to accommodate issues arising out of AI, Crypto assets etc.

While we can interpret several aspects of AI or Crypto Assets or any other technological developments including cyber crimes such as ransomware by suitable interpretation of the

current laws itself, there is always a preference in judicial circles to bring a specific legal provision to bring in more uniformity of interpretations.

In this context, we can deliberate if India needs to think on "Neuro Rights Law" as a separate law or work with interpretations of ITA 2000 and DPA 2021 to meet some of the requirements related to the same.

In the DPA 2021, "psychological manipulation which impairs the autonomy of the individual" has been defined as a "Harm" and therefore the entire Act applies to any activity that could cause such a "Psychological Manipulation". It would be interesting to see if this concept of "Psychological Manipulation" can be extended to the concept of "Neuro Rights" which primarily address manipulation of the functioning of human brains with electronic impulses.

Chile is credited to be the first Country in the world to pass a law on "Neuro Rights" in September 2021 to protect the "Mental Privacy", free will and non-discrimination in citizens' access to neurotechnology. The stated aim is to give personal brain data the same status as an organ, so that it cannot be bought or sold, trafficked or manipulated.

There is one view that the development of such law is a little premature since the "Neuro Manipulation Technology" (NMT) is still in its infancy.

There is no doubt that NMT has many positive applications related to medical science for treatment of Alzeimer's decease or even impairments of hearing or vison. But the possibilities of the technology becoming another "Bhasmasura" cannot be ruled out. Today the technology of Crypto Currencies is threatening to destroy our economy. AI and Humanoids may turn into rogue applications and devices like of which are seen in today's movies. Similarly NMT has the potential to transform the human race into a hybrid entity which is ethically and morally questionable.

So far "Manipulation" which is recognized as Cyber Crimes relate to data residing inside a computer which has a recognized owner. When data is changed without the permission of the owner, it is recognized as a "Cyber Crime". Even our Privacy law is built on "Right of Choice" where a person opts-in or opts-out of a data collection and processing environment out of his own free will.

The thought of adding "Psychological Manipulation" as a part of "Harm" was perhaps driven by the Cambridge Analytica experience where a powerful coordinated messaging campaign could brainwash the audience into a chosen behaviour. Inducing a hypnotic state of mind through audio suggestions and visual imagery has been effectively tried in some games such as the "Blue Whale". The new immersive technologies like the Meta Verse have made this hypnotization techniques more sophisticated.

We have also developed and accepted technologies of "Implants" within the body which can regulate heart beatings or blood sugar. Essentially we are already intruding into the human body to interpret the electro chemical changes happening in our organs and convert them into some action. The artificial limbs technology have gone beyond attaching an extendable arm or leg to responsive hand where artificial fingers can be managed with twitches in the arm. In a way these technologies already convert muscular impulses into guiding the fingers to grab or hold an object and otherwise substitute the normal movements of the human fingers.

The new technologies that are triggering the concern for a new law on Neuro Rights is the development of "Chips" which can be implanted on a human which will directly interact with the brain and create sensory perceptions within the brain. These sensory perceptions may be gathered from the sensory devices or otherwise.

To understand the nature of this new technology, we can look at the following example.

Let us assume that there is a computer application that requires a password for access. In the simplest case, the password is entered into the computer in plain text and it may go to the secured application which already has a copy of the password and matches the two to open the access gates.

In a more secured method, the secure application may not store the password in plain text. The plain text password may be converted into a hash at the user's end and the hash is presented to the application which matches it with the hash already in its store and grants access.

In such a hash based authentication system, knowing the hash of a password is sufficient to access the server since the server responds when the right hash is provided. The application may not be able to distinguish if the hash was calculated in real time after the user entered the plain text password in his computer or was replayed from a hash store. Such stored password attacks have been successfully carried out even when biometric was used though technology has now been updated to check if the finger print recognizes an underlying living hand or not etc.

The fact is that access to the secured application can be gained through the input device or directly at the entrance of the secure application.

The “Chip” method of access to the human brain involves an electro magnetic link with which the Chip may be able to communicate with the neurons of the human brain and make the brain think it is seeing some thing or hearing some thing which is not there in the physical world.

This sort of “Brain Signal Manipulation” impairs the functioning of the human brain to see things or hear things which are not real. This is a manipulation of the free will of a person and makes the discussion of “Right of Choice” etc completely meaningless.

The legal issues that are being raised by the NMT is different from the issues arising on the Metaverse, where a person has accused another of inappropriate touch of an avatar causing mental trauma equivalent to rape in the physical society. Here the interaction is between two digital avatars in a digital platform and its equivalence to a physical society action is being debated. But here the perception of the victim is an induced feeling of the pain of the digital avatar as imagined by the victim. It is more in the mind of the victim than otherwise but the perception of shame felt by the victim in a virtual rape of her digital avatar may be as real as the experience of the Blue Whale game player.

Philosophers may however ask what is the difference if you can see things which are not real? As long as the perception is real, it is an experience. For example if you are in the 3D Trick Art Museum in Dubai or the 7D hologram show, the perceptional experience may be as real as it can get. A person may get frightened enough to have a heart attack though the snake he sees may only be an image.

The NMT with embedded chips is much more than the current technologies such as the 7D hologram show since in these technologies, the perception is captured by the normal human eye or ear and transmitted to the brain. In the NMT embedded chip technology, the perception is created directly in the brain and hence it is indistinguishable from real experience.

Once the embedded chips can respond to WiFi signals or the technology advances to the extent that brain manipulating waves can be transmitted through air, brain hacking becomes easier and can be achieved without the need for an embedded chip and a wiring between the chip and the neuro channels within the body.

In the Indian law, under ITA 2000 there is a provision under Section 11 that any electronic record shall be attributed to the person who programs a system to behave in a specific manner. Hence the "Induced Experience" can be attributed to the person who caused the Chip to send the specific signal which induced the experience.

By combining the provisions of ITA 2000 as well as the concept of "harm" under DPA 2021 it is therefore possible to consider that "Inducing mental experiences" is nothing different from introducing a "Computer contaminant" into a computer system. Hence hacking of human brain may be equivalent to hacking of a computer.

The analogy of human brain being considered as a computer is also corroborated by the neuro science. According o neuro science, sensory perceptions travel as electrical impulses and gets transmitted from the nerve edges through the nerves to the receptors in the brain. There after the brain interprets the impulse based on its memory where similar impulses are stored earlier. The Eyes, ears, nose tongue or skin or are like input devices and the mouth may be an output device. The processing in the spinal cord may be similar to the RAM response. The arms, legs and other muscles are like various mechanical devices that may be taking the output from the brain and converting into physical actions.

In view of the above, the "Neuro Rights" in India may be exercisable even under the current laws. However, a thought process has been sown where by a debate on whether a separate Neuro rights law is required in India.

Naavi would invite thought leaders in this domain to contribute to the development of Neuro Rights Jurisprudence in India so that Judiciary can be provided with necessary guidance when required.

Naavi

Jnaana Vardhini

FDPPI conducts periodical webinars under the Jnaana Vardhini series as its effort to continue spreading of relevant knowledge to its members.

In the period upto April 2022, the following programs were conducted

Month	***Date***	***Topic***	***Speaker***
Jan	5	Application of AI in Cyber Security Landscape	Ketan Paithankar
	12	Crown Funding Ventures and data protection	Chet Jain
	19	Data Valuation from the CA angle	Milan Rupchandani , CA
Feb	2	Preparing to be a professional	Sudhakar Reddy Gade
	9	Understanding privacy and ethics on backdrop of technology	Dr Rizwan Ahmed, CTO, Delaplex
	16	Understanding military perspective of privacy laws	Brig. Hemanth Mahajan
	23	Discussion on techno legal aspects of cyber security	Vishwanath PB
Mar	2	EU GDPR- HIPAA comparison	Ramesh Venkataraman
	9	ISO 27002- Impact & Implications	Bondaiah Adepu
	16	Training Manpower and journey of data security awareness in India	Dr Anil Sethi, Ex CIO, ESPN
	23	Securing the modern enterprise/ understanding technology solutions	Unmesh Deshpande
	30	Understanding data privacy from corporate eye	Adv Athul Khadse(Genereal Counsel L'oreal)
Apr	13	Customer Data in Life Insurance	Manju TC
	20	Privacy Quiz	Ramesh Venkataraman
	27	Moot Court	Meena Lall/ Ruchika Kumar/ Tripti Kumar

In addition to the weekly webinars, a panel discussion was conducted celebrating Privacy Day (Jan 28) where industry experts and legal luminaries discussed legal and technical perspectives of data privacy. The Moot Court conducted on April 27 was a novel concept, which garnered much appreciation. The team of Ms Meena Lall, Ms Ruchika Kumar and Ms Tripti Kumar gave a glimpse of the court room drama while presenting a French privacy judgement. We also had a "Quiz Session on Data Privacy" which was conducted by Mr. Ramesh Venkataraman which resulted in an interesting and informative discussion

All videos of the sessions are available at : https://fdppi.in/wp/events-2022/

A Discussion to Remember

K.N.Narasinga Rao

The International Privacy Day, on the 28th of January each year, may not be such a popular day and understandably many would not even notice it. But it was different at FDPPI. There was a buzz with members looking forward for the evening online chat that was organized with Mrs Meena Lal, who is advocate and Chief Legal at Tata Steel speaking to Sr Counsel Mr Sajjan Poovaiah (respectfully referred to as Sajjan further in this writeup) and Advocate Mr Rodney Ryder(respectfully referred to as Rodney further in this writeup). Needless to say the panel discussion was intense and highly informative.

In his opening comments, the candid and expressive Sajjan, said that the data protection bill is an absolute necessity, but the exemptions accorded to the Executive needs to be looked into. He acknowledged the need to honor legitimate state interest, but a certain tempering is essential instead of being absolute. The State, Sajjan said, has to be as much governed by the law as the citizen. The Data Protection Bill has very good provisions but is eroded by the exemption for the Government's collection of data. Sajjan said that it is difficult to state upfront as to what law will succeed and what will fail, and that the bill, though notified, will be a long drawn affair with affected parties and litigants approaching the courts over the provisions.

Rodney, admitted that while surveillance is not an issue, what gets done with the data collected is to be looked into. He said that the digital tools available today for ease of doing things, have capabilities that could be used for sinister purposes. Pouring through enormous amount of text would have taken a lot of time if done manually, but with sophisticated search capabilities, the same can be done in seconds today. He was obviously referring to tools that are used by hackers to execute attacks and tools used for figuring out exploits. On the privacy bill front, Rodney said that the GDPR is gold standard looking at data scrutiny at a stark level, and should serve as such for many legislations across the world.

Madam Meena, then turned the spotlight upon the problem of rapid obsolescence in technology and the challenges of the ever-changing laws. She based her question on 2 core elements – churn in technology, and the statutes which are followed by rules, administrative circulars and judicial pronouncements. Sajjan, significantly opined that a law that works good in a particular period of time and indeed addresses the welfare of society, may fail in a different period and may be considered to be oppressive in a different setting in another time period. He said amendments are inevitable and it may take a decade for the provisions of the Data Protection Bill to stabilize and mature following many amendments. He made a reference to the Insolvency and Bankruptcy Code Bill. The panelists agreed that it is wise to learn from others experience rather than try to experience our own and better to learn from the GDPR.

The next aspect of discussion shifted to the potential mediation bill and how it will exist with the data protection laws. Sajjan expressed pessimism with respect to the effectiveness of mediation. He elaborated that most of the issues with technology is due to the incorrect understanding of the role of the intermediary. He questioned the effectiveness of Right to be Forgotten when so

many CCTVs are recording video of people. He referred to an example of traffic light offence, as to how once the fine is paid, the recording still persists, even though the issue is done and dusted once the fine is paid. Responding to a question from audience about how a balance can be achieved between the needs of national interests on one hand and the privacy of individual on the other, Rodney said that the surveillance cannot be done away with but has to be moderated and tempered. Sajjan said that the digital tools are inevitable to deliver societal needs to the last mile. He said that it is however important to ensure that the use of tools are restricted to legitimate purposes. He emphasized that the citizens have to be sensitized about the consequences of sharing private information to be put in the digital domain. Interestingly, Sajjan mentioned that the elite are more exposed to privacy breaches as they are more into the digital domain as compared to a remotely placed citizen with no access to digital tools.

Madam Meena, asked as a matter of fact – is Right to forgotten a fundamental right at all ?? Rodney, in his response preferred to quote a scenario to drive the point home. He narrated about how a person on his death bed requests his trusted friend to destroy all that he had written in the pages kept in a bundle under the cot. He apparently did not want to be remembered for writing stuff of that kind. His friend reaches out to the bundle and after going through finds the writing to be remarkable and decides not to honor his friends wish of destroying the writing. So Rodney questioned – what happened to the Right to be Forgotten ?? Sajjan opined that the ability to withdraw private information from public domain should form the crux of the need today.

As the curtains were drawn on an absorbing discussion, it could be felt that there were more questions than there are answers in the domain of data protection and privacy. Only time will tell, perhaps …

Thanks,

25th Apr 2022

Narasinga Rao

Q & A

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

Q 1: The Government of India has re-named PDPB 2019 as DPA 2021. Does it mean that ITA 2000 compliance be part of DPA 2021 compliance?

A: DPA 2021 is primarily the law to protect Privacy of individuals. Hence compliance of DPA 2021 will remain its primary focus. This requires compliance to the collection principles, protection of rights, cross border transfer restrictions as well as need to maintain security of the target information under protection and the audit requirements. The Data Breach Notification of non personal data alone is the additional responsibility that comes from the change of title of the Act. However prudence demands that a company should have adequate compliance to ITA 2000/8 since there could be criminal offences and other provisions of ITA 2000/8 regarding retention and disclosure which may have overlapping impact on DPA 2021. These overlapping provisions will be presented as "Legitimate interest" but may be challenged by the DPA. At that time, compliance to ITA 2000/8 may become a necessary defence.

Q2: Why is FDPPI using the terminology "Data Protection Compliance Management System" and "Data Protection Compliance Standard" instead of PIMS etc.

A: Though the basic objective of DPA 2021 is protection of Privacy, the provisions are expressed as different requirements of collecting, processing, sharing and safeguarding of data. Whether the provisions of DPA 2021 will really protect the Privacy or not is a matter of sophisticated legal interpretation. It is considered that Compliance executives may always be dealing with certain grey areas of legal interpretation if they take up the mantle of being able to develop a

"Personal Information Management System" that can protect the privacy of an individual which is anyway not fully defined in law. Hence instead of declaring the objective of the system as "Protecting the Privacy", it is more transparent to declare the objective as to "Comply with the law as prescribed" and leave the adequacy of the law to the Courts on a later day.

Though the provision of the Indian law which recognizes a "Fiduciary" responsibility is meant to be more than a "Check list" compliance, it is considered reasonable for compliance purpose to focus on compliance of the provisions of the law as stated. For this reason and also to maintain a distinction in the approach compared to other compliance tools including the standards such as ISO 27701, FDPPI has adopted the term as "Compliance Oriented". Accordingly, the standard which is a guideline framework is also called "Compliance Standard".

In the context that a Data Fiduciary has a duty to protect the privacy of an individual, it is not possible to completely distance the organization from interpreting the law. Hence it may not be feasible to be reckless and consider interpretation of law in letter is adequate in a given context. Law has to be interpreted taking into account the legislative intent also.

For example, the implementation specifications of DPCSI do include requirements such as Data Valuation being made visible, DTS to be calculated in all cases, Compliance responsibility to be considered as distributed as part of the employee's work responsibility, augmented whistle blower requirement etc which are beyond what is expressed in the letters of the law.