www.pwc.in

An overview of the changing data privacy landscape in India

January 2018

pwc

Table of contents

Executive Summary

Technology is one of the major forces transforming our lives. However, its misuse causes detrimental effects. The digital era has opened up a Pandora's box of various concerns such as Data Theft, Scams, Eavesdropping, Cyberbullying, to name a few, with the overarching concern on the intrusion to the privacy of Individuals.

In an Indian context, various factors such as Nuclear families and cultural views, have for ages, stifled the need for personal space and privacy. However, urbanization, digitization and changing lifestyles have resulted in a growing demand amongst Indians for Privacy and protection of the Information they share, specifically on digital platforms.

In the wake of recent developments and the Supreme Court holding 'Right to privacy' as a fundamental right lays the corner stone for a strong data privacy regime in India. The data protection framework, proposed by the Committee of Experts under the chairmanship of former Supreme Court judge Shri B N Srikrishna, is the first step in India's Data Privacy journey.

While it is not possible to deter the growth and use of technology, it is important to strike the right balance between the digital economy and privacy protection which is the key objective of the Data Privacy Framework.

Technology as an enabler for compliance

The key objective of the proposed data privacy framework is "to ensure growth of the digital economy while keeping personal data of citizens secure and protected". In the current scenario where everything is moving into the digital space, it is important for us to move from manual processes to more automation. In the arena of data protection & privacy, technology serves as a key enabler to ensure and demonstrate compliance. Listed below are 7 key ways that provide Organizations with practical assistance on how to build data protection into technology.

Accountability

In addition to policies, procedures and processes, a well configured and comprehensive technology stack helps an Organization to demonstrate how it protects and safeguards personal data. It is vital for Organizations to plan, assess and evaluate its existing technology stack so that it may be leveraged to ensure and demonstrate compliance with the Data protection law once it becomes effective.

Data Lifecycle management

Many Organizations are assessing existing/ new technical systems to effectively manage the lifecycle of personal data they process within their environment, starting from data discovery to storage, transfer, retention and finally disposal. These systems help Organizations have end-to-end visibility of the personal data received from multiple channels and have control over it. This would go hand in hand in ensuring compliance to some of the key requirements, under the proposed data privacy framework, such as 'Processing Sensitive Personal Data', 'Purpose specification, use & limitation', 'Data Retention & Quality' etc.,

Case Management

Organizations should evaluate and implement technical systems for managing data subject requests, complaints and communications surrounding emergencies including personal data breaches as a step to plan ahead and demonstrate compliance once the proposed framework becomes effective

Data protection by Design or Default (PbD)

Instead of an 'add-on' or afterthought within business operations, protections for personal data will now have to be designed into the very fabric of data processing systems, meaning that entities will need to re-examine how they approach the use of technology in their organisations. (Such as data minimization, data validation, psuedomization, encryption etc).

Assessment of Technology Risks

Before an Organization can make decision on the technical measures it should adopt for data protection, it needs to understand the data protection risk posed by its data processing activities and the wider environment in which it operates. Assessment of technology risks is essential to improve the technology stack of an Organization so that they are better equipped to address the threats that they are exposed to given the nature of service and operating environment. This would require deployment of Technical systems specifically around network security, application security and IT Infrastructure in order ensure personal data is collected, stored and handled in a secure manner.

Active Monitoring driven by Analytics

Organizations should evaluate existing/ new technologies w.r.t to data leakage detection/ prevention, audit logging/ monitoring etc., in order to analyse how personal data is being accessed and used, by whom, and how value can be derived from it.

Breach Management

Organizations should evaluate existing/new technologies which will in real time detect, manage and resolve breaches (e.g. identify breached data, identify impacted users and notify all relevant parties).

Introduction

The world has progressed from the Industrial Revolution, which came about with the advent of rapid industrialisation, to the age of the Information Revolution, which is distinguished by an economy based on information, computerisation and digitalisation.

However, increasing globalisation and digitalisation have brought a lot of challenges. There has been an alarming rise in cybercrimes on a global scale. With India also moving towards a digital economy with the adoption of Aadhaar and an ever-increasing dependency on information, the concerns over cyber security, data protection and privacy are justified.

Further, in the wake of the Supreme Court ruling that privacy is a fundamental right, there is a growing sense of urgency in India to have in place a proper legislative framework to address the concerns over cyber security, data protection and privacy.

Given the growing concerns, the Central Government of India had set up a Committee of Experts, headed by Justice B. N. Srikrishna, to study the challenges surrounding data protection in India and provide their valuable suggestions and principles on which to base the data privacy legislative framework. The objective is to 'ensure growth of the digital economy while keeping personal data of citizens secured and protected'.

On 28 November 2017 the committee released a white paper seeking public comments on the recommendations made on the draft data protection framework.

The paper is divided into three major parts:

- Part II – Scope and exemptions;
- Part III – Grounds of processing, obligations on entities and individual rights; and
- Part IV – Regulation and enforcement.

Each part consists of brief notes on various aspects envisioned to be a part of the data protection framework. Each note, in turn, sets out the key issues that need to be considered, international practices relevant in this regard, provisional views of the committee based on its research and deliberations, and questions for public consultation.

Through this white paper, we have attempted to provide a glimpse of the committee's vision in the data protection framework, along with our perspective on the challenges that may be faced by an organisation in complying with the framework.

The paper released by the committee is based on global best practices on data protection from the European Union (EU), especially the upcoming General Data Protection Regulation (GDPR), the United Kingdom, Canada and the United States.

The paper identifies seven key principles on which the data protection framework must be built:

1. ***Technology agnosticism:*** The law must be technology agnostic. It must be flexible enough to take into account changing technologies and standards of compliance.

2. ***Holistic application:*** The law must apply to both private sector entities and the government.

3. ***Informed consent:*** Consent is an expression of human autonomy. For such expression to be genuine, it must be informed and meaningful.

4. ***Data minimisation:*** Data that is processed ought to be minimal and necessary for the purposes for which such data is sought and other compatible purposes beneficial for the data subject.

5. ***Controller accountability:*** The data controller shall be held accountable for any processing of data, whether by itself or by entities with whom it may have shared the data for processing.

6. ***Structured enforcement:*** Enforcement of the data protection framework must be by a high-powered statutory authority with sufficient capacity.

7. ***Deterrent penalties:*** Penalties on wrongful processing of data must be adequate to ensure deterrence.

1. Scope and exemptions

1.1. Territorial and personal scope

As per the principle of territoriality, a state can exercise its jurisdictional powers within its territories. However, the borderless nature of the Internet raises several jurisdictional issues with respect to data protection. A single act of processing of personal data could very easily occur across multiple jurisdictions (outside the state territory), where the state might not have the authority to exercise its jurisdiction.

To address this, at minimum, the paper states that the data protection framework shall apply to entities (both public and private) within India and processes involving the personal data of Indian residents and citizens. However, extraterritorial applicability and jurisdiction is a major concern.

The paper recognises the need to extend the applicability of the data protection framework to any entity that processes the personal data of Indian citizens or residents irrespective of where they may be located. However, the extent of its applicability is still under discussion.

1.2. Natural/juristic persons

At its heart, any data privacy law has a person (data subject) and that person's right to privacy is what the data privacy law intends to safeguard.

In the eyes of the law, two kinds of person exist:

- a natural person and
- juristic person.

The framework recognises a natural person as a living person. On the other hand, a juristic person is a bearer of rights and duties that a natural person does not have (that is, this person is not a human being) but which is given a legal personality by the law—for example, a company.

The framework provides that the data protection legislation would apply to only to a natural person and not a juristic person.

The paper calls for a distinction between corporate data and certain categories of data held by a juristic person which can reasonably identify an individual or a 'natural person'.

Therefore, for instance, a company's Permanent Account Number or its financial information, being data identifying a juristic person and not an individual, may be excluded from the purview of the data protection legislation.

Key impacts

The law shall apply to:

1. Entities incorporated within India and processing personal data of Indian residents and citizens; and
2. Foreign entities conducting business in India and processing personal information of Indian residents and citizens.

US-based product companies incorporated in India would be subject to law.

E-commerce websites that are not incorporated in India may still be subject to law if they cater to Indian citizens and residents.

1.3. Personal data

The framework defines personal data as follows:

'Data from which an individual is identified or identifiable/reasonably identifiable may be considered to be personal data. The identifiability can be direct or indirect.'

The framework also recognises that data about/relating to an individual that would be the subject matter of protection under the law. It further speculates that data in this context ought to include any kind of information, including opinions or assessments, irrespective of their accuracy.

Additionally, the framework recognises that all data within the category of information identified as personal data is not qualitatively similar. The following definition has been provided for sensitive personal data:

'Such types of data are termed as sensitive, and may include religious beliefs, physical or mental health, sexual orientation, biometric and genetic data, racial or ethnic origin and health information.'

1.4. Public sector vs private sector

The paper recognises that both public and private sector entities process personal data about data subjects. It further identifies the need to protect an individual's informational privacy rights through a comprehensive data protection framework which covers both public sector and private sector entities.

1.5. What about past processing – retrospective application

Compliance with any law becomes mandatory after it comes into effect. The white paper suggests that, ordinarily, the regulation will impact the processing activities performed on data (e.g. collection, use, storage, disclosure, retention) after the legislation comes into force. This means that all processing activities carried out once the legislation is active will come under the ambit of the law.

However, ensuring that the past processing activities are carried out and meet the standards and requirements laid out under the new law remains a challenge.

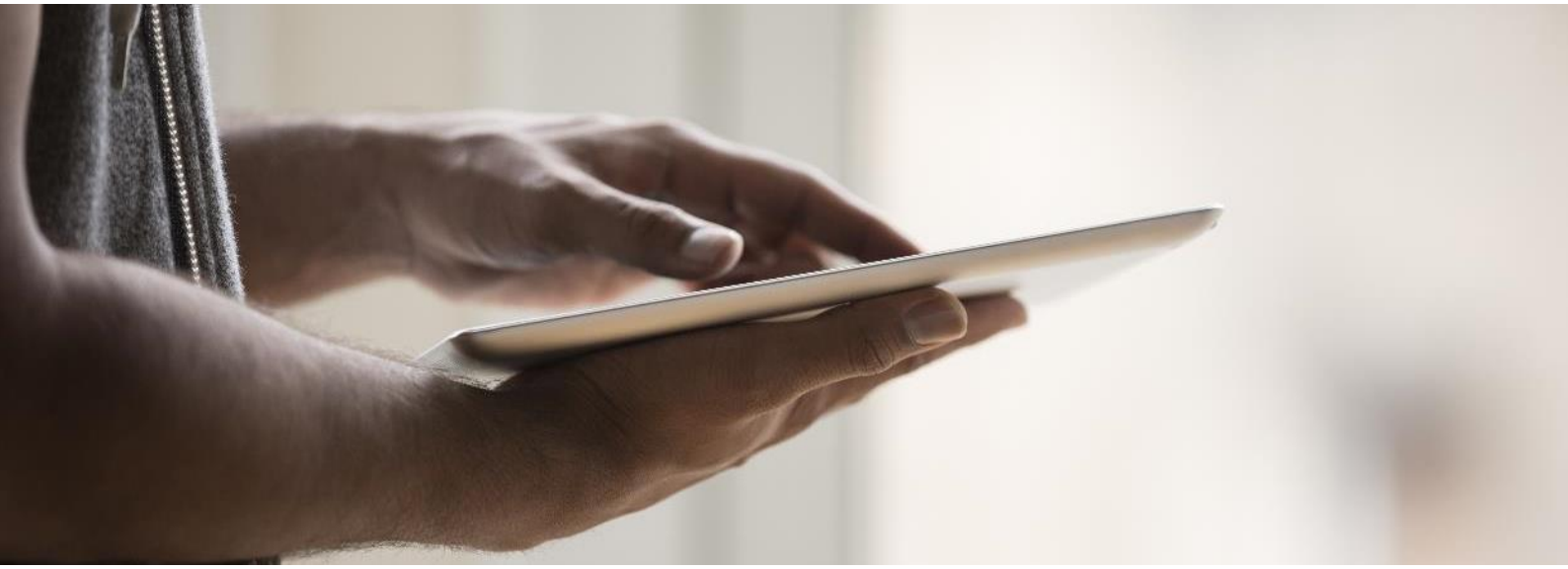
To address this challenge, the paper briefly talks about the concept of a transition period, which is provided to entities to comply with the regulation in a consistent manner.

An organisation that collects personal data from the consumer and determines the purpose and manner in which the personal data is to be used is a data controller.

Personal data can be sent outside the boundaries of the controller for further processing. Organisations that merely store, collect and process data on behalf of a controller are data processors.

Key impacts

1. The framework recognises the concept of data controllers, making it essential for entities playing the role of a data controller to demonstrate accountability.
2. Even though concepts such as data processors and third parties are under speculation, the framework carefully evaluates how these concepts are implemented by various countries, making it imperative for all entities (including processors or third parties) to demonstrate accountability and compliance.
3. Any organisation which transfers data across the borders for any legitimate purpose has to ensure that the data is transferred only to those countries which are identified by the regulators as having an adequate level of protection or ensure another mechanism to provide assurance around the necessary protection.
4. As proposed in the paper, entities shall be required to comply with the legislation once it comes into action. This shall mean implementing a data protection programme in line with the requirements to ensure compliance.
5. Entities shall be required to ensure the integrity and confidentiality of information that is already in the control of the processor as a result of past processing activities (where compliance with the new requirements is not possible).



1.6. What will processing under the new bill imply?

The paper broadly classifies the processing of personal or sensitive data about natural persons into three categories:

- Collection,
- Use,
- Disclosure.

While the law may not attempt to exhaustively list operations that constitute processing, the framework recognises that:

- Processing shall also cover operations/activities incidental to the above operations.
- Processing would imply both manual and automated processing.

1.7. Where does the accountability lie?

Accountability is a central principle in data protection. To translate data protection norms into action, a widely used method is to identify the party accountable for compliance with these norms. For this purpose, the concept of control over data is used.

In such systems, control over data refers to the competence to take decisions about the contents and use of data.

An organisation that collects and processes personal data for its business transactions can fall under two broad categories—data controller and data processor.

The framework recognises the concept of a 'data controller' to ensure accountability. However, the need to define 'data processors', 'third parties' or 'recipients' is currently under discussion in order to define the level of detail with which the law must allocate responsibility.

2. Key concepts put forth in the framework

2.1. Consent

Consent has been globally recognised as an effective means of processing personal data as data subjects use it to allow or deny organisations the right to process their personal data.

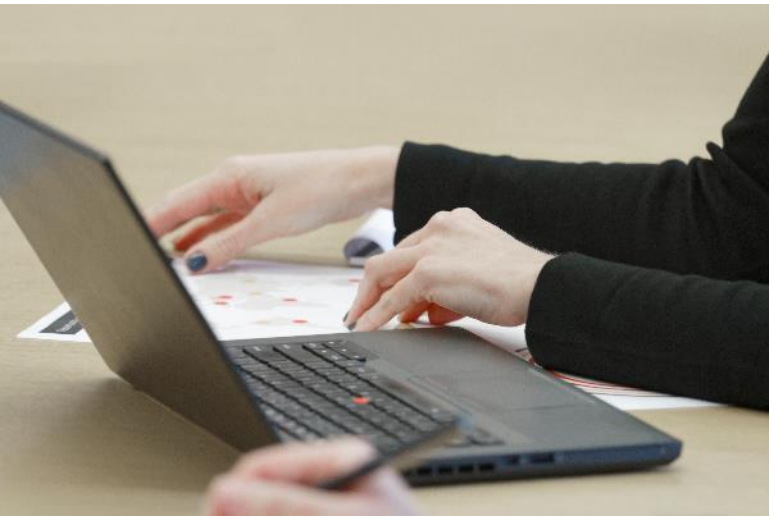
While the framework recognises consent as one of the grounds for the collection and use of personal data, it also puts forth the following views which are currently under discussion:

- Consent should be freely given, informed and specific to the purpose of processing.
- All transactions do not warrant the same standards of consent.
- The validity of consent needs to be carefully determined.

2.2. Other grounds for processing

Although the paper recognises consent as a very important part of data processing activities, it acknowledges the need for other legally recognised grounds to permit the processing of personal data. The paper recognises contractual necessity, compliance with legal obligations, and situations of medical emergency as grounds to permit personal data processing. It also considers other grounds adopted by the GDPR such as:

- Public interest;
- Vital interest;
- Legitimate interest; and
- Other residuary grounds of interest.



Key impacts

The following points need to be considered:

1. Gain visibility on transactions involving collection and use of personal data.
2. Maintain necessary documentation to demonstrate the grounds leveraged for personal data processing.
3. For instances where consent is used as the ground for processing, implement organisational and technical measures to obtain consent:
    - Prior to collection, use and processing of personal data;
    - Retrospective application for existing and previous personal data processing.
4. The framework requires explicit consent to be obtained for the collection, use and processing of personal data.

2.3. Children's personal data

With various advancements, especially in the field of technology, it has been observed that children are becoming increasingly tech savvy. This makes them highly vulnerable to attacks, especially online. The paper recognises that prohibiting the processing of children's personal data may not be the correct approach to address this issue, as it would greatly restrict children from availing of the legitimate benefits of technology, such as academic growth, awareness of world events, and creative expression. The paper has also put forward the following views:

- Need for entities to implement higher standards of data protection;
- Requiring parental consent prior to processing of children's personal data;
- Prohibiting use of children's personal data for potentially harmful purposes, such as profiling, marketing and tracking;
- Establishing rules for the manner in which schools, educational institutions and government bodies handle children's personal data.

E-commerce websites, social networking platforms and travel portals, amongst other businesses, would be specifically impacted by the outcome of this regulation. Specific requirements such as clearly differentiating a child from an adult, parental consent options and higher data protection standards could pose challenges with respect to operationalisation. Organisations therefore need to relook at their current processing methods and tailor their methods to ensure compliance.

Key impacts

Children's personal data

Organisations processing children's personal data, either incidentally or for specific purposes, will be required to:

1. Implement appropriate measures to verify the age of data subjects from whom they are collecting personal data.
2. Implement appropriate measures to obtain valid parental consent prior to processing a child's personal data.
3. Implement appropriate organisational and technical measures to:
    - Secure personal data.
    - Ensure that children's personal data is not utilised for purposes of tracking, advertising and marketing.

Notice

Organisations will be required to:

1. Issue privacy notices to all data subjects prior to the collection or use of their personal data.
2. The notice should be designed in a manner that is easily understood by the data subject.

Keep track of guidelines that may be issued by data protection authorities.

2.4. Notice

Despite considerable discussion on and criticism of privacy notices, the paper recognises it as the means of placing individuals in a position that allows them to make an informed decision about the collection and use of their personal data. Like various laws, the paper provides that a privacy notice should be designed keeping the end user always in mind. Further, it also recognises the need for privacy notices to be concise, intelligible and provided in an easily accessible form. The paper has also put forth the following views that are currently under discussion:

- Define requirements on the form and substance of the notice.
- Require data protection authorities to issue guidelines and codes or practice to guide organisations in designing effective privacy notices.
- Use privacy impact assessments and other enforcement tools to evaluate the effectiveness of privacy notices.
- Assign data trust scores to organisations.
- Set up a consent dashboard to allow greater transparency and visibility to individuals.

2.5. Purpose specification and use limitation

The paper notes that there are several operational issues in ensuring that personal information is only obtained for a specific purpose and the use is limited in alignment with the purpose. It identifies three major issues faced by companies that need to be considered by regulators:

- Technical changes/advancements may result in a new purpose.
- Companies face operational hassles in assessing the delta between the original purpose and new purpose.
- Purpose specification for companies is a challenging activity as data may be used for several related purposes.

The paper recognises this requirement as critical in ensuring individuals rights while limiting the collection, use and disclosure of their personal data. It suggests the use of a privacy notice which provides links to more detailed notice practices and prohibits processing for other purposes. The paper highlights the need for discussion on the following:

- Need to define standards and guidance for data controllers.
- How to determine whether a subsequent use of data is reasonably related to/compatible with the primary purpose.

2.6. Sensitive personal data

The paper notes that there are certain categories of personal data which, if compromised, may result in greater harm to an individual in the form of social, financial and reputational repercussions. The paper recognises this requirement as crucial to protect the interests of individuals when collecting and processing critical data.

However, the paper identifies the following topics for discussion:

- Evaluation of personal types categorised as sensitive under section 43 A of the IT Act (SPDI Rules) in the context of the Indian socio-economic environment;
- Need to identify controls for protection while processing sensitive personal data.

Organisations processing sensitive data, such as medical/healthcare, behavioural, demographic and financial data, will see additional requirements being placed on them under the proposed framework.

The penalties in case of any offences related to sensitive personal data are also going to be higher.

2.7. Storage limitation and data quality

The paper notes that most of the comprehensive data privacy laws and regulations have identified requirements for storage limitation and data quality when handling personal data. However, the paper mentions that this requirement would be identified in the Indian data protection laws at a later stage of maturity.

In addition, the paper identifies the following topics for discussion:

- Need to issue guidelines for clarity of implementation;
- Exception requirements to be identified for data quality and accuracy.

Key impacts

Purpose specification and use limitation

1. Organisations will need to define the purpose of collection and processing of personal data and limit usage of data in line with the purpose.
2. Implement adequate organisational processes and controls to assess that data is used in compliance with the original purpose and identify any new purposes if applicable.

Processing sensitive personal data

1. Organisations will need to define a process to identify and limit the collection of sensitive personal data.
2. Implement adequate organisational processes and security controls (e.g. pseudonymisation) to ensure informed consent by individuals and secure processing of sensitive data types.

Storage limitation and data quality

1. Organisations will need to have a clear understanding of the purpose(s) for the collection and processing of personal data. Based on the purpose, a retention schedule and guidelines will have to be defined and adhered to.
2. Implement adequate organisational processes and controls to ensure the accuracy and quality of personal data collected and processed.

2.8. Individual participation rights

The paper notes that there are three rights to be granted to individuals: right to confirmation, right to access and right to rectification. Further, the paper recognises these rights as important to ensure that personal data is transparent and can be influenced by individuals.

The paper highlights the following points for discussion:

- Need to identify exception requirements where it is not feasible to respond to requests;
- Need to define fees to be paid by individuals for exercising their rights.

2.9. Right to be forgotten

International practices such as the General Data Protection Regulation (GDPR) in Europe and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada envisage the right to be forgotten in some form and manner. The paper also recognises the need to incorporate this right. However, it also highlights the following areas for discussion:

- Need to design the right to be forgotten in such a manner that it adequately balances the right to freedom of speech and expression with the right to privacy;
- Need to determine the scope and extent of such a right;
- Need for sector-specific guidelines for entities in each sector to comply with such requests.

Key impacts

Individual participation rights

1. Organisations will need to have a defined and robust communication channel (internally and externally) to be able to fulfil requests for right to access, right to rectification, etc., within a reasonable time.

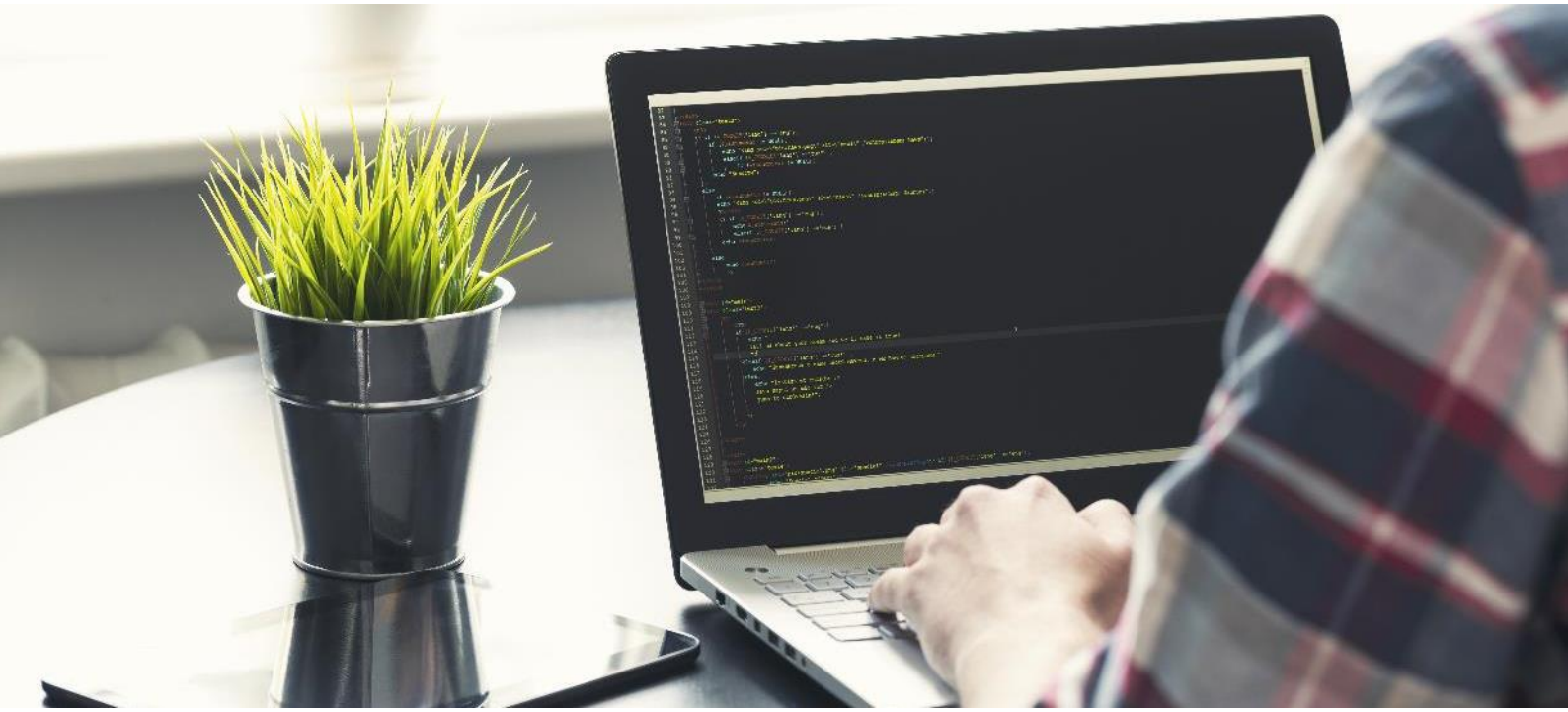
Right to be forgotten

1. Organisations will have to completely map the capture, usage and storage of personally identifiable information to enable the deletion of data based on the request received from the data subject.

Cross-border transfer

Organisations will have to ensure that either:

1. The data is transferred to countries which offer an adequate level of data protection; or
2. Data subjects are offered a level of protection comparable to that they would have received had the data stayed within India.



2.10. Cross-border transfer

The paper sets the context for cross-border data transfer in today's global and digital day and age. It states that data can seamlessly and freely flow across borders. This exchange of data leads to the exchange of information and ideas, which stimulates innovation and drives growth.

The paper lays out two conditions for cross-border data flow:

- Adequacy: Data can be allowed to be transferred to countries which provide an adequate level of data protection.
- Comparable level of protection: Under this, the data controller shall be responsible to ensure that the data is subject to adequate safeguards and that the data will continue to be subject to the same level of protection as in India.

Organisations planning to move their systems onto the cloud may need to gain visibility on data storage locations and also ensure adequate safeguards, where necessary, when such data relates to the personal data of Indian residents.

2.11. Globalisation vs localisation

Under data localisation, entities are required to store and process personal data on servers physically present within their national boundaries. Although this approach helps address concerns over data privacy, security, surveillance and law enforcement, it increases the burden on businesses by way of increased cost of compliance, and may also impact the building blocks of the economy, which rely on data exchange.

The paper aims to take a call on data localisation after considering a cost-benefit analysis between the enforcement benefits arrived at from data localisation and the costs involved pursuant to such requirements.

3. Regulation and enforcement

3.1. Regulatory model

It is very important to have a governmental enforcement and industry perspective when defining a data protection framework. Given this context, choosing the right model for the Indian context is of great significance. Although the paper talks about three models (command and control, self-regulated [US being the best example here] and co-regulated), given the large-scale presence of almost all industries in India, it is imperative to consider industry perspectives while developing a data privacy framework.

3.2. Accountability

The paper primarily focuses on data controller accountability/obligations and brings out, on a very high level, cases where the data controller shall be held liable. However, there is very little or no mention of a data processor obligation, which is also very important in this context.

The paper also touches upon the existing privacy framework in India. Rule 8 of the SPDI Rules mentions the importance of having security controls in place in order to safeguard sensitive personal information. This can only be achieved by having a very comprehensive information security programme in alignment with the current landscape of threats.

Further, the importance of performing regular audits has been discussed in this paper in order to maintain proof of compliance for data controllers. However, the paper does not bring out the periodicity at which the audits are required to be performed.

3.3. Categorisation of data controllers

The paper also calls out various obligations of a data controller, including:

- Registering with the supervisory authority,
- Conducting data protection impact assessments before processing personal data that could pose potential risks to individuals,
- Conducting data protection audits,
- Appointing data protection officers, etc.

However, the paper also understands and emphasises the fact that the above-mentioned aspects can only be applicable in cases where the data controller processes high volumes of data or performs high-risk processing activities.

With respect to data protection audits, the paper proposes that data protection audits may be conducted by third parties or by the regulators themselves. Importantly, the paper also highlights the need for external auditors who are registered/empanelled with a data protection authority to maintain oversight in companies.

Key impacts

The following points need to be considered:

1. To ensure compliance and showcase accountability, data controllers/processors may consider implementing adequate security safeguards (ISO 27001, NIST) or techniques such as data pseudonymisation.
2. Further, organisations may need to implement a governance programme to ensure that processing of personal information is carried out in a legal manner and the necessary proofs of compliance are maintained.
3. The paper proposes that breach notification requirements be dependent on the size and scale of the organisations and the quantum of the data breach. Accordingly, bigger organisations may be faced with the challenge of stringent breach notification requirements, while smaller organisations might be given some leeway with the same.

Like any other regulation across the globe, the paper touches on the need for having adequate security safeguards, along with the importance of implementing the 'privacy by design' or 'privacy by default' concept.

Organisations who are data controllers may be subject to obligations such as:

- Registering with the supervisory authority;
- Conducting data protection impact assessments before processing personal data that could pose potential risks to individuals;
- Conducting data protection audits; and
- Appointing data protection officers.

3.4. Various tools proposed for enforcement

Data breach notifications: The paper calls out the significance of defining a personal data breach and has provided some guidance on it. There is also reference to the EU GDPR and US laws to bring in a broader perspective on a personal data breach, which is nothing but a subset of a security breach. For example, all security breaches may not be data privacy related breaches. However, every personal data breach is a security breach. Thus, it is important to have a comprehensive information security programme, as mentioned in the previous section.

The interpretation of the security framework (such as ISO 27001, NIST) required to offer adequate safeguards to its data subjects is left to the organisation.

3.5. Adjudicating process

The paper stresses the importance of adjudication as an integral part of any law enforcement and ascertains the rights and obligations of parties involved in a dispute, prescribing corrective actions and remedies.

Under a data protection regulation, adjudicating would involve an unbiased assessment of whether an individual's data protection rights have been infringed and, if yes, to what extent?

Various geographies have identified and granted powers to a commission or a supervising authority to regulate and investigate complaints relating to the breach of any rights of a data subject.

3.6. Penalties, compensation and offences

The paper highlights the shortcomings of the IT Act, 2000 (and subsequent amendments to it in 2008 and 2011), in relation to data protection violations. Based on the inputs from other legislations, the paper has put forward three different models for the calculation of civil penalties.

The first two models proposed in the paper mostly refer to the models followed by other regulations. However, the most interesting model is to have penalties per day, which could be the highest form of deterrence, with a major impact on small and medium business (SMB).

With respect to compensation, the paper refers to section 43A of the IT Act, 2000, and clearly calls out factors that are being used by adjudicating officers to arrive at compensation. However, it is very clear that these aspects are only applicable to body corporates and not to government entities and public authorities. The proposed framework should look to have more stringent models around this by adopting similar points from other regulations such as the EU GDPR and the UK Data Protection Act.

Key impacts

1. Penalties for non-compliances may be calculated in a manner that ensures that the quantum of civil penalty imposed acts not only as a sanction but also a deterrent to data controllers who have violated their obligations under a data protection law. The quantum of penalty/compensation is not specified in this whitepaper.

At the given point in time, there is no clarity on what activities could qualify as criminal offences under the proposed data protection framework. The view is that there should be more stringent penalties and compensation in cases where sensitive personal information is recklessly disclosed or sold by organisations.

It remains to be seen how the enforcement model will be designed and how the penalties will be enforced. However, we can reasonably assume that large organisations, such as major telecom, banking, healthcare and IT/ITeS organisations, will need to consider stringent data breach notification norms, along with higher penalty limits in case of any offences.

Conclusion

Given the proposed regulations in the white paper on ensuring the data privacy of individuals, it is very important that organizations start aligning their processes and IT investments in such a way that the regulation, once enacted, does not affect them. Although the paper does not clearly outline anything on past processing activities or retrospective action, CIOs/CISOs are advised to see how capable their existing IT infrastructure is and what it requires to handle the changing data privacy landscape in India.

As the paper is based on global best practices on data protection from the European Union, especially the upcoming GDPR, the United Kingdom, Canada and the United States, organizations can start referring to business cases in these markets and understand how they have defined processes and planned IT investments. In the new data protection regime, timely planning/action will help them to continue their business as usual, protect them from penalties and enhance business reputation, particularly in the light of the proposed data trust scores that will be assigned to organizations.

About PwC

Contacts

Sivarama Krishnan Leader, Cyber Security sivarama.krishnan@pwc.com	***Siddharth Vishwanath*** Financial Services Leader, Cyber Security siddharth.vishwanath@pwc.com
Murali Talasila Partner, Cyber Security murali.talasila@pwc.com	***Manu Dwivedi*** Partner, Cyber Security manu.dwivedi@pwc.com
Sundareshwar Krishnamurthy Partner, Cyber Security sundareshwar.krishnamurthy@pwc.com	***Ramanathan V. Periyagaram*** Partner, Cyber Security ram.periyagaram@pwc.com
Anirban Sengupta Partner, Cyber Security anirban.sengupt@pwc.com	***Rahul Aggarwal*** Partner, Cyber Security rahul2.aggarwal@pwc.com
Unnikrishnan P Partner, Cyber Security unnikrishnan.padinjyaroot@pwc.com	***PVS Murthy*** Executive Director, Cyber Security pvs.murthy@pwc.com
Hemant Arora Executive Director, Cyber Security hemant.arora@pwc.com	***Sriram Sivaramakrishnan*** Executive Director, Cyber Security sriram.s@pwc.com

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 2,36,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

GG/January 2018-11554