Technology Law Analysis

June 04, 2021

DATA PRIVACY STANDARDS ISSUED IN INDIA – LEGAL COMPLIANCE OR NEW BRAND DIFFERENTIATOR?

The Bureau of Indian Standards ("**BIS**") issued new standards for data privacy assurance i.e. the IS 17428.[1] It is intended to provide a privacy assurance framework for organizations to establish, implement, maintain and continually improve their data privacy management system. It is a certification for organizations to assure its customers and employees of its privacy practices, and can be strategically used as a differentiator amongst market competitors. BIS is a national standards body constituted to regulate standardization, conformity assessment and quality assurance of goods and services in India.

The IS 17428 is divided into two parts:

- Part I sets forth Engineering and Management Requirements ("**IS Requirements**") which lay down basic requirements of engineering design and information management and are mandatory in nature; and
- Part II sets forth Engineering and Management Guidelines ("**IS Guidelines**") which provide detailed practices that aid in implementing these requirements and are suggestive in nature.

In absence of the much awaited comprehensive personal data protection legislation, we delve into what this standard would mean for businesses to safeguard personal information in India.

CURRENT INDIAN DATA PROTECTION FRAMEWORK

1. Data protection in India is currently governed by the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* ("**Data Protection Rules**") notified under the *Information Technology Act, 2000* ("**IT Act**"). The Data Protection Rules impose certain obligations and compliance requirements on organizations that collect, process, store and transfer sensitive personal data or information[2] of individuals such as obtaining consent, publishing a privacy policy, responding to requests from individuals, disclosure and transfer restrictions.
2. The Data Protection Rules further provides for the implementation of certain reasonable security practices and procedures ("**RSPPs**") by organizations dealing with sensitive personal data or information of individuals.[3] The Data Protection Rules provide as follows:
    1. Organizations may demonstrate compliance with the RSPP requirement via implementing security practices and procedures and having a documented information security programme and information security policies. These information security policies must contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected;
    2. The international standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is prescribed as one such standard that would help demonstrate compliance with the RSPP requirement;
    3. Codes formed by any self-regulatory organization must be approved and notified by the Central Government; and
    4. Organizations who have implemented standards either as per (i), (ii) or (iii) above would be deemed compliant with the requirement to implement RSPPs upon having audits performed periodically by independent Government-empanelled auditors.
3. The Data Protection Rules prescribe the IS/ISO/IEC 27001 as a standard that may deem compliance with the RSPP requirement. It is also possible that the IS 17428, if implemented, could act as a reference standard that could demonstrate compliance with the RSPP requirement too. We analyse the IS 17428 below.

THE IS 17428 STANDARD

1. At the outset, the IS 17428 clarifies that implementing the IS Requirements is not a substitute for regulatory compliance and the implementation of this standard is a strategic decision taken by the organization. It is also noted that the IS 17428 is formulated based on two current international standards i.e.
    1. IS/ISO/IEC 29100 : 2011 Information Technology — Security Techniques — Privacy framework; and
    2. IS/ISO/IEC 27001 : 2013 Information Technologies — Security Techniques — Information Security Management Systems — Requirements.
2. The IS Requirements broadly require an organization implementing the IS 17428 to follow the specifications provided here:

Research Papers

From Capital to Impact: Role of Blended Finance
June 15, 2024

Opportunities in GIFT City
June 14, 2024

Start-up Governance Essentials
May 30, 2024

Research Articles

Private Client Insights - Sustainable Success: How Family Constitutions can Shape Corporate Governance, Business Succession and Familial Legacy
January 25, 2024

Private Equity and M&A in India: What to Expect in 2024?
January 23, 2024

Emerging Legal Issues with use of Generative AI
October 27, 2023

Audio

Why is the ad industry unhappy with MIB's self-declaration mandate?
June 18, 2024

Incorporation of arbitral clause by reference: Position in India and other Asian Jurisdictions
June 12, 2024

Third-Party Funding: India & the World
April 27, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

Future of India-Mauritius tax treaty – Impact of new Protocol on M&A deals and Private Equity structures
April 23, 2024

1. The IS Requirements provide key definitions of a data controller,[4] data processor,[5] personal information,[6] sensitive personal information,[7] processing,[8] consent,[9] etc for an organization to adequately identify its role and responsibilities. With the aid of these definitions, an organization would need to assess the role that it plays vis-a-vis the relationship of the individual involved whose data is being processed, the nature of the data being processed and to whom the data is being shared to.
2. The organization must incorporate certain engineering and design requirements at the time of the development life cycle of any product, service or solution. These requirements include:
    1. Determining the organization's privacy requirements considering the applicable jurisdiction, regulatory requirements and business needs;
    2. Design considerations based on privacy principles such as collection, use and storage limitations, privacy notice, choice and consent, data accuracy, security, disclosure and transfer, portability, etc; and
    3. Verification and testing of applicable data privacy controls prior to development and at regular intervals.
3. The organization must also establish certain privacy management processes / functions such as:
    1. determine objectives based on the nature of the organization's business, industry domain, nature of personal information and outsourcing policies;
    2. provide adequate resources for the data privacy function within the organization, defining its structure, responsibilities, accountability, communication and governance systems;
    3. establish a system that includes criteria for classifying personal information, inventory and flow of such information, and procedures to introduce new information or change existing attributes;
    4. implement privacy policies, and other processes and guidelines that complement the level of detail involved, exceptions or deviations to processing and accounting of responsibility for every activity in the organization;
    5. record logs and evidence, preserve obsolete policies, and determine the retention period of the data by the organization;
    6. establish a privacy impact assessment methodology that identifies triggers for an assessment, its procedures, tools, techniques and a template to capture the outcome of an assessment;
    7. determine processes to evaluate and shortlist data processes, transfer of data privacy obligations along with contractual transfer of data outside the organization to a data processor and the option for periodic re-evaluation of data processor capabilities;
    8. establish and document a privacy risk management methodology that considers triggers and criteria for a risk assessment within the organization along with a response strategy;
    9. establish and document a mechanism to discover privacy incidents, investigate, report and take corrective and preventive actions;
    10. establish and document a mechanism for the organization to honour individual requests to verify identities, provide access, update or delete a individual's personal information and contractually capture cost and timelines;
    11. set up a grievance redressal mechanism to identify and publish contact information of the grievance officer, set up complaint filing and escalation procedures, and provide timelines;
    12. upskill the relevant staff of the organization handling personal information by laying down their role, establishing accountability, traceability and disciplinary measures;
    13. monitor and review the organization's mechanisms in relation to compliance of applicable regulations;
    14. conduct periodic audits to determine regulatory compliance of the data protection management system of the organization by independent auditors at least on an annual basis; and
    15. set up a documented process to measure and continuously improve the data protection management system of the organization.
3. To ensure compliance with IS 17428, organizations must mandatorily comply with all the specifications set forth in the IS Requirements unless they can demonstrate that certain sub-clauses do not apply to them based on an evaluation and such demonstration must be documented. The IS Guidelines are only recommendatory.
4. The IS Guidelines provide detailed guidance on best practices and procedures to achieve compliance with the IS Requirements. The IS Guidelines also provide special considerations to be considered in terms of security and privacy of cloud infrastructure.

SIGNIFICANCE OF THE IS 17428

1. One of the prescribed ways to comply with the RSPP requirement under the Data Protection Rules is by implementing security practices and procedures and having documented information security policies that contain managerial, technical, operational and physical security control measures. Currently, apart from the IS/ISO/IEC 27001 standard which is prescribed under the Data Protection Rules to deem compliance with the RSPP requirement, there are no other standards stipulated. It could be evaluated whether implementation of the IS 17428 by organizations could deem them compliant with the RSPP requirement. However, given that the Data Protection Rules and the IS 17428 fall short of explicitly specifying that implementation of the IS Requirements is deemed compliance with the RSPP requirement, the onus may be on the organizations to demonstrate that implementation of the IS Requirements meets the RSPP requirement.
2. The IS 17428 does not itself specify if it is only applicable to Indian organizations or if it can also be implemented by non-Indian organizations. The compliances under the Data Protection Rules do not apply to foreign

Q&A 2024 Protocol to the Mauritius India Tax Treaty
April 22, 2024

Boost to India's Space Potential: India Liberalizes Foreign Direct Investment
April 03, 2024

organizations. However, under the IT Act, foreign organizations which are negligent in implementing reasonable security practices and procedures and consequently cause wrongful loss to an individual may be held liable to pay damages by way of compensation to such an individual, if the organization meets certain territorial nexus requirements. Hence the IS 17428 could be implemented by Indian organizations to demonstrate compliance with the RSPP requirement under the Data Protection Rules and can also be evaluated by foreign organizations to demonstrate that they have not been negligent in handling an individual's sensitive personal data.

3. Further, India is in the process of introducing a new and exhaustive data protection law which is currently under Government deliberation. The proposed law, based on the version made available in December 2019, prescribes broad security safeguards to be implemented by a data fiduciary (akin to a data controller) and data processor, such as de-identification and encryption of data, steps to protect the integrity of data and steps to prevent misuse, unauthorized access, modification, disclosure or destruction of data. However, the 'how' aspect of implementing such security safeguards is absent in the proposed law. A Data Protection Authority, contemplated to be constituted under the proposed law, is conferred with the power to issue or approve codes of practice on standards for security safeguards. Given that the IS 17428 is a comprehensive standard formulated by the Information Systems Security and Privacy Sectional committee and approved by the Electronics and Information Technology Divisional council of the BIS, it may act as a point of reference or precedent for complying with the security standards under the proposed law in India, as and when enacted.

– Purushotham Kittane, Aaron Kamath & Vaibhav Parikh
You can direct your queries or comments to the authors

[1] The IS 17438 was established on November 20, 2020 and notified in the official gazette on December 4, 2020. Please see the notification available at: https://egazette.nic.in/WriteReadData/2020/223869.pdf (last visited May 20, 2021).

[2] Rule 3 of the Data Protection Rules provide that sensitive personal data or information of an individual contains the following items of personal data: 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; and biometric information.

[3] Rule 8 of the Data Protection Rules.

[4] Sub-clause 3.3 of the IS Requirements: "*Data Controller — Any organization that determines the means and purposes of processing the personal Information.*"

[5] Sub-clause 3.5 of the IS Requirements: "*Data Processor — Any organization that processes personal information on behalf of and in accordance with the instructions of a data controller.*"

[6] Sub-clause 3.14 of the IS Requirements: "*Personal Information — Any information that (a) can be used to identify the Individual to whom such information relates to, or (b) is or might be directly or indirectly linked to an Individual.*"

[7] Sub-clause 3.22 of the IS Requirements: "*Sensitive Personal Information — A special category of personal information, whose nature is either sensitive, such as those that relate to the Individual's most intimate sphere, or that might have a significant impact on the Individual.*"

[8] Sub-clause 3.18 of the IS Requirements: "*Processing — Any operation or set of operations performed upon personal information, whether or not by automatic means.*"

[9] Sub-clause 3.2 of the IS Requirements: "*Consent — Data subject's freely given, specific and informed agreement to the processing of their personal information.*"