भारतीय मानक
Indian Standard

IS 17428 (Part 2) : 2020

डेटा गोपनीयता आश्वासन

भाग 2 इंजीनियरिंग और प्रबंधन दिशानिर्देश

Data Privacy Assurance

Part 2 Engineering and Management Guidelines

ICS 35.030

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI-110002
www.bis.gov.in www.standardsbis.in

December 2020 Price Group 10

Information Systems Security and Privacy Sectional committee, LITD 17

FOREWORD

This Indian Standard (Part 2) was adopted by the Bureau of Indian Standards, after the draft finalized by Information Systems Security and Privacy Sectional committee had been approved by the Electronics and Information Technology Divisional council.

Other parts in this series are:

Part 1 Engineering and management requirements

It is imperative for any organization processing personal information as part of its in-house business function, or its customer solution offering, to provide privacy assurance to those whose data it processes. The trigger for this is not only from data privacy regulations but also for consumer delight, market differentiation and employee satisfaction. This Indian standard is intended to serve as a privacy assurance framework for such organizations. Implementation of Part 1 of this standard will help organizations to provide privacy assurance to customers, employees, and also to achieve and sustain privacy compliance to regulatory and contractual requirements.

Implementing Part 1 of this standard and guidelines of this standard is not a substitute for regulatory compliance. Depending on applicable jurisdiction, nature of business and type of personal information processed, various data protection related laws may apply to an organization, which needs to be determined and complied to, by the organization. Besides providing certain level of assurance to consumers on data privacy, this standard will also help the organizations in developing better understanding of such privacy requirements, embedding them into design and sustaining privacy assurance.

The composition of the Committee, responsible for the formulation of this standard is given at Annex C.

CONTENTS

Page No.

FIGURES

TABLES

Indian Standard

DATA PRIVACY ASSURANCE

PART 2 ENGINEERING AND MANAGEMENT GUIDELINES

1 SCOPE

1.1 This standard (Part 2) provides only guidelines for implementation of IS 17428 (Part 1). The guidelines are optional and intended to serve as good practices for deploying various data privacy controls and also illustrates the significance of each control element which further helps in choosing the right control.

1.2 These guidelines shall not be construed as prescriptive, to comply with any particular data privacy regulation in a particular industry sector and they are not exhaustive. While establishing the DPMS (Data Privacy Management System), the organization should choose the adequate methods, processes and tools depending on factors such as the environment, culture, technology, geography (both where organization is located and location of individuals), industry domain, and data volume in terms of number of data subjects involved.

2. REFERENCES

The standard given below contains provisions, which through reference in this text constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed as follows:

IS No.	*Title*
17428 Part 1 : 2020	Data privacy assurance: Part 1 Engineering and management requirements
IS/ISO/IEC 27001	Information technologies — Security techniques — Information security management systems — Requirements

3 DEFINITIONS

For the purpose of this standard, the definitions given in IS 17428 (Part 1) shall apply.

4 PRIVACY ENGINEERING

Any product, solution or service offered that requires processing of personal information need to take into account data privacy considerations during the entire life cycle of solution development, and should cover various stages of personal data life cycle including data collection, processing operations, decommissioning, archival stages, etc. Right from requirements development, designing through testing, data privacy becomes inherent part of development life cycle. Depending on the development methodology used, the exact stages may be further broken down, as applicable. An illustration showing flow of personal information among stakeholders and triggers for data privacy is given in Fig. 1.

4.1 Development of Privacy Requirements

Prior to designing for privacy, the requirements on data privacy should be determined by the organization. In doing so, it is recommended that the organization should:

a) Ascertain applicable jurisdiction, both territorial and sectoral,

b) Evaluate the applicability of regulations, which could be omnibus or sectoral laws,

c) Identify contractual requirements pertaining to data privacy, as applicable,

d) Obtain inputs from Market and Consumer Expectations on data privacy,

e) Factor for Design-induced requirements,

f) Consider data classification criteria for the personal data that the organization is likely to process,

g) Derive privacy and security controls from organization’s own business needs, privacy and security policies and processes, and

h) Evaluate if there is any requirement originating from data localization regulations.

Detailed guidance on the above, follows:

4.1.1 *Regulatory*

Data Privacy regulations typically fall under one of the following broad categories – Omnibus, sectoral or territorial. Applicability of all these should be taken into account.

4.1.1.1 *Types of regulations*

There are various laws, rules and other legal provisions that deal with data privacy. In India, there is no omnibus law on data privacy at the time of drafting of this

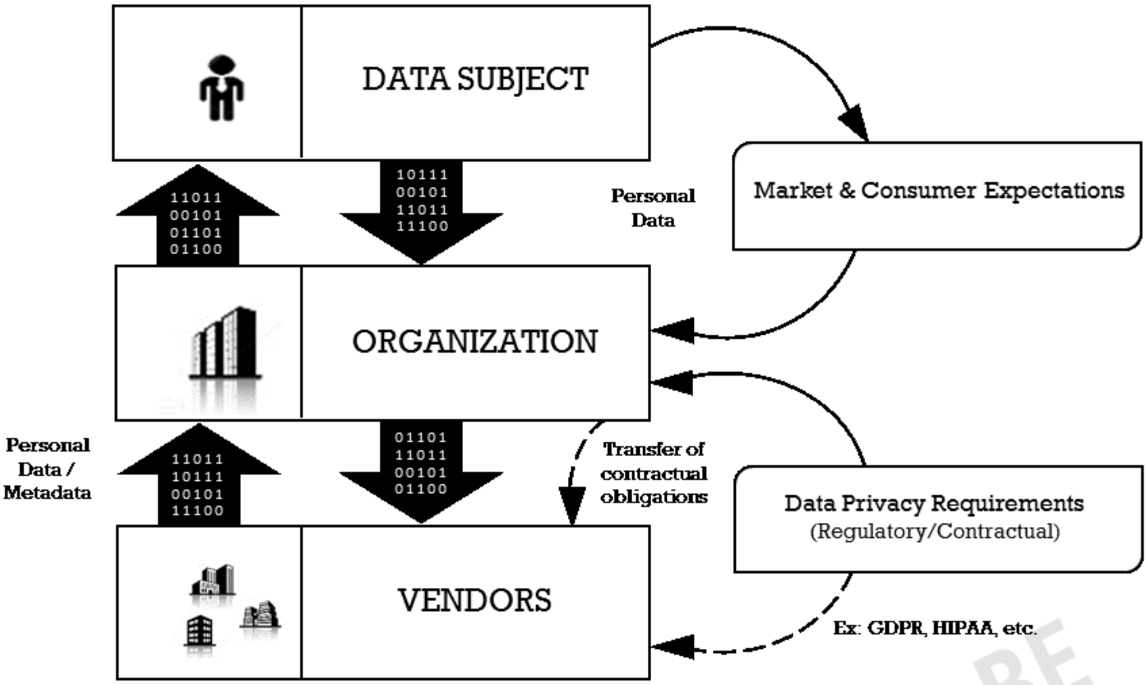

Fig 1. Flow of Personal Information Among Stakeholders and Triggers for Data Privacy

standard, but some of those that are directly or indirectly related to data privacy and protection are listed for illustration purpose, in Annex A. Also, privacy related regulatory requirements are provided with the license guidelines and other regulatory frameworks published by the sector specific regulator in India. List of some of the sectoral laws in India that deal with data privacy in that particular sector is also given in Annex A.

4.1.1.2 *Determination of jurisdiction*

With increase in online activities, and most of the personal information based solutions being online; the issue of determination of jurisdiction, in case of a privacy incident or while lodging a complaint is increasingly becoming an important point for consideration. Even when data collection is not online, this becomes important when the data subjects, the organization and the location of processing all fall under different geographical territories. This is particularly due to increasing number of disputes around data privacy with the parent organization being in one country and operations being held in local jurisdiction of another country. Hence, organizations that collect and process personal information should carefully determine their jurisdiction before determining the privacy requirements. In the event of a dispute, it is the applicable courts that have the authority to decide to take up a case and determine whether it has:

a) 'personal jurisdiction' over the parties,

b) 'territorial jurisdiction', and

c) 'subject matter' based jurisdiction.

Due to its nature, Internet and cyberspace have disrupted traditional notions of applicability of law and jurisdiction, as Internet based transactions often involve data transfer across national boundaries. Due to this, individuals and organizations can now become subject to the law of a foreign country even without a physical presence in that country.

Determination of jurisdiction will depend primarily on following factors:

1) Nature of the personal information,

2) Sector (for example telecommunication, banking, etc),

3) The country where data processing takes place, and;

4) The country to which the data subject belongs to.

In various jurisdictions, the enforcement of the law will often depend on the presence of legal entity in the country from where data subjects originate. The General Data Protection Regulation (GDPR) enacted in Europe however, is an example where the law applies to organization processing personal information of EU (European Union) residents regardless of where the organization is located.

4.1.2 *Contractual*

Extent of applicability of laws on an organization processing personal information will depend on whether the organization is a data controller or a data processor. Data Privacy laws and regulations primarily apply to data controllers, although increasingly the scope of some of the privacy regulations extend to data processors also, for example HIPAA, GDPR. However, as a data processor, organizations are bound to adhere to obligations agreed as part of contract/master services agreement. As a data processor, companies are required to follow client's instructions and process personal information on their behalf.

All the regulations and requirements applicable to an organization as a data processor should be clearly listed down in the contract. Before entering into an agreement with the client, an organization should do a thorough review of the contractual clauses and should ensure they understand all such requirements clearly. Once agreed, the organization should deploy adequate measures to comply with those requirements. Non-compliance to any such contractual requirements agreed as part of contract may lead to penalties as prescribed in the contract in form of a clause or as per the contract laws applicable in the jurisdiction.

During contract review, if the data processor comes across any client requirement which according to them conflicts with any of the requirements of the applicable laws and regulations in jurisdiction of data processor, it should be immediately flagged and brought to client's notice. Few examples of contractual requirements include personal data breach notification, records of processing, disclosure of appropriate security and organizational measures, etc.

In India, as of now, the issue of data protection is generally governed by the contractual relationship between the parties, and the parties are free to enter into contracts to determine their relationship defining the terms, cross-border data transfer restrictions, and mode of handling of the same.

4.1.3 *Market and Consumer Expectations*

Data privacy is becoming a pressing concern due to consumer's increased reliance and involvement in digital world. For any organization processing personal information of consumers, it is imperative that they determine privacy expectations before designing the solution or product. Such expectations may be obtained from various sources few of which are listed below:

a) Consumer feedback from their use of the existing solution,

b) Consumer Survey reports obtained from external parties,

c) Analysis of customer complaints and grievances,

d) Privacy choices exercised by existing consumers, and

e) Benchmarking study with similar products in the market.

4.1.4 *Data Classification Criteria*

a) It is important to establish a framework in the organization for classifying personal information based on its level of sensitivity, value and criticality, which will aid in determining baseline data privacy and security controls for the protection of data.

b) Classifying data is the process of categorizing data assets based on their sensitivity, which is determined by the likely impact and harm caused to an individual in the event of a data breach or misuse. Since the interpretation of sensitivity may be subjective and may vary depending on culture, business priorities etc. Therefore, it is the applicable regulation which determines the sensitivity of particular data. Personal information is broadly classified as sensitive or non-sensitive. Usually data such as date of birth, telephone number etc. are treated as non-sensitive whereas health, financial information, sexual orientation, biometrics, religious beliefs etc. are often considered sensitive. The exact classification should be based on applicable jurisdiction and the nature of processing involved.

c) Classification will apply both for data and metadata

d) If an organization already has information classification guidelines defined for various types of data, which includes both personal and non-personal information, the organization may choose to include the personal information under the overall classification. for example if an organization has three levels of classification 'Restricted', 'Confidential', 'Public', it may choose to put 'personal information' as part of 'Confidential' and 'sensitive personal information' as part of 'Restricted' category. Furthermore, when dealing with non- personal information, the risk of combining non-personal information to infer or derive an identity or profile of a unique user or at least small enough subset of users should be understood and evaluated.

The primary purpose of classifying data is to decide on downstream data privacy controls that an organization needs to deploy. In general, stricter controls are required for protecting sensitive data due to the potential harm they could cause to the individual.

4.1.5 *Design-Induced Requirements*

The design itself may introduce additional privacy risks and in this case organizations may need to revisit design considerations for data privacy. Organizations may decide to implement certain processes in order to meet data privacy requirements which are then likely to bring in newer privacy challenges. In such cases, organizations need to do a detailed assessment on what challenges can arise and how it needs to alter upstream design to prevent the risks. For example, an organization may decide to monitor emails, both official and personal, of its staff, in order to prevent/detect unauthorized leakage of its consumer data. In this process, employee's personal emails may also be monitored which may intrude into their privacy and cause distress especially if an email consists of sensitive personal information and found to be a false positive.

4.1.6 *Data localization*

Data localization laws are typically intended to prevent or restrict transfer of personal data to countries that do not offer similar protection and to help law enforcement agencies have access to data when there is compelling need. Such regulations, for certain types of data, may require companies to process and store data locally first and only then, if required, transfer the data to other secondary locations, while certain other types of data may not be permitted to be stored outside at all. Before transferring any data across borders, companies are expected to assess the impact and required to adhere to local data privacy regulations.

4.2 Privacy Principles Based Design Considerations

4.2.1 *Personal Data Collection Limitation*

Personal data may be required by organizations for various purposes, such as to fulfill a contractual requirement with the data subject, to comply with specific regulation, to provide an optional feature for those data subjects who choose such option, for business and commercial purposes. It may be collected by an organization either directly or indirectly. Direct collection happens when active involvement from individual is required for an organization to collect data from an individual for example when data is entered into a screen or a form by the individual. Indirect collection on the other hand are scenarios where no action is required from an individual when data is collected by an organization, for example, IP address during web browsing, placement of cookie in individual's end point device, CCTV surveillance, etc. Additionally, such indirect data collection can happen when the data is purchased from or collected through an external party.

Organizations should process data only when it is necessary and not excessive. Before collecting the data, organization should define the purpose of collecting the information. The organization then, should collect the minimum information which is required for the defined purpose. It may be tempting for organizations to collect more data even without adequate justification, with the presumption that it may need such data at a later stage. Such a practice may not only violate data privacy laws, but it will also put unnecessary burden on the organization in terms of the need to deploy additional measures to protect such data and justification why such data was collected. Any information collected more than minimum, and which is in interest of an individual, could be collected based on choice and not forced.

4.2.1.1 *Proportionality*

Every personal information collected should be proportional to the intended use and not more than minimum. It should have a valid purpose and only that information which is required to fulfill a business need should be collected and processed by organizations. For example, employer may need birth dates of employees to wish them on their birthdays, in this case collection of birth date should be in dd-mm format as year of birth will be considered excessive and not relevant to the purpose stated above. Similarly, B2C (business to consumer) organizations may collect address for billing or delivery purposes however collecting date of birth and making it mandatory for registration purposes maybe considered excessive. The organizations before collecting personal information should determine,

a) Need to collect the data;

b) Data collected is adequate and relevant; and

c) Data collected is not excessive and has a valid purpose.

Tools and processes should be designed in such a way that data collected and stored on systems is minimal and not excessive. This would also put less burden on organizations towards maintaining such personal information.

4.2.1.2 *Lawful basis*

Personal information collected and processed by organizations should be legitimate. The lawful basis for collection of personal information may vary from country to country depending on applicable regulations. Collection and processing of Biometrics for authentication purpose, for instance is considered legitimate in certain jurisdictions, whereas it is not permitted in some other jurisdiction, unless the security requirements are extremely critical and justify such processing.

Organizations should be aware of such regulations and should perform a proper assessment to ensure that data collected is legitimate. Illegitimate data collection and processing by an organization may result in fines, lawsuits, customer grievances etc., and therefore it is imperative for organizations to determine if there are any regulations applicable that prohibit collection of certain types of data that may be required by the organization. Certain checks and controls may need to be put in place so that the system flags illegitimate collection of personal information.

When sensitive personal information is collected solely for complying with a regulatory requirement, the endeavor should be to collect it anonymously. For example, when information about caste or race is collected from a new employee in an organization, to comply to diversity obligations, especially in private sector, separate forms may be made available to collect the information either in an anonymous manner or in a manner that they cannot be linked with other personal information of the employee. This way it helps prevent any scope for discrimination during employment. This example however may not be valid for government organizations, which collect and use caste data due to applicable mandatory reservation rules of recruitment and career progression.

For each type of data collection, the organization should determine the appropriate lawful basis for collection and processing of personal data and document the same. Such lawful basis will typically be one of the following:

a) To fulfill a service or contract with the individual;

b) For legitimate business interest of organization, balanced with potential privacy harms for the individual;

c) To fulfill a legal obligation;

d) To protect vital interests of the individual; and

e) For public interest.

4.2.1.3 *Collection at the right stage*

Organizations should design their processes and systems in such a way that personal information is collected at the right stage at the right time when the need for collection of data arises. Organizations should collect and process personal information only when a valid business need for data collection exists at that point of time.

While providing personal information in a web based screen, design should ensure that individuals should not face a situation whereby some of their data is captured by the organization and retained before the individual reads and agrees to privacy policy or before the individual chooses to discontinue the transaction any further. For example, situation should not arise whereby an individual may find that he is not comfortable providing one or more of the data elements being sought mandatorily in the second screen during registration process, based on which he decides to abandon registration, but the system does not allow to revoke data submitted in the first screen. This type of elusive practice of layering data collection with progressively decreasing privacy is not only privacy unfriendly but also may be treated as a privacy violation.

Similarly, data required at the time of joining an organization should not be collected from candidates at the time of recruitment, providing the reason that organization may anyway collect it at the time of joining. This may be considered as unlawful and will violate privacy regulations.

4.2.2 *Privacy Notice*

Organizations should give prior notices to individuals before processing any personal information. Use of 'privacy notice' or 'privacy notice with consent' will often depend on lawful basis determined for each type of data processing. In the absence of any regulation, table 1 may be referred to, while determining the right privacy control.

Table 1 Determining Right Privacy Control

Is data necessary to provide service/ product or to enter into a contract?	PII or SPI	Basis for data collection to be used	Data minimization required?	Privacy notice or consent	Example
Mandatory	Does not matter	Use one of the following: a) Contractual Requirement b) Legally required c) To protect vital interest of data subjects d) Legitimate business interest e) Public interest	Yes	Fair Collection Notice	Address, telephone number, bank a/c number in an e-commerce platform. Blood group, age, ailment in a hospital Photo and education certificates, during employment
Optional	Does not matter	Consent	No, unless required by applicable legislation	Explicit Consent and Choice for each non-mandatory data element	Marriage anniversary date, annual salary in e-commerce site Geo location for an app that tests students' IQ Telephone number when purchasing vegetables and grocery in retail store.

NOTE — Even in cases when data minimization is not required, all privacy principles like proportionality, fairness, lawfulness, and other data protection measures should be applied. Also certain jurisdictions may require consent for sensitive personal data, even if such data collection is mandatory, and care should be exercised in such cases to ensure fairness.

4.2.2.1 *Contents*

Organizations should design the privacy notices in such a way that it clearly provides purpose of data attributes that it intends to collect. Organizations should be open and transparent about their personal information collection practices and processes. Whenever there is a personal information processing, individuals should be clearly informed with a privacy notice about the data controller's policies, procedures and practices with respect to the processing of the personal information before commencing such processing. The organization should determine the contents of notice depending on the applicable jurisdiction and business reasons. Typical details provided in the notice are as follows:

a) The fact that specific personal information will be collected.

b) Purpose of data collection.

c) Name and address of entity collecting the personal data (Data Controller).

d) Name and address of entity retaining the data, if different from above.

e) The identity of the data controller including information on how to contact the data controller.

f) Intended data recipients.

g) Data Retention including the reasons to retain data beyond use and policies on data deletion.

h) Security measures organization will adopt.

j) Whether the data will be shared with external parties.

k) The name and contact number of the relevant data privacy officer.

m) Method to withdraw consent.

The contents of notice may vary depending on applicable jurisdiction. However, the basic elements as mentioned above should be captured in order to be transparent to the individuals.

The privacy notice should neither be too detailed nor too abstract. It should cover the necessary details and should be simple to read and understand for example, if an organization is collecting data from a consumer for delivering services, then it is not sufficient to mention 'registration and service delivery purpose'. It should mention purposes for various categories of information such as address for delivering a product, demographic details to send targeted advertising, etc. Although organizations may be tempted to use privacy notices which are too abstract, but this makes it less transparent and in the process may violate the regulations. On the other hand, if it is too detailed, every time an organization makes minor internal changes on data processing which does not impact the broad purpose of collection, they may be unnecessarily required to go back to individuals for obtaining fresh consent which makes it cumbersome for organizations and as well as for the individuals.

4.2.2.2 *Mode of communication*

Organizations may adopt various means to deploy privacy notices. An assessment should be done to determine which mode would be the most suitable and effective for the organization and business:

a) Electronic privacy notices

This mode is usually effective when personal information is being collected through a web application or through a mobile app, some common examples being ecommerce mobile apps collecting data from consumers. When the user logs into an application, a notice should be displayed before the data is captured/saved in organization's systems.

b) Hard copy privacy notices

Hard copy notices/consents may be deployed where data elements are collected through hard copy forms, for example, feedback forms in hotels usually ask date of birth, anniversary date, email ID, phone number. Notices should be provided along with these forms.

c) Posters

Notices can be displayed where it is not feasible to give a separate notice to each individual. One such example is CCTV surveillance at entry/exit points. Notices with proper messages should be displayed in such areas and should be clearly visible to the individuals.

d) Website privacy policy

Organizations may publish a privacy policy on their website broadly for two reasons:

1) for website visitors, for information collected during website browsing. Users should also be informed about indirect data collection such as cookie information, IP address.

2) to make all data subjects aware about organization's privacy policies and practices for all data collected & processed by the organization, and not confined to data collected on the website.

4.2.2.3 *Timing of providing notice*

Organizations should ensure that notices are provided to individuals at the right time during the personal data collection stage, ideally, just before the collection, regardless of whether such data is collected directly or indirectly. Providing a notice too early may lead to an individual not remembering the contents of a notice and therefore inability to take informed decision. On the other hand, providing a notice subsequent to data collection defeats the very purpose of a privacy notice and hence will lead to violation of data privacy principles.

Organization may have provided notice to employees few years prior to collection of data, but privacy practices and processes may change over a period of time and therefore in such cases privacy notices also require changes.

4.2.2.4 *Accessibility and comprehensibility*

The accessibility options for people with special needs (such as braille, special fonts, auditory versions, etc.) may be considered, as appropriate. Systems should be designed in such a way so that these privacy notices designed for people with special needs can be seamlessly embedded.

The organization may make privacy notices available in vernacular language depending on the product or solution offering caters to, the population segment. Individuals should be able to read and understand these privacy policies/notices without difficulty. For example individuals can be given an option to choose the preferred language and upon selection, privacy notice can be displayed in the language user has selected.

4.2.2.5 *Ease of readability*

Privacy Policies/Notices should be device friendly, for instance, the look and design of notice may be different for a mobile phone and a desktop computer. They should be easily readable by individuals using any type of device. Language used in the privacy notice should be simple and easy to understand. Appropriate font type and display size should be selected to make it readable and complex fonts and representation which are difficult to read should be avoided.

4.2.2.6 *Acknowledgement of privacy notices*

The organization should, as much as practicable, provide notice in a manner that requires an individual to affirmatively acknowledge that he has read and understood the contents of the notice. This helps in demonstrating evidence and prevents situations when an individual denies having read a privacy notice, for example, a notice simply sent by an email which one would not have read due to various reasons including its movement to junk folder. Organization should ensure that right versions of notices are maintained.

There may be situations where it is not feasible to record an acknowledgment receipt of privacy notices for example, hard copy notices displayed for CCTV recording, whereas for employees and staff, organizations may consider including it in their annual code of conduct or employee joining contract or its website.

4.2.3 *Choice and Consent*

When consent is the lawful basis for data collection and processing, the organizations should ensure the following:

a) That the consent given is a valid consent, being given freely and not under any compulsion /undue influence.

b) That the consent is taken only after displaying the privacy notice to individual as in **4.2.2.**

c) That the consent is an informed consent.

d) In case of a minor, the consent is given by the legal guardian.

Organizations should give enough choices to individuals through various mechanisms. Personal information of individuals should not be processed, if they opt out for such processing.

Privacy-by-default should be the norm and opt-in consent should be the preferred approach.

4.2.3.1 *Opt-in and opt-out considerations*

It is imperative for organizations to understand opt in and opt out options especially when dealing with activities related to marketing purposes.

If organizations need to use opt in mechanism for marketing activities, they need to take customer’s permission before sending newsletters, updates on emails etc. Organizations may decide on best methods to deploy such practices, for example enabling checkboxes on websites for permissions, email confirmation or an explicit action from individual like clicking on a link to provide opt in. Only those who opt in, should receive messages and calls from the organization for example, many countries in Europe require organizations to use opt in mechanism, as per e-privacy directive for electronic marketing.

Opt out is a method by which recipients may choose to unsubscribe unsolicited calls/mails and messages. Organizations should provide opt out facility before making direct marketing calls to prospects/clients. Organizations should be cautious and respect privacy preferences before adding any prospect to their marketing database. Once opted out, organizations should ensure they adhere and respect such decisions of individual and stop making calls/sending messages to these individuals immediately. An opt-out option, preferably in the first transaction itself, may be provided through one or more of the following ways:

a) Calling a phone number provided and opting out.

b) Email address to which individuals can send, in order to opt out.

c) Link – Clicking a link to opt out.

d) Customer Acquisition Forms – pre-checked box.

Organizations should use opt-out method only when risk of privacy intrusion is least and when permitted by law. In general, the decision on the right method to choose would be based on following parameters:

a) Applicable regulations in the jurisdiction.

b) Harm or distress caused to the individual and to the extent it is irreversible.

4.2.3.2 *Fairness of discretion*

When consent is the lawful basis for collection of data, such choice needs to be fair and transparent. Following scenarios illustrate the concept of fairness:

a) An e-commerce portal should not force a consumer to provide information that is not essential, for completing a transaction, and to offer a service. Such collection does not give a fair choice to consumer because by then, consumer would have already provided some personal information and entered into a transaction, and cannot reverse the collection.

b) If an app asks consent for sharing data with a third party on which it relies for fulfilling the service to the individual, such consent will not be appropriate. The app owner which will be the data controller, should take accountability for data transfer and need to ensure that the third party, most likely a data processor, is made liable contractually for data protection measures.

c) Where consent is the lawful basis for collection and processing of personal data, then organizations should present consent in such a way that it is vivid and not combined with other 'declarations' or 'Terms and Conditions'. To ensure fairness, consent for mandatory and optional personal data collection should not be combined into one.

d) Timing of obtaining consent - *see* **4.2.2.3**

4.2.3.3 *Revocation of consent*

An individual's preferences on data collection and processing may change over a period of time due to their personal choice, nature of processing by the organization etc. so individuals may have in general a reasonable expectation to have their preferences changed subsequently. Hence the organization should provide an option to individuals to revoke consents provided by them earlier for data collection and processing. In due course of time, whenever individual feels that he/she needs to revoke his/her consent due to any reason, he should be able to do that. Organizations should be transparent on consequences of revoking consent by an individual. Many countries, including India have a legal requirement to provide this.

An individual may be deprived of corresponding benefits and services if he/she wishes to withdraw consent on data processing. There might be times when it may be difficult to permit to revoke consent for example, certain laws may require few personal information elements to be retained for certain period of time, in this case, individuals may not be permitted to revoke consent before the retention period required by law.

4.2.3.4 *Preservation of evidence for consents*

The organization should maintain records of consents obtained from the individuals from time to time. Appropriate record and document management controls should be implemented in line with the individual's right to access, correct or erase the personal information pertaining to them.

Preservation of evidence of consent is to ensure and demonstrate the following:

a) Individual's active participation in the decision-making process regarding the processing of their personal information.

b) the stored consent information is related to the right version of privacy policy and is for the same intended purpose.

c) legal basis for processing the relevant personal information.

4.2.4 *Use Limitation*

4.2.4.1 *Restrict to original purpose*

The organization should use personal information only for the purpose for which it was originally collected.

As mentioned in **4.2.2.1**, if an organization specifies purposes superficially to keep the flexibility to use data as it wishes at a later stage, such processing may lead to a privacy violation. In the event that the data is required to be used for a different purpose, it should obtain fresh consent or provide notice to individuals as applicable before processing. If the organization intends to use such data for statistical analysis purpose, it should use aggregated data after de-identifying the same.

The restriction on use applies not only for the organization but also to any other entity to whom processing has been outsourced.

4.2.4.2 *De-identification*

In scenarios where organizations may need to use data for a secondary purpose or to transfer data to an external party, (for example to carry out a questionnaire based survey or to an external party to use it for larger good of the society) and the purpose can be achieved without identifying the individual, they should do so only after de-identifying data.

The objective is to prevent an individual to be identifiable from the data set. Organizations should make use of de-identification techniques wherever possible, to minimize potential privacy harms.

4.2.4.2.1 *Anonymization*

Anonymization is a de-identification technique. In this technique, identity of an individual remains completely anonymous and individual can never be identified, even by referring to other sources of information. Such technique may be used when data is shared with a third party or put in public domain after deriving meaningful insights for the larger good of society for example, illness patterns in a geographic region, traffic data, diversity related statistics etc.

4.2.4.2.2 *Pseudonymization*

Pseudonymity is another de-identification technique that involves replacing the identifiable part of the data with 'pseudonym', which is a dummy attribute used instead of a real one so that it is not possible to decipher the identity of an individual from the modified data without accessing additional information that links pseudonym to real identifier. Pseudonymization does not rule out the possibility that there might be (a restricted set of) organizations which are able to determine the individual's identity based on the alias and data linked to it. Pseudonymization is a reversible process i.e. data may be re-identified if the key is made available. It should be used when possible to minimize privacy harms, for example, when an organization engages with external parties to conduct surveys, pseudonymization is recommended, so that the external party could not establish identity, while organization/owner of the data should be able to re-identify the data set by tracing back to the original data. If organizations specifically mention that surveys conducted by them will be anonymous, they should adhere to the same.

4.2.5 *Data Accuracy*

The organization should ensure that personal information remains accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate, relevant and reliable for the purpose of use.

Inaccurate information can lead to inappropriate decisions and processing which may harm the individual. Appropriate tools, such as digital signatures, may be used to ensure data integrity. In order to prevent inadvertent modification of data while stored in servers and databases, by admin teams, dual authentication may be introduced and logs for any modification, deletion etc. from backend, should be maintained for audit trail purpose.

Accuracy is also about keeping data up to date, to prevent it getting obsolete, for which the individual should be provided access to make changes, where appropriate and required.

4.2.6 *Security*

Personal information should be secured by use of appropriate controls to ensure their confidentiality, integrity, availability and to prevent unauthorized access or disclosure. Organizations should deploy appropriate security measures commensurate to the likely harm caused to individuals' rights and freedom from a potential breach.

The organization should implement an information security program, commensurate to the need and size of the organization and relevant to the privacy risk involved. The organization should implement the Standard IS/ISO/IEC 27001 or the codes of best practices for data protection as per Rule 8 of *Information Technology (Reasonable security practices and procedures and sensitive personal information or information) Rules*, 2011 to demonstrate its commitment towards security of personal information. Additionally, other appropriate established best practices, guidelines such as NIST Cybersecurity Framework and DSCI Security Framework, etc. may also be implemented. It may also be stipulated as per the agreement between the parties or as per the laws such as medical code of ethics, legal code of ethics, Indian evidence act, etc.

The scope of such program should cover all types of personal information collected or processed by the organization. The legal and regulatory requirements should be identified and covered in the scope of security program. Compliance to all security requirements should be documented.

Security control measures will typically fall under two categories – security of data at source and securing the environment. Other categories may be relevant to the nature of business based on the applicable legislation and the risk appetite of the organization.

4.2.6.1 *Security of data at source*

Regardless of how well the environment is secured, security measures need to be also deployed on data at source. This will at the outset, require data to be classified as stated in **5.3.1**, into appropriate category, based on which suitable control measures should be planned and deployed. The controls will depend on whether data is at rest or in motion both of which need to be taken care of.

4.2.6.1.1 *Data at rest*

Data which is stored should be protected by appropriate techniques from unauthorized access, modification or destruction. The methods used such as encryption, password protection, and digital rights management, multi-factor authentication etc. should be determined based on potential threat scenarios for various categories of data.

4.2.6.1.2 *Data in motion*

Data that is in transit is subjected to different set of risks when compared to those at rest, and hence needs separate control measures. The organizations should ensure the following:

a) Documented encryption policy for protection of personal information during transmission and rest.

b) All documents and records containing sensitive personal information and where, applicable personal information, should be encrypted before transmitting them by mail or other means.

c) All personal information to external networks should be transmitted through secure channels. Any remote access to computer systems containing personal information should be restricted, or should be controlled, logged and monitored.

4.2.6.2 *Security of environment*

Securing the environment in which personal information is stored or processed will typically require logical security, physical security, network security, end-point security, cloud security, background check of people involved in processing personal information, etc.

Security considerations for cloud are provided in Annex B.

4.2.6.3 *Retention of access logs*

The organization should ensure that only authorized users access the personal information and prevent unauthorized access to the personal information. Organization should define the access logs that need to be retained in order to demonstrate compliance to data privacy regulations. Such retention plans should include the following:

a) Different types of access logs (such as read, write, update, delete), exceptions, faults and security.

b) Types of storage repositories such as database, servers, cloud etc.

c) Types of data based on sensitivity.

Organization should retain and maintain the logs of user access for a defined period, depending on regulations.

As retention of logs require significant hardware space, an organization needs to weigh the retention requirements versus the operational constraints while defining policy. Apart from retaining the logs, organization should regularly review the logs.

4.2.7 *Disclosure and Transfer*

During the life cycle of personal information, transfer or disclosure to external parties is often inevitable. Transfer often involves outsourcing part of processing to a data processor which will only process data as instructed by the data controller. Disclosure on the other hand involves providing data to an external body such as regulators, government bodies, law firms in the event of a subpoena, audits etc. not part of life cycle process.

4.2.7.1 *Disclosure to external agencies (including mandated requirements of data disclosure)*

Whenever personal information is disclosed to an external agency, it should be only on individual's consent, unless required/permitted by applicable law. In certain rare situations, where informing individual about disclosure may impede the very purpose of disclosure, consent or notice may be waived but only when legally permitted. Regardless of whether individual is aware or not, the organization should ensure that the data privacy obligations are communicated to the external party and such party is obliged to comply with all such provisions.

4.2.7.2 *Transfer for processing by data processors and cloud providers*

When personal information is transferred to a data processor for part of processing during data life cycle, the individual should be informed and consent should be obtained where appropriate. Data Privacy contractual clauses should form part of the contract with the data processor and the data processor should be contractually obliged to comply with all such stated and applicable contractual and regulatory requirements. The purpose for which data is transferred to the data processor should be clearly specified and the data processor should not use the data for any other purpose other than that stated in the contract.

In certain situations, a data processor may be authorized by the data controller to collect personal information from an individual, in which case the organization should specify what data may be collected, how it should be collected and ensure that privacy safeguards are communicated to the data processor including deployment of privacy notice as applicable.

When personal information is transferred to an external party cloud, additional safeguards should be considered depending on whether the cloud is private, public or hybrid. A detailed privacy impact assessment should be conducted by the organization before transferring data to a cloud. Some of the privacy considerations are given in Annex B.

4.2.8 *Personal data storage limitation*

Personal information should not be retained indefinitely and should be kept only as long as it is required by the law or when there is a business requirement. Requirements for retention of personal data should be determined at the time of acquisition of data.

Requirements of data deletion may also originate from 'right to be forgotten'. Individuals may at times request for deletion of their data due to various reasons. In these cases, unless there are overriding legitimate grounds for the processing or other applicable regulations do not permit deletion, the organization should have provision to remove individual's personal data promptly. Such requests are more common in the internet domain such as social media, where not deleting information may cause distress to the individual due to rapid dissemination of unwanted information.

The retention period varies based on type of data and purpose for which they were collected and hence it requires an organization to study and evolve a data retention strategy based on which a data retention policy should be defined, best suited for its business. The exact period for which data needs to be kept should be documented in data retention policy and should be based on applicable sectoral regulatory and contractual requirements.

Suitable and secure methods should be used for deletion of personal information. Such methods should be considered while decommissioning assets, media, and mobile devices.

If the organizations require data to be retained for statistical purposes beyond retention period, appropriate de-identification techniques should be adopted as an alternative but in such cases it should be ensured that data cannot be re-identified.

4.2.9 *Other Design Considerations to fulfill data subject's rights*

In order to fulfil rights of individuals, additional privacy features may need to be considered during design and taken for implementation. These could come from regulations or may be part of consumer expectations. In either case, there would be significant impact on both technology and process, dependency on external parties and hence it is prudent to factor such aspects in the upstream stage.

Examples of such considerations are:

a) Data portability

This requires provision to port personal data of an individual to a different data controller at the discretion of the individual. The benefit for individual would be:

1) to facilitate transfer of already provided data and privacy preferences to the new data controller

2) to get data deleted from previous data controller

Such feature should not put burden on individual and should not be requiring effort and skill from individual. Since technologies adopted by various organizations (competing data controllers) may be different and not compatible, use of different or same tools may be required to ease the porting of data.

b) Object to profiling and automated decision making

Profiling involves creation of a database and maintaining data against each individual to evaluate certain personal aspects, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements, and is often considered sensitive. Examples where this may be used (not necessarily legitimate) are:

a) Credit rating.

b) Premium determination by Insurance companies.

c) User and entity behaviour analytics.

When organizations use profiling, provision should be provided to individuals to let them know about existence of such profiling, the logic involved and when individual could object to such profiling and consequences.

Likewise, in today's world, more and more processes are being automated with least human intervention. When organizations focus on technology driven decision making, it can result in unfavorable consequences to individuals in the event of incorrect decision. Organizations should ensure that as a consequence of any decision about an individual, that can cause distress or harm to an individual is not solely taken based on automated processing, but should be supplemented with manual intervention. Extent of potential harm to individuals from data privacy perspective needs to be evaluated based on nature of transaction involved, for example, financial impact, health related condition, reputation loss due to public disclosure of private matters, suspension of employment, identity theft, discrimination, etc.

For example, some banks use verification services from external parties before issuing cards to customers, whereby they may scan prospective customers' digital footprints on the web and social media activity using algorithms. In such cases if the bank solely uses the recommendations from external parties in deciding issuance of credit card or downgrading credit card, it will be considered as an automated decision making and in such cases, individuals may have right to know and question the rationale for the decision, and seek human intervention. Outcomes from automated decision making often cause significant level of distress among customers and hence to mitigate the risk involved, banks should establish facts with the affected individuals before taking such actions.

4.3 Verification and Testing

The data privacy requirements incorporated in design should be verified and tested prior to deployment of solution or product. This will reduce the risk of penalties and data breach notification requirements for the organization.

4.3.1 *Privacy Test Scenarios*

For each design aspect, privacy test scenarios and test cases should be created, taking into account boundary conditions. While designing, all aspects of potential violations and breaches in each stage of processing should be taken into consideration.

4.3.2 *Independent Testing*

Prior to deployment, the solution should be tested by an independent team. Whenever the solution is reworked to fix identified bugs, it should be retested prior to deployment. Care should be taken to identify and fix new privacy bugs that may get introduced during bug fixing.

In situations when a solution enhancement needs to be released due to emergency fixes, where risk of data privacy is relatively low, the solution may be permitted to be deployed but only with a call-back procedure (in the event when subsequent testing yields a failure).

4.3.3 *Periodic Compliance Check*

In addition to testing as part of life cycle of solution development, periodic compliance checks should be done to ensure that the solutions continue to comply with applicable privacy requirements. This is necessary due to changing regulations, technology, platforms, business model on outsourcing etc. Such compliance checks may involve performing remote privacy vulnerability scans or actual on-line testing of an application. The method adopted should depend on the criticality of application.

5 PRIVACY MANAGEMENT

5.1 Privacy Objectives

Privacy objectives, along with privacy policy constitutes one of the key inputs while an organization embarks on data privacy program. It sets the directions for planning activities, and is influenced by organization's perspective on data privacy. One organization may consider data privacy as a compliance requirement, while another may want to use it as opportunity to create differentiation in the market, while for a third organization personal data may be the key raw material that drives the business. Each type of organization will therefore set different privacy objectives. While compliance to regulations is given as a necessity, there is always flexibility for organizations to choose the degree of privacy controls they may introduce while being compliant.

The objectives could differ for the same organization in case of its role as a data controller and as a data processor, since in the latter, the objectives are a lot driven by contractual terms from data controller. The privacy objectives in such cases should be documented separately for controller and processor roles clearly defining the data subjects and type of personal information it collects and processes for each of the roles.

5.2 Data Privacy Function

5.2.1 *Organization Structure*

The organization should clearly identify and define the Data Privacy organization structure within its overall organization structure. The scope of the function/role should be clearly defined, allocated and communicated to the relevant stakeholders. A member of the top management should have the overall responsibility of the privacy program and need to be clearly defined and documented. While defining responsibilities care should be taken to ensure that there is adequate independence for the data privacy function from the Operations, Sales, Marketing and IT organization, and where applicable, Security function to avoid any scope for conflict of interest.

5.2.2 *Responsibility and Accountability*

The top management should appoint management representative(s) who irrespective of the other responsibilities, should have defined roles, responsibilities and authority for:

a) Ensuring that the privacy program is established, implemented and maintained in accordance with the organization's privacy policy;

b) Reporting on the performance of the privacy program to the top management;

c) Promoting awareness of the privacy program across the organization;

d) Ensuring effectiveness of procedures developed for incident response and privacy impact assessment

Individuals with allocated privacy responsibilities may delegate tasks to others, however they remain accountable and should determine that any delegated tasks have been correctly performed.

5.2.3 *Cross-Functional Participation*

Data Privacy in an organization needs participation of several internal functions that process personal data which require such functions to work very closely with the data privacy office. Hence, a cross functional data privacy committee should be constituted, particularly in large organizations, in which representatives from each function or location of the organization should be identified to assist in the implementation of the privacy program. Such committee should convene periodically and discuss data privacy issues and performance. The roles, responsibilities and authorities of the committee members should be defined and integrated into job descriptions and skill sets which may be reinforced by including them in the organization's appraisal, reward and recognition policy.

Security and privacy functions have a significant overlap, and hence there should be good coordination between personnel handling security and privacy during the entire data life cycle and during the engineering of privacy.

5.2.4 *Governance and Senior Management Oversight*

The organization should ensure that policies and processes are defined to provide direction and oversight to the privacy program related activities.

The organization may appoint other bodies, such as a steering committee, to oversee the implementation of the privacy program. The governing body should put in a process to evaluate, direct, monitor, assure and communicate the process to govern privacy. The governance of privacy program should be an integral part of the overall organization governance.

Where possible, performance on privacy compliance should be reported and monitored using metrics and quantifiable data on periodic basis. The metrics should be reviewed for improvement trends and for performance against benchmark targets.

The program should be subject to audit periodically.

5.3 Data Privacy Management System (DPMS)

5.3.1 *Data Classification*

Organizations should classify all personal information in its possession according to defined and documented criteria (as per **4.1.4**). Possible data classification categories include, but are not limited to, general ones such as sensitive and non-sensitive personal information. A classification scheme could also include more specific categories such as personal health information (PHI), personal financial information (PFI) and so on. The actual categories used will depend upon the requirements defined in relevant data protection legislation and regulation, other legal (for example contractual) obligations, the nature and sensitivity of the information, and the risk of harm that might arise in the event of a breach.

Some personal information that may be classified non-sensitive in one country may be treated as sensitive elsewhere, depending on the applicable data protection laws.

The classification for an element of personal information could need re-evaluation and modification when associated with one or more additional attributes. Appropriate guidelines and procedures should be put in place.

All types of personal information need not require equal degree of protection. Data classification helps in channelizing right degree of protection depending on sensitivity of information which in turn may depend on applicable regulations and harm caused to individuals in the event of misuse or unauthorized disclosure.

Appropriate labelling may be used to identify records with various classification to facilitate deployment of right data protection controls.

5.3.2 *Inventory of Personal Information*

The organization should ensure that all the personal information the organization owns and holds as a custodian, is identified and an inventory of personal information is created, maintained and periodically updated. The inventory should contain all the relevant information about personal information which will be helpful in ensuring effective management of personal information and in ensuring compliance to data privacy regulations. The inventory of personal information should have the below mentioned details with respect to the personal information identified:

a) Business Process Name.

b) Data owner.

c) Type of data.

d) Applications/Systems.

e) Data attribute.

f) Individual.

g) Purpose of processing.

h) Lawful basis of processing.

j) Form of data.

k) Recipients.

m) Country of processing.

n) Whether outsourced.

p) Retention period.

Such inventory of personal information may be combined with inventory of other types of information that already exists in the organization for the sake of convenience, but such act of combining should not have any adverse impact in fulfilling any requirement of IS 17428 (Part 1).

5.3.3 *Process Depicting Flow of Personal Information*

Organizations should have documented processes in place, clearly depicting the personal information flow for each process and function. A separate documentation need not be maintained only to fulfil conformance to IS 17428 (Part 1), if respective functions already have process documentation in place, focusing on processing of personal information. Process Flows should be able to depict data flows within systems internally within organization, between organization and its various entities, subsidiaries and service providers, level of access to the data recipients, form of storage etc. Personal information inventory together with process flow documents should form the basis of defining and implementing privacy controls in an organization.

5.3.4 *Change in Processing or data inventory*

The process for any change in processing of a particular personal information, including but not limited to, collection of new data, new kind of data disclosure, access by an additional stakeholder, cross-border data transfer, addition of a process stage etc., should be defined and workflow should be built as part of internal organizational systems.

This is required to ensure that processing of personal information in the organization and by external parties happens only as agreed and base lined in the personal information inventory.

Appropriate approval process by data privacy function for any change, introduction of new personal information or processing purpose should happen before such personal information is processed.

Changes in personal information inventory may also be triggered by regulatory developments or change in technology.

5.3.5 *Triggers for Updating DPMS*

DPMS needs to be updated by the organization on a regular basis, and such need may arise due to various triggers including but not limited to:

a) Regulatory developments and updates;

b) Change in the processing;

c) New locations;

d) Merger and acquisition;

e) Data transfers to external parties.

5.4 Policies and Processes

5.4.1 *Privacy Policy*

The organization should define, approve, and publish a privacy policy that applies to all units and locations of the organization and should be authorized by the senior management representative or Board member overseeing the data privacy function. This policy should be communicated to all stakeholders setting out the approach to manage the privacy objectives.

The privacy policy should contain statements concerning:

a) Definition, objectives and principles to guide activities related to privacy.

b) Responsibility and Accountability for implementing the policy.

c) Processes to handle deviation and exceptions.

The privacy policy should address the requirements from:

1) Organization business strategy.

2) Regulation, legislations and contracts.

3) The current and projected privacy threat environment.

The structure of policy may defer between organizations and best designed depending on how it fits in overall quality system documentation and process repository. It is recommended to keep policy at sufficiently high level and more detailed privacy aspects may be covered in procedures and guidelines.

The objective of privacy policy is to state company's commitment towards data privacy, which will largely depend on the organization culture, diversity, and strategic business aspects, most of which do not change over long periods of time such as,

i) Whether it is a consumer-oriented or business to business company,

ii) Whether the company uses personal data for commercial benefit,

ii) Geographic distribution of the processing and market it caters to,

iv) Nature of data processing involved, etc.

Hence to avoid regular updates to privacy policy, it is recommended not to include in the privacy policy, those aspects that change more often - such as data privacy procedures, controls deployed, processes, templates, etc.

5.4.2 *Processes & Guidelines*

The organization should define, document and deploy processes that are needed to implement the privacy policy across the organization. Such process should cover the following:

a) Determine the inputs required and the output expected from these processes.

b) Determine the sequence and interaction of the processes.

c) Determine and apply the criteria and methods (including monitoring, measurements and related performance indicators) needed to ensure the effective operation and control of these processes.

d) Determine the guidelines required to ensure the processes are followed uniformly across the organization producing consistent and repeatable results.

e) Determine the responsibilities and accountability for each activity.

f) Determine the steps to be taken in case these processes and guidelines are deviated and how such exceptions should be handled.

The process definition and deployment should take into account the need to integrate engineering and management aspects of DPMS as illustrated in Fig. 2.

5.5 Records and Document Management

Organization should maintain records of all processing activities that demonstrate accountability towards data privacy compliance.

While the list of records depends on the organization, below is an illustrative list of records that organization may need to keep in order to demonstrate accountability:

a) Evidence of acknowledgment for privacy notice and choice for consent. Records of various versions of privacy notice.

b) Logs of Data subjects request to their personal information.

c) Logs to demonstrate accountability of staff handling personal data.

d) Personal data inventory and personal data flows.

e) List of sub processors.

f) Logs to demonstrate fulfilment of data subject rights.

g) Privacy Incidents and personal data breach analysis – Root cause analysis reports.

h) Privacy impact assessment reports.

j) Records of deployment of various data privacy and security controls.

k) Periodic Risk Assessment Reports.

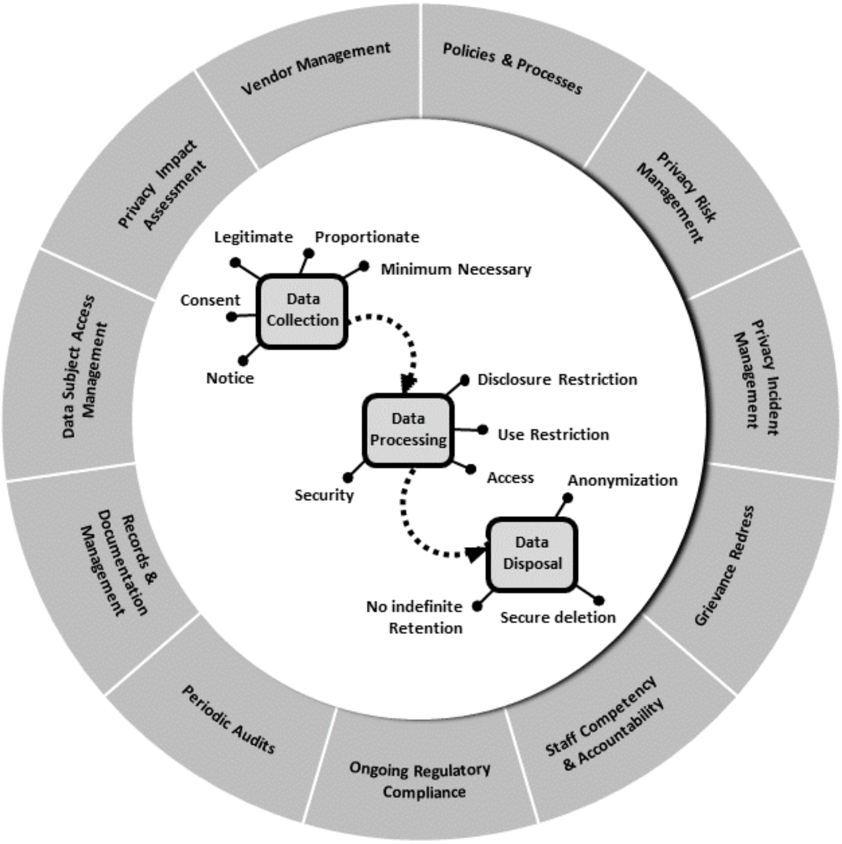

FIG 2. INTEGRATION OF PRIVACY ENGINEERING AND MANAGEMENT ASPECTS

5.6 Privacy Impact Assessments

Privacy Impact Assessment (PIA) is a set of activities which is conducted by an organization to identify and analyze the impact on data privacy due to a change either in regulation, business process or a technology platform, and to recommend data privacy controls and measures to minimize the impact of such change on data privacy of applicable stakeholders including data subjects. Such assessment should be conducted according to documented process, and records of the same should be retained for verifications and audit purpose. A typical PIA process is shown in Fig. 3.

Following are minimum recommended steps for PIA:

a) Develop thorough understanding of data processing involved, the data flow (both internal and external to the organization), various actors involved, applicable jurisdictions, type of information, purpose, etc.

b) Analyze the applicability of privacy principles depending on jurisdiction, organization’s own privacy policy and contractual requirements.

c) Determine if the data collected is appropriate, legitimate, proportionate, not excessive and has a clear defined purpose.

d) Identify areas of potential non-compliance, or gaps and identify alternative solutions. Emphasis should be privacy by-design and use of technology to minimize possibility of breach.

e) Recommend the solution based on privacy principles and regulatory requirements.

f) Verify compliance once recommendations are implemented.

The organization should ensure effectiveness of privacy impact assessment process for identifying, analyzing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personal information.

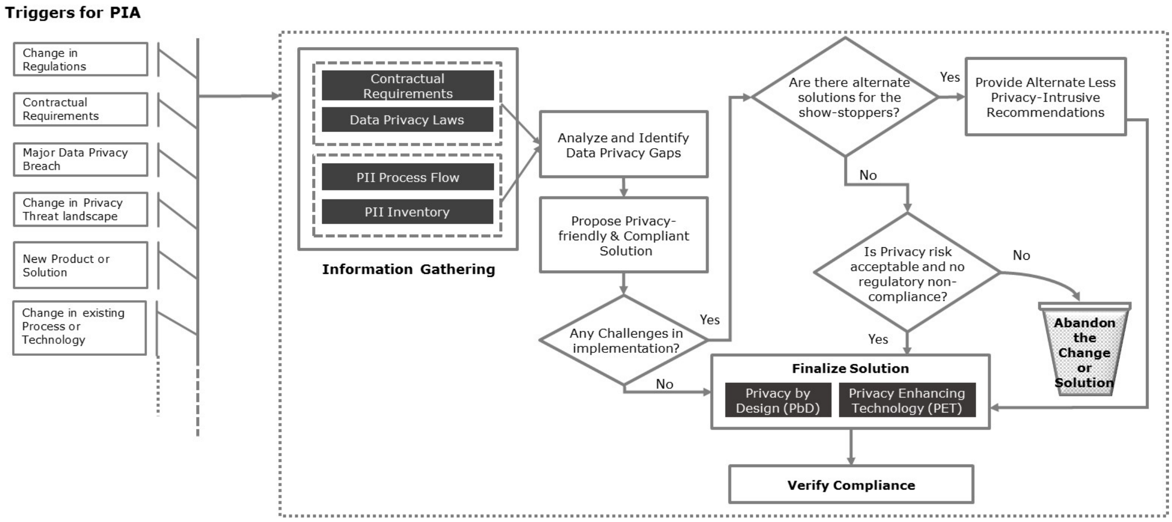
Triggers for PIA
Change in Regulations
Contractual Requirements
Major Data Privacy Breach
Change in Privacy Threat landscape
New Product or Solution
Change in existing Process or Technology
Contractual Requirements
Data Privacy Laws
PII Process Flow
PII Inventory
Information Gathering
Analyze and Identify Data Privacy Gaps
Propose Privacy-friendly & Compliant Solution
Any Challenges in implementation?
Yes
No
Are there alternate solutions for the show-stoppers?
Yes
No
Provide Alternate Less Privacy-Intrusive Recommendations
Is Privacy risk acceptable and no regulatory non-compliance?
No
Yes
Abandon the Change or Solution
Finalize Solution
Privacy by Design (PbD)
Privacy Enhancing Technology (PET)
Verify Compliance

FIG. 3 TYPICAL “PRIVACY IMPACT ASSESSMENT” PROCESS

5.6.1 *Triggers for Conducting PIA*

A review of different components of the PIA process may be triggered by the following considerations:

a) Technology change.

b) Periodic review.

c) Change in business or data ownership.

d) Change in business strategy.

e) Product or service change.

f) Regulatory change.

g) Customer and/or contractual change.

h) Operational change, including new/change application, supply chain (insourcing/ outsourcing), and site/facility resources.

j) Structural change.

k) Privacy incident or personal data breach.

5.6.2 *Assessment Templates and Tools*

The organization should use standardized assessment templates and tools across the organization to ensure uniform, reliable, accurate and repeatable privacy impact assessment. Records of privacy impact assessment should be retained for future reference.

5.7 Data Processor Management

5.7.1 *Data Processor Evaluation and Shortlisting*

The organization should have an effective process to evaluate and shortlist its data processors from a data privacy perspective to ensure that its controls are effective throughout the life-cycle of products and services.

Data processor evaluation allows an organization to understand and assess the capability of the data processor and its suitability for processing the personal information with minimal privacy risks. It helps in understanding the risk, the data processor brings with it into the organization. The evaluation and shortlisting approach should be consistent, however, the depth of analysis of any given data processor needs to reflect their criticality to the organization’s activities and the level of risk to which they are exposed.

The approach used for data processor evaluation will depend on the sensitivity of data. An organization may adopt the following broad structure for evaluation and shortlisting of data processors:

a) Organize relevant documentation currently available within the organization, for example, privacy impact analysis, business impact analysis, risk assessments, etc.

b) Define and document the approach, including defining parameters which will be used to assess the data processor criticality, privacy requirements etc.

c) Undertake the privacy impact analysis and privacy risk assessment with each data processor

d) Assess the overall level of privacy risk from each data processor

e) Review the results of data processors’ own analysis of its compliance to data privacy laws and data privacy contractual terms with the organization on periodic basis

f) Produce an overall analysis of the data processor capability against their criticality and organizations’ needs

5.7.2 *Transfer of Obligations*

The organization should ensure that proper contracts (clearly mentioning the data processor obligations) with the data processors are executed. Organizations should ensure the obligations are documented, understood, agreed by the data processor, and they are enforceable at the instance of the organization or the data controller as permissible by law.

The organization is expected to take responsibility for its data processors. Individual has the option to hold the organization (rather than its data processors) responsible for failure to protect their personal information and hence accountability in the event of a data breach should be agreed between the parties and clearly documented as part of contract. Therefore, an organization's brand is also at risk of damage in the event of a privacy incident by its data processor.

The organization may deploy suitable mechanisms to ensure that the data privacy function is made aware whenever a data processing is outsourced, so that proactively the privacy aspects are addressed.

5.7.3 *Periodic Reports and Compliance Checks*

The organization should ensure a process to report the privacy health of a data processor periodically. The nature of reporting can be defined based on the criticality of the data processor and the organization policies. The privacy key performance indicator's (KPI) of critical data processor should be reported to the top management as per the governance defined. The privacy KPI's should be reviewed with respective data processors periodically and accordingly actions should be prioritized.

The organization should ensure privacy compliance checks are done periodically to determine the privacy health of a data processor. These can be part of the organization internal audit program. The organization can consider doing a second party audit or a third party audit on the data processor depending on the criticality of the data processor to the organization. The summary of the results of these compliance audits and checks should be presented to the top management as part of the organization's governance and management review and actions should be formulated for the issues crossing the organization's risk thresholds.

5.8 Privacy Risk Management

Data Privacy as a need for individuals often conflicts with business interests and innovation in organizations that collect personal information from such individuals. Any enterprise needs to make profit to survive and in the digital era, personal information is often not only an information asset that needs to be protected but also leveraged for business benefit within legally permissible limits. Hence, there is a delicate balance which organizations need to maintain by taking into account the privacy risk exposure vis-a-vis business interests. Privacy risk management involves identifying, analyzing and evaluating privacy related risks, responding to them by building or modifying controls to reduce their likelihood or consequences in order to maintain the residual risks within acceptable limits, before a solution or product is rolled out.

5.8.1 *Triggers and Periodicity for Privacy Risk Assessments*

The organization should define, document and implement a process for assessing the level of risk to individuals associated with the processing of their personal information. Such risks should be conducted periodically for various entities such as data processing functions, units, locations, products or solutions. Such assessment should be done separately for privacy and should not be combined with security since there are areas where there could be conflict between the two.

The risk assessment process should define the method of risk evaluation adopted which could include a risk outcome metric derived as a factor of parameters such as estimation of probability of occurrence of event, impact the risk is likely to have on individuals and organization, detectability of risk before it materializes, etc.

Risk assessment is quite similar to privacy impact assessment, except that the former is a periodic exercise, whereas the latter is triggered based on certain events, as mentioned in **5.6**. The periodicity of risk assessment should be determined based on risk exposure and how dynamic the organization environment is. Organizations typically follow periodicity of one year, although in rapidly changing environment, half-yearly frequency or even more often, may be desirable.

5.8.2 *Criteria for Risk Evaluation*

Organizations should define privacy risk evaluation criteria and the same should be used consistently while assessing privacy risks. Such criteria should take into various factors such as:

a) Sensitivity of personal data.

b) Potential harm to data subjects in the event of a personal data breach.

c) The volume of data.

d) The extent of data use by various recipients.

e) The degree of data protection measures implemented, such as encryption, pseudonymization, etc.

f) Involvement of external party in processing data.

g) Data transfer to a country outside organization's jurisdiction.

h) Organization's risk exposure in the event of a privacy incident.

5.8.3 *Privacy Risk Response Strategy*

The organization should define the strategy for reducing privacy risks to acceptable levels. Based on the outcome of the risk evaluation, privacy risks are typically classified into relevant severity levels. The risk response strategies would define how risks will be treated based on evaluation. Privacy risk response options may include the following:

a) Mitigating the risk by reducing the likelihood.

b) Mitigating the risk by reducing the consequences.

c) Building contingencies to manage the risk at a later date.

d) Transferring the risk to external party.

e) Terminating the process that leads to the risk.

f) Accepting the risk.

Risks with low probability may not be ignored and care should be taken to focus on those risks the probability of which is very low but impact is extremely high. Compensating controls may need to be planned when a risk needs to be accepted. The appetite for risk may vary from organization to organization. It is also important to implement a program to periodically exercise the contingencies planned, if this is the chosen risk response.

5.9 Privacy Incident Management

Despite adoption of best practices and processes, no organization can be completely immune from data privacy incidents, including personal data breaches, and hence they should be always prepared to handle such incidents effectively, in case they happen. Organizations should put in place a data privacy incident handling process that includes awareness of incident occurrence, management, reporting obligations to regulators and affected individuals, corrective and preventive action planning and implementation.

Organizations should put in place mechanisms on how individuals (whether affected party or not) can report data privacy incidents to the data privacy function within the organization. The organization should communicate these incident reporting channels to all individuals through various means including the company website.

5.9.1 *Incident Handling*

Any incident reported, should be promptly attended to and tracked to closure. Incident handling may typically involve following stages:

a) Incident reported and logged.

b) Acknowledgement to the person or organization who reported incident.

c) Immediate corrective action to contain data privacy violation.

d) Root cause analysis, including determination of involvement of any data processor /external party.

e) Data Breach reporting to affected individuals and regulators (if applicable as per regulations).

f) Preventive action.

Functions within the organization and any external agencies that need to support incident management, should be promptly involved during various stages of incident handling based on the need. In the event that external party is responsible for having caused the breach and there are penalties levied or individual claims, the incident management should also involve determination of accountability for the incident and sharing of any financial impact between the parties involved. Often personal data breaches occur due to a security lapse, in which case the information security function should also be part of incident handling.

5.9.2 *Personal Data Breach Reporting*

Personal data breaches often impact individuals, and hence, organizations should determine the need for reporting the breach to affected individuals, if they have reasonable grounds to believe that individual’s privacy has been compromised. Such notifications should have a clear purpose such that the individuals who have been affected can take steps to protect themselves. Not all personal data breaches impact individuals, for example when a file consisting of personal information is inadvertently sent by an employee of an organization to his personal email address, if the organization ensures that the same is promptly deleted, and if it was not forwarded or distributed further, reporting to individuals may not be required. But if personal information is exposed in a website to public inadvertently or accidentally, the same may have been viewed by public, and hence may need reporting. It also depends on the nature of personal data involved and likely harm the disclosure can cause to individuals.

Organizations may also be required to report to regulators and appropriate government bodies, about a data breach, if required by the applicable laws. Timeline within which data breach needs to be reported should be as per the timelines specified in applicable law. The need for this should be established by the organization and relevant procedures should be promptly followed. Personal data breach reporting may depend on various factors such as:

a) Legal requirement from applicable regulations to notify.

b) Contractual obligations, in the event the organization is a processor.

c) Sensitivity of personal information.

d) Notification of such breaches will help the individual protect themselves.

e) Number of data subjects affected.

When organization is a data processor, it should not decide on breach reporting to Data Privacy Authorities and instead act as directed by data controller organization.

The notification may include the following:

1) Description of data breach.

2) Number of individuals, type of data subjects, nature of data.

3) Action taken to contain the consequences of breach.
4) Root cause.
5) Measures being undertaken by the organization to prevent recurrence.

The organization may also consider notifying external agencies such as law enforcement agencies, insurers, industry bodies, bank or credit card companies which can assist in containing the damage or help in reducing the risks of financial loss caused by the data breach.

5.9.3 *Preventive Actions*

Privacy incidents including personal data breaches may invoke penalties not only from regulators and customers (if the organization is a data processor for that customer) but sometimes victims may also claim compensation, depending on applicable laws. More importantly instances of non-compliance and data breach lead to negative brand impact.

The penalties can be significantly lower or can be avoided if the organization can establish that the breach is not caused due to absence of process, control measures and that the due diligence was exercised. Hence, organizations that process personal information should take appropriate measures to minimize possibility of data breaches.

Organizations should define, document and implement process to conduct detailed investigation for root causes of privacy incidents with help of all stakeholders including any external parties involved in data life cycle and determine a preventive action plan to minimize probability of recurrence of incidents. Records of preventive action should be maintained.

5.10 Data Subject's Request Management

5.10.1 *Access to View Data*

Organizations should be able to provide access to individuals to view their own data available with the organization. An individual may typically like to know what data is held about him/her, how long it is kept, how to access his/her data and may request such data to be provided. In certain jurisdictions, organizations may levy a small fee for providing data, particularly to prevent frivolous requests from individuals. Most of the data privacy regulations require organizations to have a mechanism in place to receive individual access requests and handle them to respond within reasonable amount of time.

Organizations may face penalties and fines if they are unable to do so in timely manner. However, organizations need not provide data when the retention period for the data has lapsed and data is deleted as per defined policy on periodic basis.

It is extremely important for organizations to establish the identity of an individual before providing data, to avoid unauthorized disclosure.

5.10.2 *Ability to Update Data*

Organizations should provide means for individuals to update their data. Personal information often changes with time, for example photograph, marital status, etc. and it is individual's right to ensure that these changes are correctly reflected in organization's database. If online access cannot be provided then organizations may have an email address to which individuals can write to, and organizations should, within a reasonable time, update the data, and also once updated a notification should be sent to individual to check the correctness of data.

5.10.3 *Access to Privacy Notices*

Privacy notices which an individual would have read and agreed to, should be always available for them to access. This helps an individual to know what terms they agreed to for processing.

The organization should therefore retain evidence of consent provided and options chosen.

This may be made available online to the extent possible, but only after establishing identity. Alternatively, they may be provided on request.

5.10.4 *Requesting Mechanism*

For any access request from individual to be valid, it should be made in writing. Although organizations can provide a standard format for individuals to include all the details the organization might need to locate the information they want, such formats should not be deemed mandatory.

Data requests may be valid in some jurisdictions even if the individual has not sent it directly to the person or function which normally deals with such requests and hence organizations should put in place procedures that make it easy for anyone in the organization to recognize such requests and route it appropriately.

Organizations should seek enough information, as appropriate to establish identity of the person making the request. This is to avoid personal information about one individual being sent to another, accidentally or as a result of deception. The level of checks to be made depends on the possible harm and distress which inappropriate disclosure of the information could cause to the concerned individual.

5.10.5 *Service Level Agreements*

The organization should ensure that they respond to an individual's access request promptly or as communicated in the privacy policies. If regulation or contracts specify time for servicing access requests, the same should take precedence.

If a longer duration is required to retrieve information being sought, the individual should be informed about the possible delay.

5.10.6 *Considerations for Fee*

Organizations should be allowed, if they so require, to charge a fee to service individual's access requests. Such fees should not be charged for access requests to health records. Even though, organizations need not comply with a request until the fee has been received, they should not ignore a request simply because the individual has not sent a fee. If a fee is payable but has not been sent with the request, the organization should contact the individual promptly and inform them about the same.

5.11 Grievance Redress

The organization should implement an efficient and effective grievance redress mechanism. Depending on jurisdiction, certain regulations may specify timelines within which a grievance should be resolved, as in case of individual access requests. Such mechanism should also take into account the possibility of the cause for the grievance originating from the processing undertaken by a different entity, external or internal.

5.11.1 *Identification and Publication of Identity of the Grievance Officer*

Depending on applicable laws and regulations, there may be a requirement where an organization should appoint an Officer, who should be in charge of the grievance redress process. Once appointed, the name and contact details of the Officer should be published at the various public and internal touch points that the organization has.

The organization, may chose the Data Privacy officer to play the role of a Grievance officer or keep these roles different.

5.11.2 *Channels for Receiving Complaints*

Apart from providing contact details (as mentioned in **5.11.1**), the organization should also provide alternate mechanisms to the individuals so that they are able to direct their grievances regarding the data privacy to the appropriate department in the organization. These mechanisms or channels may take various forms including, but not limited to:

a) Online forms.

b) Telephone contact centers.

c) Kiosks/help desks.

d) Email addresses.

5.12 Staff Competency and Accountability

In any organization, staff and employees have a key role in protecting personal information held by the organization, since they will often have access to the data, during processing operations, Any mishandling of data, whether due to ignorance or negligence can lead to personal data breach, financial and reputational damage to the organization. It is therefore important for the organization to establish accountability for staff responsible in ensuring data privacy, and create regular awareness.

5.12.1 *Traceability to Employee's Actions*

The organization should establish mechanism for maintaining traceability, logs and audit trails to employee's actions on data processing. This is extremely important to,

a) Comply with the 'due diligence' requirements of applicable laws.

b) Identify root causes in the event of a personal data breach.

c) Defend the organization from a litigation.

d) Bring ownership to data processing activities from employee's actions.

e) Reduce incidence of personal data breaches.

5.12.2 *Training and awareness*

The organization should define and document process to create awareness, and train staff involved in processing personal information. Appropriate interventions should be introduced to ensure that such training and awareness programs are conducted periodically, cover entire staff involved in data processing, in any of its functions, departments and business units.

Training modes should take into account the varying needs and capabilities of participants from different functions, countries, cultural group, and educational background.

The mode of delivery could be class-room based, web based, live meetings, e-learning, emails, video conference, etc. Awareness and training content should be regularly updated to reflect regulatory developments, process changes, etc.

Attending such programs should be mandatory for entire staff, failing which appropriate disciplinary action may have to be taken.

5.12.3 *Employee Declaration*

In any organization, staff from certain functions have relatively higher access to personal information by nature of their work responsibility. Such employees should be signing a privacy declaration stating that they will exercise due diligence and they are aware of impact due to a privacy incident including personal data breach. Such declaration could be in hard copy form or electronic.

Signing of such declaration by employees acts as a deterrent and not a substitute to make them aware of new developments on regulations, technologies, threats etc.

5.12.4 *Disciplinary Actions*

If any staff who is responsible for data privacy is proven to be negligent or ignorant, and leads to causing a privacy incident, that individual should be subjected to disciplinary actions. The action could be ranging from an email warning to termination depending on severity and applicable employment laws.

Such actions not only help in conveying a serious message to entire staff that the organization takes data privacy very seriously, but also helps to set an example to regulators and customers.

5.13 Ongoing Regulatory Compliance

Ongoing compliance with all applicable regulations and contracts is a hallmark of a good Privacy Program. Privacy and related regulations evolve and get updated regularly, which may impact the effectiveness of data privacy controls deployed by the organization.

The organization should put in place policies and procedures that allow data privacy function to continually assess whether the Data Privacy Management Systems will be able to demonstrate compliance with the applicable data protection legislations and regulations, and any changes to regulations are incorporated in timely manner.

Some of these day-to-day responsibilities should include:

a) Ensuring the organization has access to legislative updates and appropriate guidance related to data protection legislation.

b) Conducting management reviews of the privacy policies and processes.

c) Continuously checking that the DPMS reflects changes in legislation, practice and technology.

d) Assist in the interpretation and application of the various regulatory exemptions applicable to the processing of personal information.

The organization should incorporate policies and procedures that allow it to identify when amendments to contracts or regulatory changes occur and trigger alerts so that changes are undertaken on data processing and privacy controls in solutions and products. In the event that the amendments require a revision of the organization’s privacy procedures related to these contracts, such changes will need to be assessed prior to implementation to ensure that the requirements of the privacy policy and regulations are met.

5.14 Periodic Audits

Like in case of any other compliance and risk function, conducting periodic audits is a very important activity for data privacy program. In order to make audits effective, the audit function should be independent from the function responsible to implement data privacy controls. The audits should be conducted at a periodicity appropriate for the organization, at least once in a year.

5.14.1 *Compliance to DPMS and Effectiveness of DPMS*

Privacy Audits may be broadly classified into following two types:

a) Adequacy Audits

These are intended to verify whether the planned arrangements in the organization, when implemented will lead to compliance to data privacy regulations and intended privacy objectives.

b) Compliance Audits

These audit activities are focused on verifying the actual deployment of privacy controls with reference to the planned arrangements such as privacy policy, privacy processes, guidelines etc.

Since an organization can never be sure that all kinds of privacy threats are known and take mitigation action on them, it is important for audits to not restrict itself to verification against plans and processes, but examine if the mechanisms to identify privacy risks are being effectively implemented.

5.14.2 *Audits Reporting*

Audit findings may pertain to non-conformance to established data privacy policies and processes or may be related to planned policies and processes not being effective to meet regulatory requirements. While the former category of non-conformances are attributed to business enabling and support functions within the organizations, the latter ones are normally in the purview of the data privacy function. Hence, the reporting of audit findings should be done to the senior management function to which the data privacy functions reports, in order to avoid conflict of interest and should be tracked for timely closure.

5.14.3 *Auditor Skills*

Since detecting non-compliances in data privacy requires thorough understanding of data privacy laws, data processing activities, data processing technologies, information security domains, it should be ensured that the audit team possesses all these skills and experience.

5.15 Measurement and Continuous Improvement

Measurement is key to demonstrate improvement hence appropriate metrics should be developed to track various aspects of DPMS. The metrics could be qualitative or quantitative, and need to be chosen among other factors, based on the current maturity of the organization. Examples of metrics are:

a) Lead time to mitigate privacy risks.

b) Number of critical privacy incidents.

c) Service Level Agreement to address and close privacy incidents/breaches.

d) Number of changes that were not subjected to PIA.

e) Percentage of staff trained on data privacy.

Continuous improvement requires sustained improvement in specific aspects of the DPMS without adversely impacting other aspect of DPMS. The triggers for improvement initiatives could be from unfavorable performance as reflected by the measurement program.

Improvement can be demonstrated broadly in two forms:

1) Consistent trend in improvement.

2) Exceeding set target based on industry standard.

ANNEX A

(*Clause* 4.1.1)

LEGAL PROVISIONS IN INDIA ON DATA PRIVACY

The list given below is not exhaustive and the latest applicable version with any Amendment (if any) should be referred to:

A GENERAL LAWS

A-1 INDIAN CONSTITUTION

'State' as defined in Article 12 of Indian constitution is obliged to protect Right to life defined in Article 21 of Indian Constitution. In August 2017, in a landmark judgement, the Indian supreme court declared "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under article 21 and as a part of the freedoms guaranteed by Part III of the constitution."

A-2 INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

a) Section 43 and 43 A: Deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.

b) Section 72 A: Deals with disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract. The offence has been also made punishable with imprisonment and fine as prescribed.

c) Section 85: Imposes corporate criminal liability and liability upon the officers of the company for offences related to privacy breach committed in a company.

A-3 IT RULES (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL INFORMATION OR INFORMATION):

The most comprehensive regulation as on date that is applicable to data privacy in India is IT Rules notified in 2011 under Sec 43A of IT (Amendment) Act 2008, which applies to body corporate processing Personal information.

A-4 SECTORAL LAWS

A-4.1 Banking

a) The Negotiable Instruments Act, 1881

b) The Prevention of Money Laundering Act, 2002

c) The Bankers Book Evidence Act, 1891

d) Credit Information Companies (Regulation) Act, 2005

e) The Insurance Act, 1999

f) Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983

g) Payment and Settlement Systems Act, 2007

h) The Banking Regulation Act, 1949

j) Indian Income Tax Act, 1961

k) Reserve Bank of India Act, 1934

m) Foreign Contribution Regulation Act, 2010

n) Fair Practice Code for Credit Card Operations, 2010

p) RBI regulations with reference to the Gopalakrishna Working Group report, 2011

q) Goods & Services Tax (GST) Act, 2017

A-4.2 E-governance and Identity

a) The Passport Act, 1967

b) The Representation of People Act, 1950

c) The Indian Penal Code, 1860

d) The Census Act, 1948

e) The Citizenship Act, 1955

f) The Registration of Births and Deaths Act, 1969

g) The Collection of Statistics Act, 2008

h) The AADHAAR (Targeted Delivery of Financial And Other Subsidies, Benefits And Services) Act 2016

A-4.3 Consumer

a) The Indian Contract Act, 1872

b) The Consumer Protection Act, 2019

A-4.4 Freedom of Expression

a) The Press Council Act, 1978. Cable Television Networks Regulations Act, 1995

b) Content Certification Rules, 2008

c) Justice (Care and Protection of Children) Act, 2000

d) Contempt of Courts Act, 1971

e) Indian Penal Code 18607.

f) The Indian Copyright Act, 1957

A-4.5 Law Enforcement

a) The National Security Act, 1980

b) The Indian Evidence Act, 1872

c) National Investigation Agency Act, 2008

d) Intelligences Organizations (Restrictions of Rights) Act, 1985

e) Central Bureaus of Investigations Bill, 2010

A-4.6 Internet and Communications

a) The Information Technology Act 2000

b) The Telegraph Act 1885

c) The Unlawful Activities (Prevention) Act, 2002

d) Internet Service Provider (ISP) License

e) Unified Access Service License (UASL) License

f) TRAI Regulations on Unsolicited Marketing Calls

A-4.7 Health & Medical

a) Medical Council of India's Code of Ethics Regulations, 2002

b) Epidemic Diseases Act, 1897

c) Mental Health Act, 1987

d) The Persons with Disabilities Act, 1955

e) Pre-Natal Diagnostic Techniques Act, 1994

f) Medical Termination of Pregnancy Act, 1971

g) Ethical Guidelines for Biomedical Research on Human Subjects

A-4.8 Transparency & Other Regulations

a) The Right to Information Act, 2005

b) The Official Secrets Act, 1923

c) The Prevention of Corruption Act, 1988

d) The Securities and Exchange Board of India Act, 1992

e) The Competition Act of 2002

f) The Lokpal and Lokayuktas Act, 2013

g) Whistle Blowers Protection Act, 2011

ANNEX B

(*Clause* 4.2.6, 4.2.7.2)

SECURITY AND PRIVACY CONSIDERATIONS FOR CLOUD INFRASTRUCTURE

B-1 SECURITY CONSIDERATIONS

B-1.1 The organization should consider extending organization security policies to the public cloud infrastructure and assets.

B-1.2 Perform security architecture review to assess that cloud service provider's electronic discovery capabilities does not compromise privacy or security of data and applications.

B-1.3 The organization should establish clear and exclusive right to data ownership. This control should be documented in the contract with the cloud service provider.

B-1.4 The organization should perform a risk assessment for virtualization and other logical isolation techniques that the cloud service provider employs in a multi-tenant architecture.

B-1.5 Define and document cryptographic key management with the facilities and processes of cloud service provider in the organization encryption policy.

B-1.6 Evaluate data security policies including security of data at rest, transmission and during disposal and deletion.

B-1.7 The organization should regularly analyze, monitor, and perform system audits for indication of inappropriate activity affecting personal information or to investigate suspicious activity.

B-1.8 The organization should ensure that incident management processes of the cloud service provider is aligned with organizations' requirement to prevent, detect, and report personal data breaches in compliance to applicable regulations.

B-2 PRIVACY CONSIDERATIONS

B-2.1 Compliance to Applicable Regulations

Organizations should be aware that despite outsourcing the processing activities to the cloud provider, it continues to be a data controller. Data Controller should comply with data protection laws which vary from country to country. Data Processor/Cloud provider is also required to adhere to laws and regulations to the extent applicable and stated as part of the contract.

B-2.2 Data Transfer Restrictions

In public cloud, organizations may not have control on which employee's data is located in which jurisdiction at different points of time. There are restrictions imposed by Privacy laws on data transfer between countries, for example, GDPR and other member nation laws put certain restrictions on data transfers outside Europe. Organizations should determine if such restrictions apply to them and if applicable implement appropriate controls to ensure data transfer is as per the applicable regulations.

B-2.3 Data Deletion

Data deletion may not be effective due to following reasons:

a) Data is not strictly wiped.

b) Timely data deletion may not be always possible, either because extra copies of data are stored elsewhere, or because the storage media also stores data from other clients.

c) In scenarios where organizations use less space than estimated, the part of storage media which usually stores their data could be used for another organization by the cloud provider.

d) Organizations should ensure that relevant clauses on deletion are added to the contract and cloud provider effectively deletes the data as per the requirements agreed.

B-2.4 Neighbor Subpoena Risk

In the event of a subpoena on another customer of the cloud provider, if physical hardware of cloud provider is confiscated by law-enforcement agencies as part of e-discovery, due to the centralized storage as well as shared tenancy of physical hardware, there is a risk of disclosure of organization's data to unwanted parties. The organization may be required under various regulations to inform their customers about the circumstances of the transfer of personal information to the cloud provider and the purposes of the transfer. Cloud provider should promptly inform the co-tenant of the cloud in case of subpoena and organizations should ensure the same is also added as part of the contract.

B-2.5 Data Breach Reporting

In the event of a data breach, regulations in certain countries require disclosure to the individuals and regulators. Cloud providers are expected to promptly inform the organizations about the breach and same should also be added in the contract. The cloud provider need to deploy mechanisms to proactively monitor and carry out timely reporting in the event of a data breach.

B-2.6 Logs and Audit Trails

Logs and audit trails should be maintained by the cloud provider and made available to organization for processing of data in the cloud.

B-2.7 Data Custody

Organization should clearly determine the following and take appropriate steps to have this documented in the contract as well:

a) Who actually owns the data on cloud?

b) What happens to the data if the contract gets terminated by either parties?

B-2.8 Data Privacy Clauses

Appropriate Data privacy clauses should be agreed and added to the contract between organization and cloud provider.

B-2.9 Data Subject Access

Data Privacy regulations may require organizations to provide timely access to personal information when requested by employee. Cloud provider should ensure that data retrieval and recovery is in line with customer expectations.

ANNEX C

(*Foreword*)

COMMITTEE COMPOSITION

Information Systems Security and Privacy Sectional Committee, LITD 17

Organization	*Representative(s)*
Ministry of Electronics & Information Technology, New Delhi	Shri Arvind Kumar (***Chairman***)
Bharat Electronics Ltd (BEL), Bengaluru	Shrimati Sangeetha Mangal Shri Devesh Kumar Singh (*Alternate*)
Centre for Development of Advanced Computing	Dr M. Sasikumar Shrimati P. R. Lakshmi Eswari (*Alternate*)
Centre for Internet & Society	Shri Sunil Abraham Shri Amber Sinha (*Alternate* I) Shri Gurshabhad Grover (*Alternate* II)
Data Security Council of India (DSCI)	Shri Aditya
Department of Science and Technology	Shri Sujit Banerjee Dr Rajeev Sharma (*Alternate*)
HCL	Shri Sanjeev Chhabra
Indian Cellular & Electronics Association (ICEA)	Shri Bijesh Kumar Roul Shri Rajesh Sharma (*Alternate*)
Infosys Technologies Limited	Mr Srinivas Poosarla Shri Rajeev Thykatt (*Alternate* I) Ms Ashwathy Asok (*Alternate* II)
In Personal Capacity	Dr Gargi Keeni Ms Amutha Arunachalam
Indian Statistical Institute	Prof Bimal K. Roy
KCPIL	Dr V. K. Kanhere
Larsen & Toubro Limited	Shri N. Sathyan Shri Tirumala Rao K. (*Alternate*)
Ministry of Electronics & Information Technology, New Delhi	Shri Rakesh Maheshwari Shri Tarun Pandey (*Alternate* I) Shri Santosh Soni (*Alternate* II) Dr Somnath Chandra (*Alternate* III) Shri S. K. Nehra (*Alternate* IV)
Ministry of Defence (DRDO)	Ms Noopur Shrotriya Shri G Anil (*Alternate*)
National Accreditation Board for Certification Bodies	Shri A. S. Bhatnagar Ms Anajna Jain (*Alternate*)
Narnix Technolabs Pvt Ltd	Shri Narang N. Kishore
NEC India Pvt Ltd	Ms Jidnya Shah Shri Abhay Pimplikar (*Alternate*)
Oxygen Consulting Services Pvt Ltd	Shri Sanjiv Kumar Agarwala Shri Sachin Jadhav (*Alternate*)
Patanjali Associates Pvt Ltd	Shri Kanti Mohan Rustogi
Qualcomm India Pvt Ltd	Shri Vinosh Babu James
ReBIT	Shri Prashant Lotlikar Shri Deepnarayan Tiwari (*Alternate*)

Organization	*Representative(s)*
Smart Chip Private Limited	Mr Divanshu Gupta Mr Ankit Gupta (*Alternate*)
Standardisation, Testing & Quality Certification (STQC)	Shri A. K. Sharma Shri A. K. Upadhayay (*Alternate* I) Shri Nakul Aggrwal (*Alternate* II)
Tata Communications Pvt Ltd	Shri Mahesh Kalyanaraman
Tata Consultancy Services	Shri Sateesh Sriniwsaiah Shri Natarajan Swaminathan (*Alternate* I) Shri Abhik Chaudhuri (*Alternate* II) Shri Anupam Agrawal (*Alternate* III)
Telecommunication Engineering Centre (TEC), DOT	Shri Arvind Chawla Shri S. Sridhar (*Alternate*)
THE PERSPECTIVE	Shri Rahul Sharma
Unique Identification Authority of India	Shri Yashwant Singh Shri Anup Kumar (*Alternate*)
WYSE Biometrics Systems Pvt Ltd	Shri Y. D. Wadaskar
BIS Directorate General	Shrimati Reena Garg, Scientist 'F' and Head (LITD) [Representing Director General (*Ex-officio*)]

Member Secretary

Shri Kshitij Bathla
Scientist 'C', BIS

Panel 3 "Privacy Information Management System" LITD 17/P-3

Organization	*Representative(s)*
Infosys Technologies Limited	Shri Srinivas Poosarla (***Convener***)
Reliance Jio	Shri Mohit Malik
Centre for Internet & Society	Shri Gurshabad Grover
Data Security Council of India (DSCI)	Shri Aditya
Genpact	Shri Srinjoy Banerjee
HCL	Shri Sanjeev Chhabra
Infosys Technologies Limited	Shri Rajeev Thykatt Ms Neha Agrawal (*Alternate*)
In Personal Capacity	Ms Amutha Arunachalam Ms Dimple Santwan
KPMG	Shri Srinivas Potharaju Shri Merril Cherian (*Alternate*)
Larsen & Toubro Limited	Shri Tirumala Rao K.
Ministry of Electronics & Information Technology, New Delhi	Shri Rakesh Maheshwari Shri Praful Kumar (*Alternate*)
Tata Consultancy Services	Shri Vijayanand Banahatti
THE PERSPECTIVE	Shri Rahul Sharma
Unique Identification Authority of India	Shri Yashwant Kumar Shri Anup Kumar (*Alternate*)

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: LITD 17 (12163).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices: *Telephones*

Central : Manak Bhavan, 9 Bahadur Shah Zafar Marg
NEW DELHI 110002
{ 2323 7617
{ 2323 3841

Eastern : 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi
KOLKATA 700054
{ 2337 8499, 2337 8561
{ 2337 8626, 2337 9120

Northern : Plot No. 4-A, Sector 27-B, Madhya Marg
CHANDIGARH 160019
{ 265 0206
{ 265 0290

Southern : C.I.T. Campus, IV Cross Road, CHENNAI 600113
{ 2254 1216, 2254 1442
{ 2254 2519, 2254 2315

Western : Manakalaya, E9 MIDC, Marol, Andheri (East)
MUMBAI 400093
{ 2832 9295, 2832 7858
{ 2832 7891, 2832 7892

Branches : AHMEDABAD. BENGALURU. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. DURGAPUR. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. JAMMU. JAMSHEDPUR. KOCHI. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAIPUR. RAJKOT. VISAKHAPATNAM.

Published by BIS, New Delhi