DSCI
PROMOTING DATA PROTECTION

DSCI Digest

January 2025

DSCI Digest

The DSCI Digest is brought to you for a peripheral understanding of the industry-relevant studies conducted by DSCI. It aims to help you learn and understand the subjects in discussion in a succinct composition.

About this Edition

The edition comprises the publications of the DSCI Privacy Leadership Forum, convened to bring together privacy leaders in a common council to enable the industry's privacy preparedness.

For more details, visit: https://www.dsci.in/content/dsci-privacy-leadership-forum

Table of Contents

PRIVACY BY DESIGN

Guidance on Practical Implementation for Businesses

The collection and use of personal and sensitive personal data is increasing day by day and is expected to grow to more than 180 zettabytes by 2025 owing to the usage of technologies such as social networks, big data, mobile computing, among others. Personal data has become a key asset across the globe, being characterized as the new oil that should be managed with high responsibility and accountability. However, reports on privacy violations suggest that implementing good data privacy practices and Privacy by Design and default principles are still not the universal norm.

In the context of data protection, it is important to consider both the socio-cultural posture and the technical aspects of securing personal data. In simple terms, data protection can be understood as the ability to exercise control over personal information, maintaining agency over the collection, use, and disclosure of one's personal information. In an organization, each function has a role to play with respect to protection of personal data or Personally Identifiable Information (PII).

Today, digital technology dominates the data collection paradigm which has furthered digital footprint penetration of an individual. This makes it important for organizations to process personal data lawfully and implement the right measures to process the data securely.

In addition to this imperative, the observed overarching principles in most data privacy laws and regulations are found to be transparency and lawful processing of personal data, and protection of the rights and freedoms of data subjects where the term data subject refers to individuals who are identifiable in relation to such personal data. It may be read to include inferences to data principals, natural persons, individuals, etc. as called in different data protection laws.

Foundational principles for processing personal data include: Purpose Limitation, Data Minimization, Accuracy, Storage limitation, Integrity and Confidentiality.

Hence, implementing Privacy by Design (PbD) becomes significantly important.

It was first proposed by the Information and Privacy Commissioner of Ontario, Canada, Ann Cavoukian, in the 1990s. It is further governed by 7 foundational principles, that emphasizes on:

1.Privacy as a default setting
2.Preventative rather than remedial approach
3.Privacy embedded in the design
4.Full functionality for efficiency at business and privacy level
5.Privacy protection throughout the lifecycle of data processing
6.Visibility and transparency in data processing
7.Keeping data processing user-centric

At present global recognition of PbD is being done across various data privacy regulations. Few of the notable regulations where PbD has been adopted include GDPR-Europe, California Consumer Protection Act (CCPA)-US, Lei Geral de Protecao de Dados (LGPD)-Brazil and the most recent being ISO's adoption of PbD as a norm in ISO 31700 framework.

In India, under the Digital Personal Data Protection Act, 2023 (DPDPA), the Privacy by Design principle is not explicitly stated. However, obligations on data fiduciaries require them to implement appropriate technical and organizational measures to ensure compliance with the Act. This working paper briefly explains the theoretical concepts of Privacy by Design along with the aim to act as a jurisdiction and sector-agnostic playbook to operationalizing PbD in the practical world of business and services.

In addition to Privacy by Design (PbD), which integrates privacy into IT systems, operations, and business practices from the start, ensuring personal data is processed lawfully and ethically, there is Privacy by Default. This concept ensures the strictest privacy settings are applied automatically, requiring minimal user intervention after a product or service is released.

The mentioned foundational principles along with the data privacy principles can then be combined to establish the practical implementation of PbD. Furthermore, effective implementation can be achieved by implementing PbD from three different but related vectors of:

Business processes
IT systems/ applications
Operations

The approach to operationalizing it can be derived from various anchor points. The most appropriate approach can vary based on the size, scale, complexity and nature of the organization, systems, and stakeholders in scope of the program, which include, business goal driven, risk driven and collaboration driven.

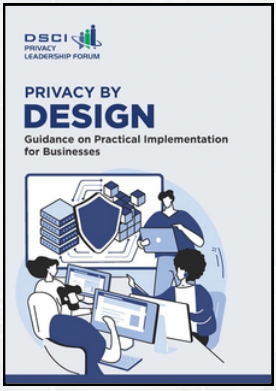
Adoption of PbD in these related vectors can be observed via multiple examples including building a data inventory, mapping data transfers, identifying data collection points, setting up a functional DPO (Data Protection Officer) office, crafting a robust data privacy training module that covers all roles, implementing strong technical controls, usage of PETs, and many more.

Further magnifying the vectors in the discussion that follows, it can be learned that effective realization of PbD for organizations can be done if several business processes are in place. Like, understanding all sources of data collection will help the organizations to
understand how and what data is coming into an organization. A lawful basis of processing to every category of personal data that is collected and processed. Establishing a process to know your data, particularly the inventory. Implementation of relevant privacy policies is also a must to assess the impact. Moreover, having complete transparent knowledge on the storage of the personal data.

When talking about operationalization certain steps can be taken for ensuring PbD irrespective of the chosen approach. Like an accountable and empowered data privacy office with the appointment of accountable personnel. Identifying accountable stakeholders who will help implement, fulfill, run, and help govern the data privacy and protection obligations. Adoption of a governance model to measure, update, and govern the privacy framework.

Implementing Privacy by Design (PbD) relies heavily on technology interventions, including the alignment of PbD with technology and adopting PETs. Key measures include using strong authentication methods, minimizing generic accounts, and deleting temporary work files.

However, these efforts are effective only with a strong privacy culture within the organization. Utilizing identified vectors and principles is essential. For more on this concept, visit:
https://www.dsci.in/resource/content/privacy-design



PRIVACY AT THE WORKPLACE

A Practical Guide to Ethical Employee Data Management

Right to Privacy at the workplace is important to ensure better safeguards to the personal data recorded pre and post-employment. But the attempt here is to learn about privacy beyond the traditional employee-employer relationship. Other types of economically beneficial engagements, such as those involving gig workers or freelance service providers connected via digital platforms are also included in the scope. The central principle here refers to the workers who in exchange for economic benefit in terms of compensation, trade in their skill/ labour to add value to the organization.

Privacy is understood to be of four types: (i) informational privacy, (ii) bodily privacy, (iii) territorial privacy, and (iv) communications privacy. These mentioned privacy types are equally applicable to workers and employees but the focus is drawn here to informational privacy. This type of privacy is exercised by workers over the data/information collected and processed about them by the organization. This includes the processing of personally identifiable data collected through the range of technologies, tools, and equipment deployed in the process. The degree of control that can be exercised by a worker directly implies the 'rights' and 'protections' that are granted or guaranteed to them.

But the privacy rights of employees and business interests of the organization may become contradictory or conflicting in certain scenarios where there is paramount interest in organizational data confidentiality, need for better optimized working by tracking employees, the want to safeguard employees against harm, and breach resulting from remote working. Having said that, the key focus needs to be on balancing organizational objectives with ethical and responsible processing of personal data of employees.

Today many work models have emerged, the traditional definition of an employee and worker have expanded to include third-party deployment, consultants/ freelancers/subject matter experts, Interns, Apprentice, Volunteers, Assistants, Gig workers, and Employment Applicants. However, there may not be stringent documentation or oversight over the

processing of personal data due to the informal, and often short-term nature of the relationship. A lack of governance and accountability here could detrimentally impact the data protection and privacy rights of individuals who engage in this type of informal work. Moreover, it is difficult to rely on consent as a valid ground for processing, as the requirements of 'free' and 'unambiguous' consent cannot be fully established between employer and employee as unequal negotiating parties, where one of the parties is dependent on the other for economic benefits. As technology becomes more integrated into the workplace, it's crucial to establish clear guidelines for processing employees' personal data. With rapid digitization and pervasive data-driven decision-making, escaping incidental data processing is difficult.

We therefore try to look at guidance across the EU, US, U.K. and China on privacy of employees to analyze the situation.

In the EU, personal data may be processed under any of the lawful bases under the General Data Protection Regulation (GDPR), however, in the context of employment, consent cannot be said to be freely given due to the power imbalance between the employee and the employer.

In the UK, the Information Commissioner's Office (ICO) has published the Employment Practices Code, and started consultation for developing guidance around 'monitoring at work.' Monitoring of workers to be done in a manner which is lawful and fair to the employees, constantly incorporating established data protection principles in all forms of occasional or systematic technologies or purposes.

China enacted the Personal Information Protection Law (PIPL) in 2021 which provides for the legal basis and obligations for employers while processing personal data of their employees in a similar phrasing as Article 88 of the EU law.

In the US, there is no comprehensive federal legislation. Instead, sectoral and state regulations continue to govern the space.

Following this, in India, after the enactment of the DPDP Act, its section(7)(i) has empowered organizations to process personal data for the purposes of employment without consent to protect and prevent any loss or liability, avoid corporate espionage, and maintain the confidentiality of trade secrets, intellectual property and clients.

Data processing takes place across different stages in employment, namely; pre-employment stage, employment stage, outsourcing, cessation of employees and processing data of former employees.

We therefore pan out recommendations for data processing in these stages.

The pre-employment stage begins with advertisement and ends in background verification for the shortlisted candidate. It is recommended the candidate should be notified of data keeping in advance. Necessary consent must be obtained before the personal data of reference is disclosed. The data collected for processing and the intended processing must be proportional to the objective pursued.

In the employment stage it is recommended that apart from informing them of the stored data, employees should have the right to rectify the details when needed. Employers should look for less invasive means to capture employee data and delete data in case of candidature dropout. For ensuring accurate records, regular checks should be done with the employee.

Oftentimes, organizations outsource the data processing of employee records. In that scenario, it is then advised to define the obligations in a clear manner. It is also necessary to highlight the data demarcation for processing with clarity. In case of change in jurisdiction, it is advisable to check for data transfers in accordance with the same.

When there is cessation of employment records, the account access should be monitored to avoid undue access.

For data processing of former employees it is suggested that bare minimum and only requisite data should be collected.

And for gig workers, it is recommended to have explainable, transparent, fair and accurate data processing. Additionally, having a third-party evaluator would further strengthen the commitment to anti-discrimination.

But the details are more expansive with regard to the subject, all enclosed here at our report on "PRIVACY AT THE WORPLACE: A Practical Guide to Ethical Employee Data Management": https://www.dsci.in/resource/content/privacy-workplace

PRIVACY ACROSS BORDERS

Guidance on Cross-Border Data Transfers for Indian Organisations

Privacy, as a discipline, has moved forward substantially over the last few years. Multiple dimensions, facets, and nuances of the subject are coming to the fore, nudging the ecosystem in a direction where Privacy is taking center stage.

Data protection regimes are also cautiously getting strategized, comprehensive legislation anchored on the principles of transparency, accountability, and demonstrability are being enacted. Taking a leaf from the current understanding it has been observed that in the increasing pace of digitalization, global companies are rendering services to users in India, and similarly, Indian corporations are offering their products and services to a worldwide customer base. The phenomenon, in turn, has made data transfers between jurisdictions inevitable.

In the digital era, accessing, utilizing, and transferring data across borders is critical in driving economic growth in every industry and country. This interdependence triggers a meticulous evaluation of the specific locations and methods used for data storage and processing.

Factors like cost of location i.e., data centers, and nature of data information are relevant factors to consider for data transfers between entities and jurisdictions.

For example, the protection of sensitive information like health and financial data requires additional implementation of safeguards. Adding to the complexity, the rapid transfer of huge volumes of data between jurisdictions with varying degrees of privacy protection laws means that the privacy and security of such data are in a constant state of limbo.

For instance, the European Union (EU) jurisdiction imposes stringent requirements for personal data transfers to countries outside the EU by requiring adequacy decisions or, in the absence of such a decision, appropriate safeguards. India's recently enacted Digital Personal Data Protection Act, 2023 (DPDPA) also restricts Data Fiduciaries from transferring personal data to certain notified jurisdictions. Similarly, retail cross-border transactions including e-commerce purchases, bank transfers, card payments, alternative

payment methods (e.g., digital wallets and mobile payments), and remittances, typically occur between different parties located in different countries.

Therefore this guidance focuses on providing mechanisms for enabling data transfers that offer two-fold benefits in meeting business and operational requirements while championing privacy protection in the context of the DPDPA.

This guidance is particularly suitable for the following individuals and entities for their work and data transfers per the Indian DPDPA 2023:

- Privacy Practitioner(s)
- Data Protection/Privacy Officers and related functions
- Organisations (Indian and non-India-based) need data transfers to provide goods or services

The scope and applicability of DPDPA Provisions on Data Transfers includes the following considerations:

- Activities that fall under the ambit of cross-border data transfers include processing the personal data of individuals within the territory of India.
- The Central Government can restrict the transfer of personal data to certain countries or territories outside India by way of a notification.
- The scope of DPDPA provisions on cross-border data transfer applies to all industry sectors, private and government organisations, startups, Micro, Small, and Medium Enterprises (MSMEs), and Significant Data Fiduciaries (SDF).
- If sensitive and critical personal data needs to be processed outside India, the personal data elements should be protected using adequate technical and security controls before commencing processing activities in other countries.
- The act would not restrict the "applicability of any other sectoral or specific laws" currently enforced in India that provide a higher degree of protection.
- The DPDPA notably has an extraterritorial reach, extending its applicability to Data Fiduciaries located outside India.
- Limitation still prevails based on context for those scenarios of the personal data being transferred via video/audio-based conversation or e-mail, which needs to be deliberated in future guidance.

The government has also laid plans for the basis of data transfers. It will ensure the circulation of a negative list, consisting of countries or territories outside India where a data fiduciary may not be able to transfer data. But the list also includes exemptions, which are made for any court, tribunal/legal body in India, or when there is a need for necessary enforcement of a law or right, or to prevent/investigate/prosecute the violation of any active law.

For business stakeholders and industries, exemptions have been made on contracts involving the data processing of data principals outside India; the merger/acquisition/division of organization(s) that is approved by a court/tribunal or any competent authority by law; the financial institutions who seek defaulters for payment.

Research and security exemptions are made for the central government for Indian sovereignty and security of the State and for data that will not influence the decisions about a data principal.

Regarding outbound data transfers, it is suggested that technical, process, and security controls be exercised before transferring critical data. Maintaining a record of which will be handy for reference and audits. In addition, identifying your obligations in the process is equally crucial for transferring digital personal data across borders.

Many countries now have laws to restrict personal data movement outside their territories. These laws can impact how companies use service providers in locations such as India. Owing to this, data transfers to emerging economies are generally only permitted where appropriate safeguards have been put in place. This would require understanding data transfers in and out the country, observing due diligence obligations, and discharging contractual obligations like:

- Purpose limitation
- Accuracy, Data Minimization, and retention
- Third-Party Discoure restrictions
- Security Considerations
- Data Subject Rights
- Subcontracting and onward transfers
- Liability Provisions

This will help the process. Besides these, a proper analysis of the risks to EU transfer will be an important consideration. Moreover, organizations may use this guidance to adhere to the DPDPA and global privacy laws while carrying out cross-border transfers or accessing personal data outside of Indian territory. More details on the obligations and cross-border data transfer are available in our report on "PRIVACY ACROSS BORDERS: Guidance on Cross-Border Data Transfers for Indian Organisations": https://www.dsci.in/resource/content/privacy-across-borders

PRIVACY DUE DILIGENCE

A Practical Guide for Data Protection Impact Assessments

Data protection refers to the process taken by organisations or businesses to ensure fairness in data processing and management of personal data, which is typically enshrined in data protection laws, regulations, and best practices. Data protection measures may include restricting access to information to prevent unauthorized access, obtaining consent from individuals when required, and maintaining the confidentiality, integrity, and availability of personal data.

In today's economy, collecting and processing personal information is vital to business operations. However, organisations also have a significant responsibility to safeguard their customers' data. To strike a balance between these objectives, businesses must evaluate the benefits and risks of their data processing activities. This is where a Data Protection Impact Assessment (DPIA) can help. Conducting DPIAs provides organisations with the opportunity to conduct due diligence on their data processing activities, identify privacy risks, and address them before commencing operations.

From a compliance standpoint, a DPIA is a type of privacy risk assessment mandatory under most data protection laws worldwide. Its purpose is to assess an organisation's adherence to overarching privacy principles and sectoral compliance requirements outlined in data protection laws.

A DPIA enables organisations to become more conscious and purposeful in their collection, storage, sharing, selling, or other transfer of personal data. But if the organization fails to adhere to state-of-the-art security measures or holds the data for too long, it becomes vulnerable to data breaches like identity theft, etc.

While DPDPA hasn't included sensitive personal data under its purview yet, businesses must understand its flow within the organization from a sectoral legal framework's standpoint. For example, RBI mandates data masking or redacting for sensitive data. Sensitive data includes but is not limited to children's data, biometric data, criminal conviction data, health, and financial data,

government-issued ID and more.

However, the sensitivity of data is determined by the legal definitions, the data's context, and the parties involved. On the other hand, sensitivity is only one aspect of privacy-related risks.

A DPIA primarily focuses on the reasons why personal data is processed, how it is processed, and the potential negative consequences of mishandling, misusing, or abusing the data. During the DPIA process, it is crucial to prioritize privacy rights, freedoms, and evolving expectations of data subjects. What triggers DPIA may range from Systematic and Extensive Processing, Cross-Border Data Transfers, Profiling or Automated Decision-Making, Sensitive Data Processing, Surveillance and Monitoring, Data Matching or Combining, New Technologies or Innovations, Publicly Accessible Data. Thus, conducting DPIA at these points can ensure that potential privacy risks are identified, assessed, and addressed early in the project lifecycle.

The benefits of conducting a DPIA cannot be missed and include:

- Ensuring privacy requirements are integrated into the project's conceptualisation and design phase.
- Raising awareness within the organization about data protection risks linked to the project to improve its design and enhance communication with stakeholders.
- Demonstrating compliance and avoiding penalties with privacy laws and regulations like DPDPA, GDPR, CCPA etc.
- Building public trust and confidence by improving communication about data protection compliance.
- Protecting customer data privacy rights and preventing potential violations.
- Streamlining information flows within projects and eliminating unnecessary data collection and processing to reduce operational costs.
- Integrating data protection safeguards into project design early to reduce costs and disruptions.
- Establishing trust and value amongst stakeholders.

This further solidifies that privacy should be considered an equal stakeholder in the risk management process rather than an afterthought. For a better DPIA, charting self-assessment criteria also becomes important in benchmarking the data processing activities. This may include questions regarding projects involving processing any special category of personal data, considerations on collections and sharing, project considerations surrounding consent, evaluation or scoring of personal data (including profiling and predicting), and use of new technology or data in novel ways.

With this in mind, following a

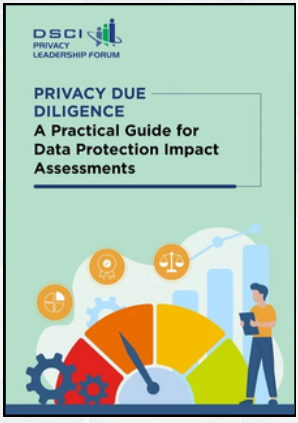
checklist regarding DPIA awareness and the DPIA process can help to address the prerequisites at an organisational level before initiating a project. Moreover, other regulatory considerations via inquiries can help with DPIA.

To conduct DPIA, the following steps should be taken:

- Describe the scope, context, and size of the data processing requirement.
- Identify whether there is a need for a DPIA based on applicable regulatory mandates.
- Assess the necessity and proportionality of data collection, whether it is required or achieved through any other means or legal basis.
- Carry out a risk assessment in terms of financial losses, data owner's rights, and data breaches or violations.
- Consult with internal and external stakeholders and record their views on the data processing.
- Establish measures to mitigate the risks by implementing security controls and data masking techniques.
- Prepare a report on the outcomes and take sign-off.

It also has to be noted that the scope and requirements of a DPIA are based on country-specific data protection laws, necessitating considerations that align with the legal frameworks of the respective countries. Therefore, inter and intra-country requirements for DPIAs can vary based on different factors, including data protection laws, regulations, and cultural considerations.

The specifics of inter and intra-country requirements for DPIAs will vary widely based on the legal, cultural, and regulatory context of each jurisdiction. Completing a DPIA also sends a clear message to others that your organisation is committed to protecting individuals' privacy and using their information responsibly. Regardless of the specific privacy and consumer protection laws applicable to your business, conducting timely and genuine privacy risk assessments can foster trust among your clients and customers. More on the DPIA screening exercise and data protection impact assessment is available in our report titled, "PRIVACY DUE DILIGENCE: A Practical Guide for Data Protection Impact Assessments" at: https://www.dsci.in/resource/content/privacy-due-diligence



What to Expect in the Next Edition

The DSCI Digest offers a condensed version of all our publications, giving you a quick overview to help you decide on your next read.

The subjects catered here enable you to gain first-hand information on the volumes we bring out for the industry. The information shared is a brief account of the conducted studies. You are requested to visit the reports on our website for better understanding.

https://www.dsci.in/knowledge-center/study-and-reports

Authors

- "PRIVACY BY DESIGN: Guidance on Practical Implementation for Businesses" by Shivangi Malhotra
- "PRIVACY AT THE WORKPLACE: A Practical Guide to Ethical Employee Data Management" by Shivangi Malhotra
- "PRIVACY ACROSS BORDERS: Guidance on Cross-Border Data Transfers for Indian Organisations" by Deepika Nandagudi Srinivasa
- "PRIVACY DUE DILIGENCE: A Practical Guide for Data Protection Impact Assessment" by Deepika Nandagudi Srinivasa

Compiler and Editor

Mridushi Bose, Content Marketing Manager

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by Nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit https://www.dsci.in/

DATA SECURITY COUNCIL OF INDIA
NASSCOM CAMPUS, FOURTH FLOOR, PLOT. NO. 7-10, SECTOR 126, NOIDA, UP - 201303
+91-120-4990253 | INFO@DSCI.IN | WWW.DSCI.IN

dsci.connect dsci.connect dscivideo data-security-council-of-india DSCI_Connect