DSCI
PROMOTING DATA PROTECTION

DSCI Digest



July 2024

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.

Table of Contents

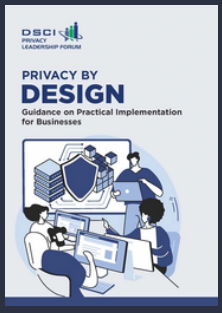
- PRIVACY BY DESIGN: Guidance on Practical Implementation for Businesses 4
- PRIVACY AT THE WORKPLACE: A Practical Guide to Ethical Employee Data Management 7
- Mitigating Security & Privacy Risks: A Guide to Enterprise Use of Generative AI 10

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

Personal data has become a key asset across the globe, being characterised as the new oil that should be managed with high responsibility and accountability.



Read the entire report

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

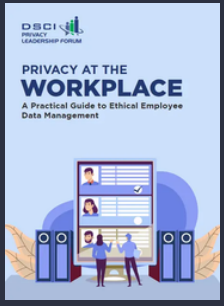
PRIVACY AT THE WORKPLACE

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

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.



Read the entire report

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

Mitigating Security & Privacy Risks

A Guide to Enterprise Use of Generative AI

We have stepped into the era of AI, where AI marvels itself to mimic human behaviors. Within AI, Machine Learning (ML) is found to employ mathematical methods to enhance computer performance through data-driven learning. DL (Deep Learning) is a subset of ML that utilizes multiple layers to encode data abstractions for constructing computational models and make intelligent decisions autonomously. This highlights that advancement in AI has revolutionized the ability of machines to perform complex tasks previously reserved for humans.

A new derivative in this domain is Generative AI (GenAI), which is built upon with neural networks, emulating the human brain's interconnected 'neurons,' recognizing patterns without explicit programming. Ian Goodfellow's Generative Adversarial Network (GAN) in 2014 sparked the field's growth, joined by models like Variational Autoencoders

Ian Goodfellow's Generative Adversarial Network (GAN) in 2014 sparked the field's growth, joined by models like Variational Autoencoders (VAEs) and Recurrent Neural Networks (RNNs), showcasing their content generation abilities.



Read the entire report

(VAEs) and Recurrent Neural Networks (RNNs), showcasing their content generation abilities. From basic language models to sophisticated content generators, generative AI evolved into an innovation powerhouse. Moreover, Gartner predicts over 100 million people will be engaging robo-colleagues by 2026, thus transforming enterprise work.

What we see today in the name of ChatGPT, Bard, DALL-E or Midjourney is the actualization of GenAI. The user interacts with the model by providing prompts, and the model leverages data from both cloud and on-premises sources. This data can be diverse, including text, images, speech; both in form of structured and un-structured data.

The rapid adoption of LLMs and GenAI is transforming businesses and promising significant advancements. However, unmanaged adoption for them can pose serious cybersecurity risks. As their capabilities in cybersecurity evolve, a two-fold approach is crucial; first, understanding the inherent risks and second, developing robust strategies to mitigate them.

Malicious actors could weaponize LLMs for crafting sophisticated cyber-attacks, spreading misinformation, or even gain unauthorized access to sensitive data. The vulnerabilities range from hardware and software to user-level threats like misinformation and fraud.

There are certain vulnerabilities and threats inherent to LLMs. For instance, attackers might manipulate input data to produce incorrect outputs. A few of these threats include adverserial attacks, involving intentional manipulation of machine learning models; data poisoning, where attackers insert malicious data in the training dataset; backdoor attacks, where training data manipulation embeds hidden backdoors that activate at certain triggers.

What is more alarming is that nearly half (48%) of the organizations do not have specific guidelines and/or policies put into effect yet for responsible AI. Enterprises must, therefore, prioritize the adoption of a proactive and comprehensive approach to cybersecurity to safeguard their digital assets, protect sensitive information, and maintain the trust of their stakeholders.

On the other hand, MITRE ATT & CK and ATLAS offers valuable resources for understanding and mitigating threats specific to AI systems . If organizations map the LLM's security strategy to these frameworks, they can identify areas where existing security processes lack in addressing potential vulnerabilities.

The National Institute of Standards and Technology (NIST) has developed a classification and vocabulary for adversarial machine learning threats and countermeasures. This resource is intended for those involved in various aspects of AI, including design, development, deployment, evaluation, and governance. The classification system is structured across five key aspects: the type of AI system (Predictive or Generative),

the phase of the machine learning lifecycle where attacks take place, the objectives of the attacker, the capabilities of the attacker, and the attacker's knowledge of the learning process. The indispensable need for international and national standard setting organizations to establish a regulated regime for evaluation of the LLMs is therefore necessary to tackle the adversarial threats.

The need to use GenAI's capabilities varies across industries and domains. Therefore, it becomes crucial to understand the need of the AI tools amongst employees within the organization. Utilization of audits, surveys, and endpoint monitoring tools can help you access that need. You can then leverage use cases emerging out of this need to define the demand for the AI tools.

Furthermore, the rewards and risks associated with the usage require you to analyze each AI use case, meticulously weighing its benefits against potential security implications and privacy concerns. All while ensuring a balance between risks and advantages.

Formulating a governance framework is also crucial in the effective utilization of this not so new found technological faculty. Where you can work around policy compliance to ensure that AI practices strictly adhere to company policies and establish risk tolerance levels.

You can also create sandboxes for testing AI technologies and mitigating potential risks before real-time deployment. This will give you more room to experiment and exercise the necessary checks. Similarly, you can encourage supervised exploration of new AI use cases with controlled testing and rollout strategies to further keep things under control.

When you finally deploy the output, make sure to keep a vigilant eye in the process. Partner with CISOs, tech teams, and risk management experts to effectively classify data. Identify and isolate highly sensitive data, restricting access for AI tools.

At the end of the day, it's the controlled intervention and usage that decides the fate of any new area of development in the cyber landscape. More to this segment is entailed in depth in our report on 'MITIGATING SECURITY & PRIVACY RISKS: A Guide to Enterprise Use of Generative AI'. Where we also make you abreast with the applicability of data protection regulations and principles to GenAI. Along with an expanded understanding of cybersecurity risks and precautions at various hierarchical levels.

To read the entire report, visit: https://www.dsci.in/resource/content/mitigating-security-privacy-risks-guide-enterprise-use-generative-ai

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 AT THE WORKPLACE: A Practical Guide to Ethical Employee Data Management” by Shivangi Malhotra
- “PRIVACY BY DESIGN: Guidance on Practical Implementation for Businesses” by Shivangi Malhotra
- “Mitigating Security & Privacy Risks: A Guide to Enterprise Use of Generative AI” by Neha Mishra

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