



Unlocking opportunities
and navigating challenges:
the impact
of the Digital Personal Data
Protection Act on M&A

March 2024

About this report

[DATA PROTECTION]

Objective

- ▶ This report aims to provide an overview on the DPDP Act, 2023, encompassing the scope for India's DPDP applicability to various industries and sectors.
- ▶ It highlights the importance of adopting data privacy and the key factors organizations should consider regarding data privacy in M&A deals. As part of deal/transaction, EYP proposes the privacy due-diligence offering for a set of firms.
- ▶ The report also details out the need to combine technology due diligence and data due diligence in the M&A process to ensure a comprehensive understanding of the deal and a well-planned post-transaction roadmap.

Glossary

- DPDP Act:** Digital Personal Data Protection Act, 2023
- PDP Bill:** Personal Data Protection Bill
- GDPR:** General Data Protection Regulation
- ITAA:** Information Technology (Amendment) Act, 2022
- JPC:** Joint Parliamentary Committee
- MeitY:** Ministry of Electronics and Information Technology
- Board:** Data Protection Board of India
- Gol:** Government of India
- M&A:** Mergers and Acquisition
- PII:** Personal Identifiable Information
- SPD/SPI:** Sensitive personal data/information
- SPD/SPI includes:**



Biometric
information



Sexual
orientation



Financial
details



Security
information



Health
data

Source: Data captured from secondary research using news articles and Government publications



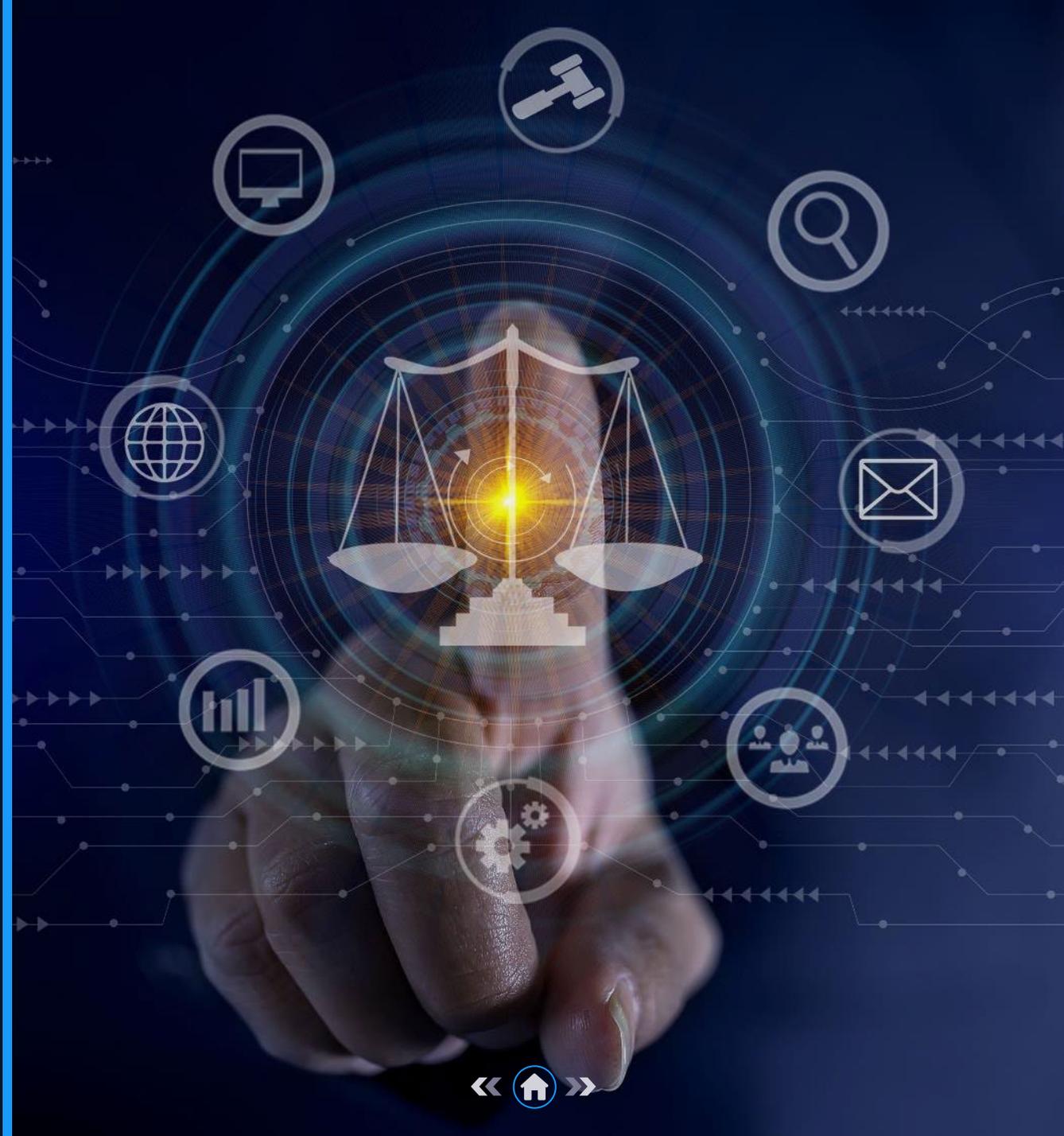
“

In the M&A process, it is critical that all parties involved must be prepared to provide adequate data privacy capabilities for the transaction to be successful. The Digital Personal Data Protection Act introduces the need to combine technology due diligence and data due diligence in the M&A process to ensure a comprehensive understanding of the deal and a well-planned post-transaction roadmap.



Santosh Tiwari

Partner, Strategy and Transactions,
EY LLP



contents

Table of

01

Executive
summary

02

Overview of
global and
Indian data
breaches

03

Introduction:
DPDP Act,
2023

04

Role of data
privacy in an
M&A
transaction

05

Impact of
the act on
Indian
businesses

06

EYP's data
protection
and privacy
offering

01

Executive summary



Executive summary

- ▶ The report covers the provisions of the new data protection act and highlights some key features
- ▶ It also highlights the expected transition period and penalties as covered in the DPDP Act, 2023



Current data privacy laws in India

Before the notification of the DPDP Act, India did not have a standalone law on data protection. Use of personal data was being regulated under the Information Technology (IT) Act, 2000, as amended from date to date along with the applicable rules and regulations. The notification of the certain Sections of the DPDP Act for their implementation is still awaited.



Financial penalties

The Act has stated to impose financial penalties of up to INR250 crores on data fiduciaries for non-compliance.



Relaxation in cross-border transfer of data norms

Section 16 of the DPDP Act allows the processing and transfer of Personal Data outside India, except to such countries restricted by Gol through notification.



Benefits and challenges of complying with the data protection law

The DPDP Act shares similarities with the GDPR law, contributing to improved data security, cybercrime prevention, enhanced customer engagement, and increased accountability. However, it also may pose challenges concerning compliance and maintenance costs.



Sectors handling sensitive data to invest heavily in compliance

Banks, technology, and energy sectors handle a significant amount of personal data, along with the increased risk to the rights of the Data Principal that may seemingly carry, potentially leading them to allocate higher expenditures to comply with data laws.



Significance of data privacy due diligence in an M&A transaction

The due diligence reports help the buyer to identify data risks associated with the target company and potential obstacles in operating the business post-integration.

02

Overview of global and Indian data breaches



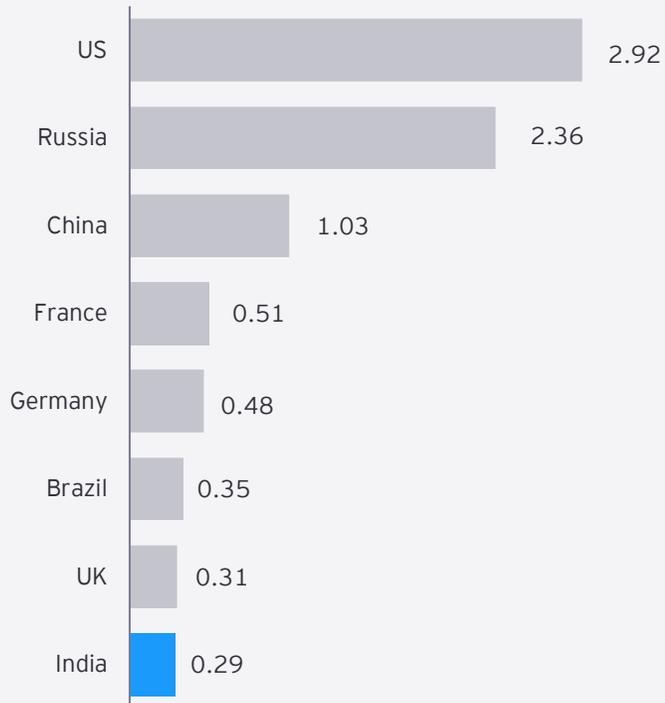
Globally, India holds the eighth position in both cumulative reported data breaches, as well as in the latest quarter of December 2023



Global reported data breaches

Top countries by number of reported data breaches*. Cumulative reported data breaches from 2004 to Dec 2023

(values in billions)



Source: [Surfshark](#)

*Data breach includes instances like personal data being copied, transmitted, viewed, or stolen from data holders, or being illegally used¹

Number of data breaches in India (by quarters)^{1,2}

India experienced a spike in data breach rates with a 116% increase in Dec'23 compared to the previous quarter, resulting in a negative shift in its rank. It shifted two ranks globally from 10th to 8th place in the latest Dec'23 quarter

Total data breaches (units in millions)



Source: [Surfshark](#)

- ▶ In the Dec'23 quarter, India has witnessed major data breaches with personally identifiable information (PII) leaked and sold on the dark web.
- ▶ With the **increase of digitization and data storing on the cloud platforms** in the post-covid period, the reported data breach count continued to increase for several quarters from Mar'20
- ▶ From Sep'20 to Sep'21, there were notable spikes in reported data breaches, **primarily due to substantial reported data breach incidents involving bigger brands**

India ranks **8th** in the latest Dec'23 quarter

Source: (1) [Surfshark](#), (2) Secondary sources and EYP analysis



03

Introduction: DPDP Act, 2023





Evolution of the Data Protection Act in India

2017 2018 2019 2020 2021 2022 2023

2017	2018	2019	2020	2021	2022	2023
<p>August</p> <ul style="list-style-type: none">▶ The supreme court of India announced the right to privacy as a fundamental right under the framework of the right to life (Article 21) as per the constitution¹▶ A committee was formed to examine the need for a data protection law in India and create a framework²	<p>July</p> <ul style="list-style-type: none">▶ The GoI published the draft PDP Bill, to strengthen the evolution of data protection law in India³	<p>December</p> <ul style="list-style-type: none">▶ MeitY Introduced the PDP Bill, 2019 in the Lok Sabha and the JPC was appointed to examine and provide suggestions related to the bill⁴	<p>November</p> <ul style="list-style-type: none">▶ The JPC suggested expanding the bill's scope with a focus on overall data protection that covers personal and non-personal data	<p>November</p> <ul style="list-style-type: none">▶ The JPC tabled the bill during the winter session of the Parliament with 81 amendments and 12 recommendations▶ The bill expanded the scope and changed its name to Data Protection Bill	<p>August</p> <ul style="list-style-type: none">▶ The PDP Bill, 2019 was withdrawn by the central government. The withdrawal aims to build a complete legal framework on the digital ecosystem⁵ <p>November</p> <ul style="list-style-type: none">▶ The MeitY released a draft of the DPDP Bill, 2022 for public consultations⁶	<p>March</p> <ul style="list-style-type: none">▶ The MeitY has received approval for the draft bill from the Parliamentary Standing Committee⁷ <p>April</p> <ul style="list-style-type: none">▶ The MeitY presented the draft bill in parliament's monsoon session for approval <p>August</p> <ul style="list-style-type: none">▶ The Act has been passed by the Parliament⁷

Source: (1) [MeitY - Data Protection in India](#), (2) [MyGov](#), (3) [The Personal Data Protection Bill, 2018](#), (4) [PIB](#), (5) [Explanatory note - DPDP Bill](#), (6) [Inviting feedback on the draft bill](#), (7) [DPDP Bill, 2023](#)

The Act governs the collection and processing of digital personal data, excluding any provisions related to non-personal data, which was covered in the PDP bill, 2019



Overview of the DPDP Act, 2023^{1,2,3}

- ▶ The DPDP Act was released in November 2022 by the MeitY, aiming to implement a robust regime for data privacy. The Act has been passed by the Parliament, and the implementation and roll-out of the Act are expected soon.
- ▶ **Purpose:** The Act to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.
- ▶ **Date of commencement:** The Act shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint. Different dates may be appointed for different provisions of this Act. Any reference in any provision of this Act to the commencement of this Act shall be construed as a reference to the commencement of that provision.
- ▶ The central government is expected to set up a **Data Protection Board (DPB)**, which shall function as an independent body to **govern non-compliance** with the act's provisions

Industry players would be given a **transition period** of

<2 years

MeitY plans to **first implement the Act on big tech companies** offering a shorter timeframe, whereas start-ups will be given more time to comply^{4*}

Key roles as mentioned in the DPDP Act, 2023³



Data Principal

The individual to whom the personal data relates and where such an individual is a child, the parent or lawful guardians will be considered the data principals



Data Fiduciary

- ▶ Any person alone or in conjunction with other persons determines the purpose and means of the processing of the personal data
- ▶ **Significant Data Fiduciary: Any data fiduciary or class of data fiduciaries, as may be notified by the GoI that deals with a high volume of data.**



Data Processor

- ▶ Any person who processes personal data on behalf of a Data Fiduciary
- ▶ Data Processor (along with the Data Fiduciary) is expected to protect the personal data under its control by adopting rational security safeguards to prevent data breaches



Data Protection Officer (DPO)

An individual appointed as such by a Significant Data Fiduciary under the provisions of this Act

*Transition period is not explicitly stated in the DPDP Act, 2023, but was announced in an interview of a senior official from MeitY

Note: The roles are covered as defined in the act

Source: (1) [INDIAai article 1](#), (2) [INDIAai article 2](#), (3) [The Digital Personal Data Protection Act, 2023](#), (4) [Deccan Herald](#)



The Act applies to the processing of digital personal data collected online or offline and then digitized, with several exemptions included as well



Who is impacted by the act?¹

- ▶ Any entity involved in the collection and processing of digital personal data **within the territory of India** from Data Principals (user) through:
 - ▶ Digital form
 - ▶ Non-digital form (digitised subsequently)
- ▶ Any entity that deals in the processing of digital personal data **outside the territory of India**, related to:
 - ▶ Activity of **offering goods or services** to Data Principals within India



Who is exempted from the act?¹

The central government is exempted from the processing of personal data used for:

- ▶ Sovereignty and integrity of India, **security of the State**, friendly relations with foreign states, maintenance of public order
- ▶ **Research**, archiving, or statistical purposes

Section 17(1), exempts entities from provisions of this Act, where the processing of personal data is:

- ▶ Necessary for enforcing any legal right or claim
- ▶ Necessary for the performance of any judicial function by any court
- ▶ In the interest of prevention, detection, investigation, or prosecution of any offense or contravention of any law
- ▶ In pursuant to any contract entered with any person outside India by any person based in India
- ▶ Pursuant to any order by a competent authority for compromise or arrangement or merger or acquisition or demerger or reconstruction
- ▶ Pursuant to any default to any default in repayment of loan/advance from any financial institution

The central government can exempt several Data Fiduciaries on:

- ▶ Volume and sensitivity of personal data processed
- ▶ Risk to the rights of the Data Principal
- ▶ Impact on sovereignty and integrity of India, risk to electoral democracy
- ▶ Security of the state or public order

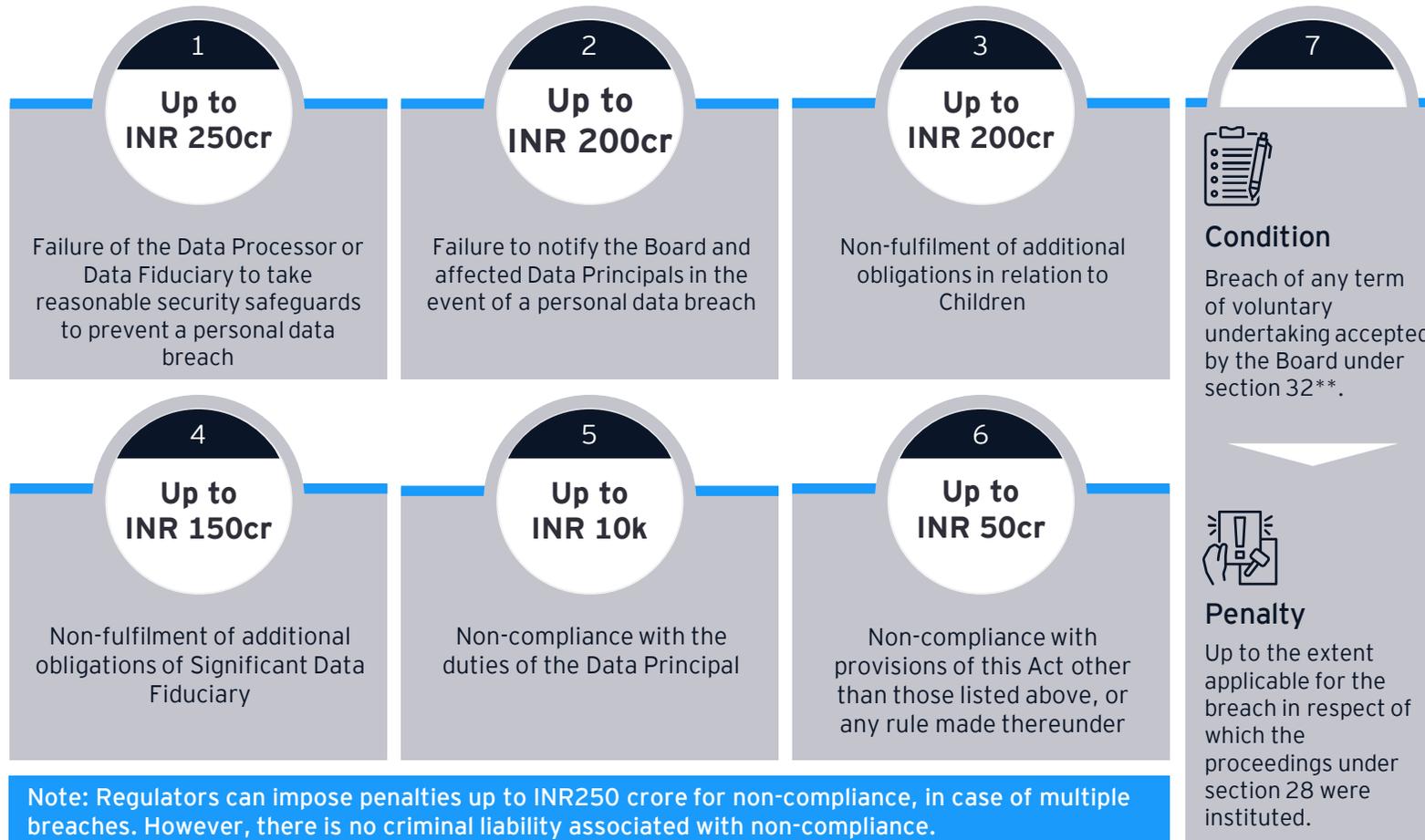
Source: (1) [The Digital Personal Data Protection Act, 2023](#)



Data Fiduciaries may be penalized over failure to comply with the Act and fined up to INR250 crore



Penal provisions under the DPDP Act¹



Note: Regulators can impose penalties up to INR250 crore for non-compliance, in case of multiple breaches. However, there is no criminal liability associated with non-compliance.

Obligations of Data Fiduciary¹

- ▶ **Seek consent:** Data Fiduciaries must provide users a notice describing the purpose of collecting personal data. The consent given by the Data Principals must be freely given and specific to the Data Principal's agreement.
- ▶ **Withdrawal of consent:** Data principals hold the right to withdraw consent at any time.
- ▶ **No conditional services:** A contract between the Data Fiduciary and the user to deliver a product cannot be made conditional on the consent to the processing of any Personal Data.
- ▶ **Accuracy of data:** Data Fiduciaries are expected to adopt reasonable efforts and ensure that the personal data processed is accurate and complete.
- ▶ **Notifying data breaches:** The Data Protection Board and the concerned Data Principals must be notified in case of a personal data breach.
- ▶ **Retention of personal data:** A Data Fiduciary must cease to retain personal data, in case the purpose for which such personal data was collected is no longer being served by its retention.
- ▶ **Appoint a DPO:** Data Fiduciaries must publish the business contact information of a DPO to answer on behalf of the Data Fiduciary.
- ▶ **Grievance redressal mechanism:** Data Fiduciaries must have a procedure and effective mechanism to redress the grievances of Data Principals.

*Section 28: Procedure to be followed by the Board | **Section 32: Voluntary undertaking by the Board
Source: (1) [The Digital Personal Data Protection Act, 2023](#)



04

Role of data privacy in an M&A transaction

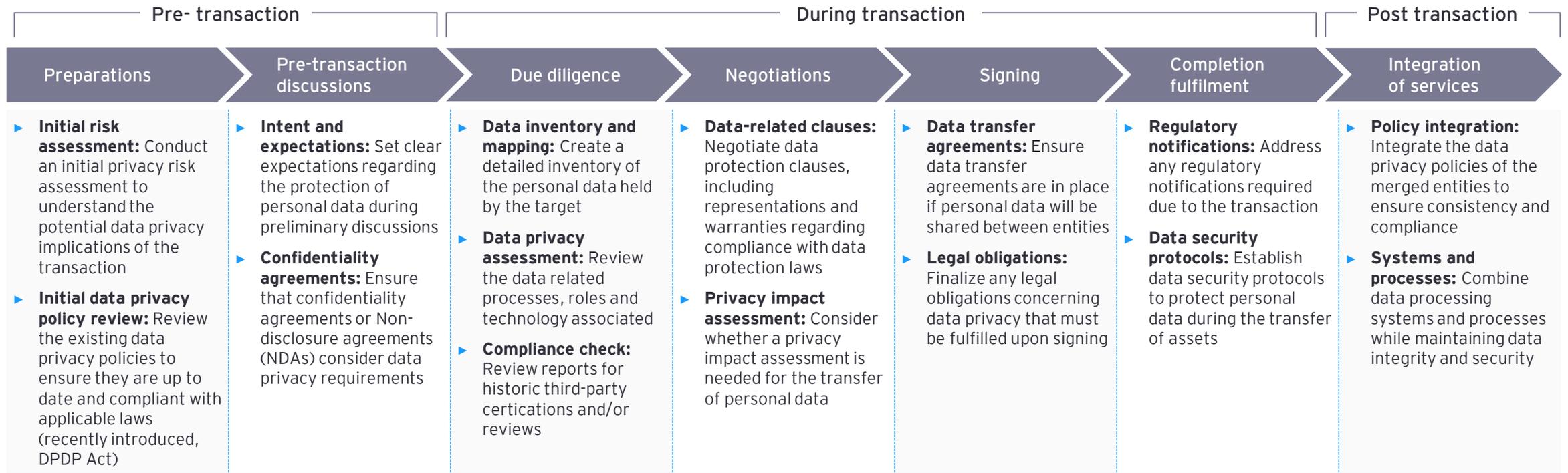


The data privacy practices of the target company are assessed in the due diligence phase, and integrated in the post-transaction phase



- ▶ In recent years, data privacy considerations in M&A transactions have seen a significant surge due to increasingly stringent regulations, heightened public awareness, and the pivotal role that data plays in the deal valuation and integration processes
- ▶ In the due diligence stage, the buyer assesses the data protection practices of the target company to ascertain its compliance with regional laws. During the integration stage, the buyer evaluates the policies concerning the processing of personal data

Data privacy considerations throughout an M&A transactions timeline¹



Source: (1) EYP analysis



EYP offers tailored services to tackle data privacy related challenges faced by clients, across the M&A transaction lifecycle



Common client concerns around data privacy in an M&A transaction¹



How will M&A deal affect compliance with data privacy laws?

- ▶ The companies involved in the M&A transaction are expected to diligently handle customer data during the merger.
- ▶ In case of non-compliance with the data privacy laws, the companies can face various legal issues



Could the buyer inherit any hidden data privacy liabilities?

- ▶ Buyers/acquirers aim to avoid inheriting any data breach or hidden compliance issues.
- ▶ Therefore, they express concerns during the due diligence stage and seek to ensure that the target's data practices align with the required standards



What is the plan for aligning the buyer-target data privacy policies post-merger?

- ▶ The buyer may encounter challenges in integrating their data systems post-merger and should focus on any gaps in privacy protection policies to avoid compliance issues and maintain customer trust

EYP addresses common data privacy challenges around compliance risks, inheriting privacy liabilities, and aligning data policies in M&A deals through its comprehensive service offerings

Common Data Privacy challenges

- ▶ Potential exposure of sensitive data due to incompatible security protocols and systems driven by disparate technology solutions
- ▶ Gaps in data mapping across different systems leading to a loss of data governance, leading to non-compliance with privacy regulations
- ▶ Legacy systems with outdated security causing increased vulnerability to data breaches due to outdated security measures in legacy systems
- ▶ Data loss or breaches during the physical and digital consolidation of data centers
- ▶ Conflicts between the compliance standards of merging entities can lead to regulatory penalties
- ▶ Data Transfer and Sovereignty Issues due to legal restrictions on cross-border data transfers can disrupt business operations

Services offered by EYP

- ▶ Conduct a thorough assessment of both entities' technologies and implement a secure integration plan that prioritizes data protection
- ▶ Utilize data mapping tools to fully understand the data flow and ensure compliance with data governance standards during and post the transaction
- ▶ Plan for a gradual phase-out of legacy systems or update the security features to meet current standards
- ▶ Develop a data consolidation strategy that includes robust data protection measures and a clear data migration protocol
- ▶ Harmonize data privacy policies to meet the highest compliance standards applicable to the merged entity
- ▶ Review the compliance to data sovereignty laws in all relevant jurisdictions and structure the transaction to ensure lawful data transfer

Source: (1) EYP analysis



EYP assists large cap, middle market organizations, and private equity funds in conducting due diligence to assess the risks associated with the target company



During transaction stage - Due diligence outcome¹

- ▶ The purpose of conducting due diligence is to identify risks associated with the target company and potential obstacles in operating the business post-completion
- ▶ The following are the key steps taken to enable the buyer to evaluate the target company's data privacy and security practices:

	Gain an understanding of the target company's business model		Examine the measures taken by the target company to adhere to relevant privacy laws
	Understand the flow of personal information, considering both online and offline data collection		Evaluate all third parties with access to the personal information collected by the target company
	Assess the privacy policies of the target company		Comprehend the background of data breaches and security incidents
	Determine the presence and effectiveness of information security policies and procedures		Value at risk to assess the possible losses over a specific time frame which would impact the Sale and Purchase Agreement

Post-transaction stage - Integration of services

- ▶ The buyer should be engaged in a discussion to explore potential changes to the target's business model and assess how these changes could impact personal data processing
- ▶ The possibility of using the target's data to promote the services of the acquired company will be considered, and this action may necessitate obtaining consent from individuals

Source: (1) EYP analysis



Organizations are expected to adopt steps like mapping data sources, storing limited data, and applying data security measures to comply with the DPDP Act



Steps to get started with the DPDP Act, 2023^{1,2,3}



Note: The above process has been observed by the companies while complying with the GDPR law. We assume a similar process to be followed by companies that adhere to the DPDP act, considering its similarities with the GDPR.
Source: (1) [The Digital Personal Data Protection Act, 2023](#), (2) [GDPR law](#), (3) EYP analysis



GoI to provide a transition period to comply with the new regime and improve their data protection, prevent cybercrimes, and enhance customer engagement



Current data privacy laws and regulations in India:

- ▶ ITAA, 2008, further revised to ITAA 2022
- ▶ IT Rules, 2011
- ▶ CERT-in Directives, 2022



The DPDP Act, 2023

- ▶ The draft was released in November 2022 and has been passed by the Parliament, and the implementation and roll-out of the Act are expected in the near future

EYP's POV on the DPDP Act, 2023^{2,3,4}



Organizations are expected to be provided a **transition period of less than two years to comply** with the new Act, with initial implementation focusing on **big tech companies with a shorter timeline and start-ups to be given a larger transition time.**



Road to Compliance

Companies are encouraged to utilize the transition phase to comply with the bill, which will aid in **improving their data protection, prevent cybercrimes, and enhance customer engagement and overall goodwill**



Failure to comply

- ▶ In case of non-compliance, organizations could **potentially incur substantial fines of up to INR250 crore**
- ▶ Organizations that experience **severe data breaches** or mishandle the data may lose **customers' trust and encounter challenges in attracting new partners**



GRIEVANCE REDRESSAL

The Act mandates large corporations to appoint a DPO to function as a point of contact for redressing any grievances that may arise



- ▶ The Digital Personal Data Protection Act requires companies to obtain consent from individuals before collecting and processing their personal data. This is a significant step towards protecting privacy in India, by giving individuals more control over their personal data.
- ▶ In the M&A process, adequate data privacy measures are essential for transactions to be successful. The DPDP Act introduces the need to combine technology due diligence and data due diligence in the M&A process to ensure a comprehensive understanding of the deal and a well-planned post-transaction roadmap.

Transaction Strategy and Execution's (TSE) Data Protection and Privacy (DPP) offering can help the organization to transform the companies from a greenfield to a more mature data privacy compliant stage.

Source: (1) [INDIAai](#), (2) [The Digital Personal Data Protection Act, 2023](#), (4) [Deccan Herald](#), (4) EYP analysis



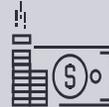
05

Impact of the act on Indian businesses



With the introduction of the DPDP Act, the companies are expected to benefit from compliance with the act. However, it may come with certain challenges



Positive impact ^{1,3}	Non-compliance impact ^{2,3}	Negative impact ³
 <p>Enhanced data protection The Act is expected to significantly strengthen privacy by establishing strict guidelines for organizations to collect, store, and process personal data</p>	 <p>Financial penalties In case of non-compliance with the act, companies, and organizations are expected to face hefty penalties of up to INR250 crore</p>	 <p>Compliance costs Enterprises often face financial challenges when implementing the necessary measures to safeguard data protection and privacy</p>
 <p>Prevents cybercrimes By implementing robust data protection measures, the organization ensures the protection of customers' personal data along with their organization's data</p>	 <p>Reputation harm Organizations that experience severe data breaches or mishandle the data will face customer attrition and encounter challenges in attracting new partners</p>	 <p>Operational complexity Organizations with limited legal expertise or IT infrastructure may find the complexity overwhelming</p>
 <p>Increase customer engagement Individuals are increasingly aware of the right to the protection of their personal data and mismanagement of personal data can quickly damage the public reputation</p>		 <p>Impact on small businesses Complying with the requirements can be especially challenging for small businesses, as they often lack the resources and expertise of larger enterprises</p>
 <p>Increased accountability Organizations are required to keep comprehensive records of their data processing activities to ensure accountability for their handling of data</p>		 <p>Multiple compliance challenges for global companies Organizations outside India may be subject to DPDP regulations and achieving global compliance with DPDP and other laws can be complex and resource-intensive</p>

Note: The above impacts have been observed by the companies while complying with the GDPR law. We anticipate a similar outcome for companies that adhere to the DPDP Act, considering its similarities with the GDPR.

Source: (1) [European Data Protection Board](#), (2) [The Digital Personal Data Protection Act, 2023](#), (3) EYP analysis



Various critical industries handling sensitive user data are adopting data privacy measures to avoid data breaches and safeguard user data



Critical industries investing in data privacy to avoid data breaches

- ▶ Data breaches can happen to organizations of any size across every industry and can affect the financial health and longevity of the business
- ▶ Various companies are investing significantly in data privacy measures, to manage the sensitive data they collect and the complexity of their data-processing activities

Critical industries



Banks allocate the significant investments in data protection due to the risk of cybercriminals gaining direct access to financial information through breaches, which can be exploited in various detrimental ways



Technology and telecom companies invest significantly in data protection, due to the substantial data they collect and the complexity of their data-processing activities



Healthcare organizations have allocated relatively limited resources for data protection law, as the industry often faces tight budgets and relies on outdated technology



The **Government** invests in data protection solutions to safeguard their critical information and to enhance data protection, it has introduced Digital Personal Data Protection Act, 2023



The **energy sector** incurs significant expenses due to its management of sensitive data, including customer information, designs, documentation for capital engineering projects, and resource location maps

[More details ahead on the critical industries](#) >>

Source: (1) Secondary research and EYP analysis



With the Act into force, historical users' data will undergo data validations and limitations, while impacting technology and compliance upgradation



Cause and impact on the banking sector



CAUSE

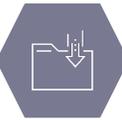
- ▶ The banks* software systems process a significant amount of PII and SPI
- ▶ There is an increase in the processing and storing of data with the rising adoption of automation and digitization of lending processes, credit profiling, and customer procedures
- ▶ For e.g. Various banks store SPI to offer auto-fill to their users, AutoPay services save the UPI data, and eKYC holds SPD wherein verification can be done through Aadhaar or offline



- IMPACTS**
- ▶ The DPDP Act annotates the privacy of the information stored by the processing of the above-said processors



- ▶ The data processors are bound to classify, and rearchitect the software systems, and processes and adhere to compliance in terms of consent recording, data storage, and data reusability



- ▶ Historical data for record processes and retention will undergo extensive validations, limitations, and restrictions for reusability
- ▶ This will have an impact on technology and compliance upgradation

RBI and SEBI continue to govern the banking sector data^{1,2}

- ▶ Even with the introduction of the DPDP Act, 2023, the Reserve Bank of India continues to mandate the banking industry players on the localization of payment, card, and personal data storage
- ▶ SEBI mandates that regulated entities (REs) storing or processing data or information in the cloud must ensure it is located within the borders of India

*Banks: Public Sector Undertakings, private banks, Non-Banking Financial Companies, Asset reconstruction companies, and digital lending platforms
Source: (1) [Reserve Bank of India](#), (2) [SEBI](#), (3) Secondary sources and EYP analysis



The technology sector has benefited from the positive impact of relaxed cross-border data flow, limited focus on personal data, and the launch of consent management



Impact on the Technology sector^{1,2}



KEY PROS



KEY CONS



Relaxed the rules for cross-border data flow and limited several clauses around data mirroring and localization

01

Sectors like edtech and gaming are significantly impacted by the mandate to obtain explicit consent for children below 18 years of age

01

The focus is limited to safeguarding personal data which allows the companies to focus more on personal data. It has simplified data processing for foreign businesses operating in India.

02

Significant controls and exemptions to the government may hinder companies' investments in data centers and data processing activities in India

02

The introduction of consent management will provide organizations with a platform to communicate to users the intended use and governance of their data

03

The removal of criminal liabilities and fines tied to the entity's turnover for non-compliance could lead to companies becoming less concerned about adhering to the act's requirements

03

Cause and impact

CAUSE

Cross-border data transfer and similar scenarios for a copy of data retention (for record purposes) outside stored in India brings a risk likelihood

IMPACT

- ▶ The data retention and reusability timeline for the purposes requires to be reviewed business case-wise.
- ▶ For example, a social media platform storing the PII use cases and re-used for analytics purposes for another entity outside India, its jurisdictions are likely.

Source: (1) [The Digital Personal Data Protection Act, 2023](#), (2) EYP analysis



Sensitive healthcare data processing makes this sector critical, but concerns arise over government exemptions for processing personal health information



Data privacy in the healthcare sector

Healthcare is considered one of the critical industries and health records like ePHI, Electronic Health Records (EHR), or patient information implies multi-dimensional data risks

Existing digital health data laws in India²

- ▶ The GoI introduced DISHA in 2018 to ensure data privacy, confidentiality, reliability and security of digital health data.
- ▶ The existing legal framework governing e-health protection in India is also governed by the IT Act, 2000, and the SPDI Rules, 2011.

Electronic protected health information (ePHI)

	Patient demographics		Blood pressure
	Height		Laboratory tests
	Weight		Medications

Concern received from the healthcare industry¹

 The GoI processes vast amounts of personal health data (on platforms like CoWIN, Arogya Setu, and Ayushman Bharat Digital Mission) creating a need for data management and protection rules for government agencies.

 Private healthcare providers may share patients' personal data with the GoI for various reasons like public health purposes, government healthcare initiatives, research, and compliance with legal or regulatory requirements

Source: (1) [National Library of Medicine](#), (2) [PIB](#), (2) EYP analysis

The increase in digital patient data has created a need to integrate the data governance platform with IoT infrastructure systems



Cause and impact on the healthcare sector^{1,2,3}

CAUSE



The automated healthcare systems and cross-border data transfer of critical health information signify a sizeable amount of data processed in the IoT healthcare systems and their communication systems



The involvement of Health care BPO and ITeS in data handling and processing

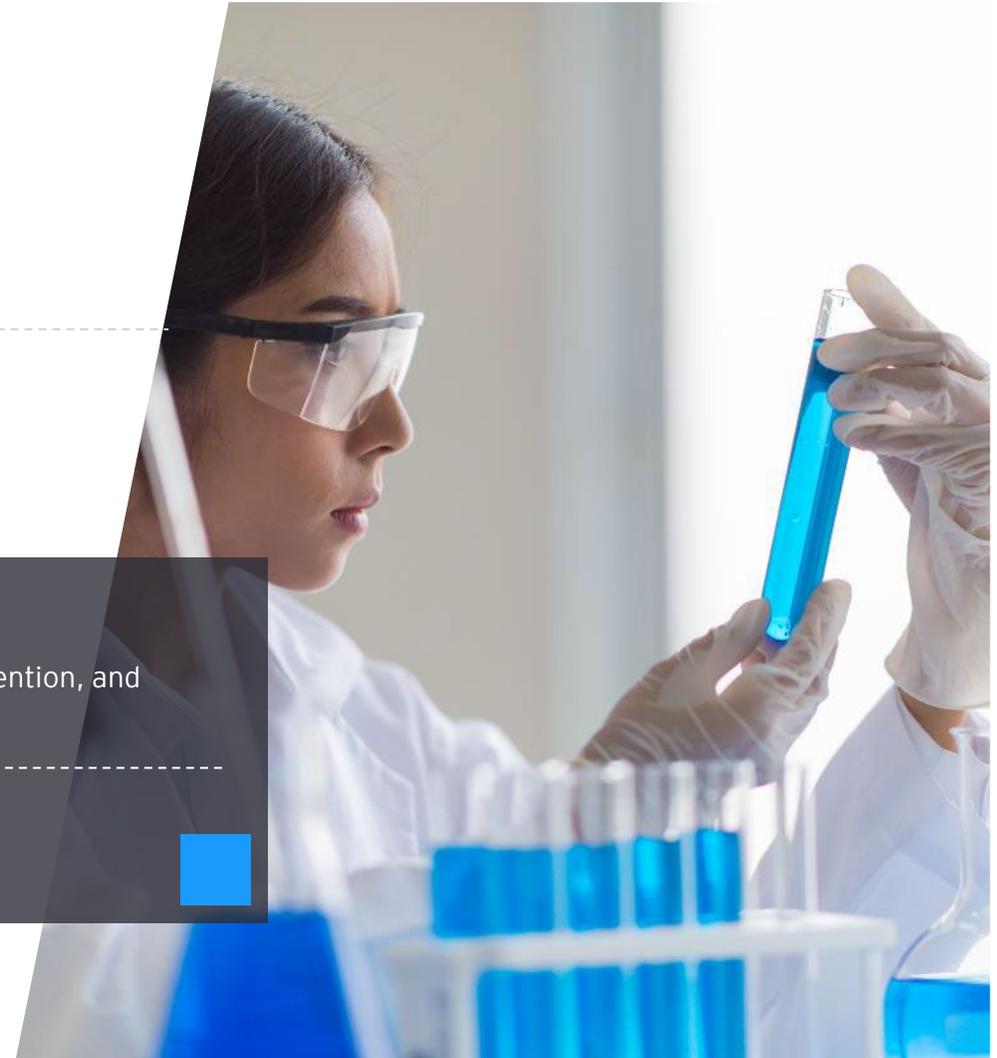
IMPACTS



The need for a complaint suite to duly engage the adequate data guidance for storage, retention, and processing. For instance, Record of Processing Activities (RoPA)



Integration of the Data governance platform with the IoT infrastructure systems is a must



Source: (1) [National Library of Medicine](#), (2) [inteq solutions](#), (3) EYP analysis

The Act is expected to disclose government agencies' exemption details and may consider regulating entities supporting the Government in processing SPD



Cause and Impact on the Government and Public Sector Undertakings (PSU)^{1,2}



CAUSE

The Act does not cover the details on the exemptions for the government agencies to process the citizen data (includes Aadhaar Card Data, Voter ID Information, PAN Card Data and other personal information) is not evident

IMPACTS



The Act could consider governing the sub-processors which are the supporting entities of the government in terms of IT service providers supporting the citizens' services and exposure to production data



The Act is expected to evaluate business impact analysis, privacy impact, and possible data threat scenarios

Source: (1) [The Digital Personal Data Protection Act, 2023](#), (2) EYP analysis



The Govt intends to provide certain exemptions for early-stage start-ups to assist them in developing their business models



Cause and impact on the start-ups

CAUSE



Like other industries, start-ups are expected to implement similar data privacy measures such as seeking consent before data use, utilizing minimal data, using data only for its intended purpose, and storing data only for a fixed period



Start-ups may need to invest in new technologies and processes to ensure secure personal data handling and enhance transparency in data collection and usage

IMPACTS



The government plans to exempt early-stage start-ups from certain penalty provisions proposed under the DPDP Act, 2023



The exemption would be limited to assisting start-ups in developing their business models. This would ensure that innovation is not suppressed due to compliance burden

The revised Act has exempted Indian government agencies from processing and collecting personal data. This could trigger other countries to ignore Indian start-ups like the Chinese companies that are barred by many nations

Source: (1) Secondary sources and EYP analysis



06

EYP's data protection and privacy offering



EYP offers a framework to understand the current DPP landscape, identify the improvement areas, and define the strategy and the remediation plan



What does Transaction Strategy and Execution (TSE) Data Protection and Privacy (DPP) offering entail?

- ▶ TSE DPP service offering will seamlessly enable the Data protection and privacy requirements for the client organizations towards its continuously changing data management landscape.
- ▶ The data governance initiative will meet the increasing requirements of regulators, clients, and employees.
- ▶ EY TSE DPP team will assess the organization's data protection and privacy maturity in line with its ambitions, identifying possible (compliance) gaps and embedding DPP in organizational practices.
- ▶ EY TSE DPP will help the clients to understand and overcome the data concerns regarding business processes. Also, it enables suitable business accelerators to generate value from data while taking appropriate care of privacy principles.

Services and solutions offered under the DPP

DPP Strategy, Governance Initiative, and Transformation

We assess, design, and help you mature your data protection and privacy program. The core activities/outcome includes:

- ▶ Design of Data Protection Privacy Strategy and roadmap
- ▶ Data Protection and Privacy Advisory and Implementation
- ▶ Data Ethics and Trusted AI design
- ▶ Data Privacy Risk Assessments
- ▶ Metrics and Dashboarding design

DPP Compliance

We help you achieve alignment with laws and standards linked to data protection and privacy in the areas:

- ▶ Data classification services
- ▶ Information Protection Assessment for Regulatory Compliance
- ▶ Implementation of Privacy Control Framework
- ▶ Privacy Impact Assessment
- ▶ Third-Party Vendor Risk Management
- ▶ Data breach support

DPP Technology Enablement

We support you to leverage suitable technical capability to enable your desired business outcomes by means of:

- ▶ Data Discovery
- ▶ Crown Jewel Assessment
- ▶ Data Access Monitoring
- ▶ Encryption and Classification
- ▶ Efficient tracking of specific business processes and applications and the ability to showcase consent records of data subjects

DPP Awareness

We help to establish organizational awareness through training, and workshops based on:

- ▶ Data-centric operating model Governance and accountability
- ▶ Measurement of Security culture and adherence
- ▶ Data Protection and Privacy Awareness Program
- ▶ Data Protection and Privacy Training Content and Delivery



Data privacy for technology services company operates in the EU, the US and western Asia



EYP client story

Background

The target company was a technology and digital services transformation company operating in multiple countries in EU member states, the US, and Asia. The target company has a large clientele in finance, manufacturing, transportation, media, entertainment, and education portfolio

Objective

- ▶ To perform a desk-based assessment of the data privacy
- ▶ To assess the maturity of the organization in terms of compliance with the data laws in the respective country/jurisdiction
- ▶ To study the data privacy enablement as per regulatory requirements and international standards
- ▶ To assess for any potential data breaches involved, the percentage involving personally identifiable information and account holders affected reported

EY Point of View

- ▶ The organization is predominantly in service operations, and having its global footprint requires building strong and collaborative data protection methods for its business and enterprise data.
- ▶ The organization's skill gap in terms of technology, people, and data management (esp. personal data) could lead to a possible data risk.
- ▶ The organization may fulfill its privacy compliance needs by regularly performing the data privacy assessment.

Value Delivered

- 1 Mapping the regulatory requirements, and scope applicable for data inventory, risk likelihood scenarios of privacy noncompliance is adequately determined
- 2 Identified non-compliances in consent management and usage of customer data for secondary purposes
- 3 Identified non-compliances in consent management and usage of customer data for secondary purposes

Frameworks Used

- ▶ EYP-tailored 12-domain DPP framework
- ▶ Broad adoption of GDPR, EU member state regulatory guidelines, ISO, and bill amendment thereof



Disclaimer

The information contained in this report has been obtained majorly from government sources and other sources that are believed to be reliable, but EYP does not represent that this information is accurate or complete.

The information provided in the report is for information purposes only. The report should not be considered a substitute for professional advice and is not intended to be relied upon as the sole basis for any decision that may impact any business.

The report is built as per EYP's understanding and interpretation of the DPDP Act, 2023 which reflects our analysis and views on the Act and its potential impact, thereof.

EYP, its partners, authors and its other entities shall not be responsible/liable for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof.

The material in this publication is copyrighted. No part of this report can be reproduced either on paper or electronic media without permission in writing from EYP. Request for permission to reproduce any part of the report may be sent to EYP.



Ernst & Young LLP

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

About EY-Parthenon

EY-Parthenon teams work with clients to navigate complexity by helping them to reimagine their eco-systems, reshape their portfolios and reinvent themselves for a better future. With global connectivity and scale, EY-Parthenon teams focus on Strategy Realized – helping CEOs design and deliver strategies to better manage challenges while maximizing opportunities as they look to transform their businesses. From idea to implementation, EY-Parthenon teams help organizations to build a better working world by fostering long-term value. EY-Parthenon is a brand under which a number of EY member firms across the globe provide strategy consulting services. For more information, please visit ey.com/parthenon.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at Ground Floor, Plot No. 67, Institutional Area, Sector - 44, Gurugram - 122003, Haryana, India

© 2024 Ernst & Young LLP. Published in India.
All Rights Reserved.

EYIN2403-027
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ey.com/en_in

 @EY_India  EY  YouTube EY India  EY Careers India  @ey_indiacareers

Contacts



Santosh Tiwari

Partner, Strategy and Transactions
EY LLP
santosh.tiwari2@parthenon.ey.com



Karthik Ramakrishnan

Director, Strategy and Transactions
EY LLP
karthik.ramakrishnan1@parthenon.ey.com



Kamal Suri

Associate Director, Strategy and
Transactions Research
kamal.suri@in.ey.com



Deepali Sharma

Manager
Strategy and Transactions Research
deepali.sharma@in.ey.com



Viren Kavil

Senior Associate
Strategy and Transactions Research
viren.kavil@in.ey.com

