

Data Audit – Opportunity under DPDP Act 2023

Understanding the Digital Personal Data Protection Act (DPDP Act) & Its Implications

Disclaimer

Data shared, discussed , exchanged etc during the session by participants or by speaker is only for academic purpose.

Overview of the DPDP Act 2023



Safeguarding Data & Lawful Processing



Transformative Framework: The Digital Personal Data Protection (DPDP) Act, 2023, marks a significant shift in India's approach to data regulation, establishing new benchmarks for handling, storing, and processing personal information nationwide.

Core Principles: At its foundation, the Act mandates collecting only essential data, utilizing it for clearly defined purposes, and always securing explicit **consent-driven** user consent. This empowers individuals with greater control over their digital footprint.



Global Alignment & Cross-Border Data



Extra-Territorial Reach: The DPDP Act extends its applicability beyond Indian entities, covering foreign organizations that offer goods or services to data principals in India. This aligns India with **global standards** like GDPR.

Regulated Data Transfers: The Act provides a framework for **cross-border transfers**, stipulating that personal data can be transferred abroad only in adherence to conditions set by the government, ensuring controlled and secure international data flows.

Key Definitions Under the DPDP Act

{ } Data & Digital Personal Data

'**Data**' broadly refers to any representation of information, facts, concepts, or instructions.

'**Digital Personal Data**' specifically refers to personal data that exists in digital form, processed and stored electronically.

This distinction emphasizes the Act's focus on information handled in the digital realm.

Digital Format

Information



👤 Personal Data: Identifiable Individual

'**Personal Data**' is defined as any data about an individual who is identifiable by or in relation to such data.

This includes information that can directly or indirectly pinpoint a specific person, making individual identity central to protection.

Identifiable

Individual-Centric



👥 Key Roles & Responsibilities

Data Principal: The individual whose personal data is being processed; the rights holder.

Data Fiduciary: Determines the purpose and means of processing; responsible for compliance.

Data Processor: Processes personal data on behalf of a Data Fiduciary.

Accountability

Consent Flow



🛡️ Personal Data Breach (CIA)

A '**Personal Data Breach**' is any unauthorized processing or accidental disclosure, acquisition, alteration, destruction, or loss of access to personal data.

This compromises the **Confidentiality, Integrity, or Availability** (CIA) of the personal data.



Personal Data Breach

Digital Personal Data Protection Act, 2023 (India)

Key Provisions and Implications for Data Fiduciaries



Definition (Section 2(u))

Any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access that compromises its confidentiality, integrity, or availability.



Data Fiduciary Obligations (Section 8(6))

Mandatory intimation of a breach to the Data Protection Board of India and each affected Data Principal, in such form and manner as may be prescribed.



Role of Data Protection Board

(Section 27(1)(a))

Upon receiving intimation, the Board can direct urgent remedial measures, inquire into the breach, and impose penalties.



Significant Penalties (Schedule)

- Up to **₹250 Crore** for failure to take reasonable security safeguards (Sec 8(5)).
- Up to **₹200 Crore** for failure to notify the Board/Data Principals (Sec 8(6)).

Data Diversion: A Digital Fraud

Treating Unauthorized Data Use and Manipulation as a Critical Cyber Threat

- **Definition of Data Diversion:** Unauthorized acquisition, alteration, or use of digital information for purposes other than those sanctioned. This includes unauthorized access, processing, and sharing of data.
- **Analogous to Funds Diversion:** Just as financial diversion constitutes fraud, data diversion represents a severe form of digital fraud, undermining trust and operational integrity.
- **Scope of Misconduct:** Encompasses data used for unapproved or illegal activities, data shared or processed without explicit authorization, and data leveraged for purposes not originally consented to.
- **The Role of Data Leakage:** Data leakage, whether intentional or accidental, often serves as a precursor or direct component of data diversion, exposing sensitive information to unauthorized parties.
- **Technology-Driven Implications:** Leverages sophisticated cyber techniques for illicit data manipulation, requiring advanced forensic and security protocols for detection and prevention. Legal frameworks are rapidly evolving to classify and prosecute these digital offenses.

Applicability and Non-Applicability of the Act

✂ Applicability Scope

🏠 Within India



- The DPDP Act, 2023, governs the processing of **digital personal data** within India.
- This includes data collected in digital form and subsequently **digitized from non- digital form**

Domestic Reach

Digital Focus

🛡 Non-Applicability & Exemptions

🏠 Exclusions from the Act



- The Act does not apply to data processed for **personal or domestic purposes**
- It also excludes **publicly available** data made by the Data Principal or under a legal obligation.

Private Use

Public Domain

🌐 Extra-Territorial Reach



🔍 Specific Exemptions



Understanding the Digital Personal Data Protection Act (DPDP Act), 2023

A Legislative Landmark & Core Objectives

The DPDP Act, 2023, is a pivotal milestone, marking India's first dedicated federal law to safeguard personal data and strengthen its commitment to a citizen-centric data governance framework.



Core Objectives:

- **Protect Personal Data:** Ensure security and privacy of individuals' digital data.
- **Foster Trust:** Build confidence in the digital economy via transparent practices.
- **Ensure Accountability:** Establish clear responsibilities and compliance mechanisms.

Applicability & Scope: A Wide Reach

Governing the processing of digital personal data, the Act's extensive reach includes:

- **Jurisdictional Clarity:** Applies to all digital personal data

Key Entities Under the DPDP Act



Data Principal

The individual to whom the personal data relates. (Sec 2(j))



Data Fiduciary

Any person who determines the purpose and means of processing personal data. (Sec 2(i))



Data Processor

Any person who processes personal data on behalf of a Data Fiduciary. (Sec 2(k))

Evolution of Data Protection in India



IT Act, 2000

Initial framework with limited data protection scope.



2011: SPDI Rules

Core Obligations of Data Fiduciaries: Processing & Consent

Lawful Purpose & Valid Consent



Fundamental Principle: Data must be processed for clear, lawful purposes only after obtaining valid, clear, and affirmative consent.

Consent Requirements: Consent must be requested **before** processing, and explicit written consent is needed for Sensitive Personal Data.

Right to Withdraw: Processing may continue only until consent is withdrawn by the Data Principal.

Affirmative Consent

Purpose Limitation

Notice to Data Principal



Mandatory Disclosure: Every consent request must be accompanied by a comprehensive privacy notice before or at the time of consent.

Content of Notice: Must inform about data categories, processing purpose, user rights, and the grievance redressal mechanism.

Clarity and Accessibility: Notices must be in plain, clear language, itemized, and specific.

Transparency

Informed Consent

Legitimate Uses & Voluntary Data



Implicit Consent: The Act covers data voluntarily provided where processing is necessary for the service (e.g., delivery address).

Legitimate Use Exemptions: Certain scenarios allow processing without explicit consent, such as for enforcing legal rights or investigating offenses.

Balancing Act: These exemptions balance individual privacy with crucial public interest and legal imperatives.

Public Interest

Legal Obligation

Core Obligations of Data Fiduciaries: Security & Retention

Data Processor Engagement



Contractual Mandate: Engage Data Processors only under a valid, legally binding contract defining scope, purpose, and processing nature.

Fiduciary's Responsibility: The Fiduciary remains accountable for data protection, ensuring the Processor implements adequate security measures per the DPDP Act.

Contractual Terms

Shared Responsibility

Third-Party Oversight

Security Safeguards



Mandatory Protection: Implement reasonable security safeguards to prevent personal data breaches, including unauthorized access, disclosure, or loss.

Risk-Based Approach: Safeguards should be proportional to the data's volume and sensitivity, potential harm, and available technology.

CIA Triad: Measures must ensure the Confidentiality, Integrity, and Availability of personal data through technical and organizational controls.

Data Integrity

Breach Prevention

Robust Controls

Data Breach Notification



Data Retention & Erasure



Key Principles & Rights under the DPDP Act

The DPDP Act is built upon non-negotiable principles and empowering rights for data principals.



Consent Management (Sec 6)

Consent must be **free, specific, informed, unconditional, and unambiguous**, requiring a clear affirmative action from the Data Principal.



Notice Requirement (Sec 5)

Data Fiduciaries must provide a **clear notice** to Data Principals about the personal data being collected and the precise purpose of its processing.



Purpose Limitation

Personal data processing must be strictly limited to a **specified and lawful purpose** communicated at the time of collection.



Data Minimisation

Data collection should be **limited to only what is necessary** for the stated purpose, avoiding excessive or irrelevant data acquisition.



Data Principal Rights (Sec 13)

Individuals have rights to **access information, correct, erase, and seek grievance redressal** concerning their personal data.

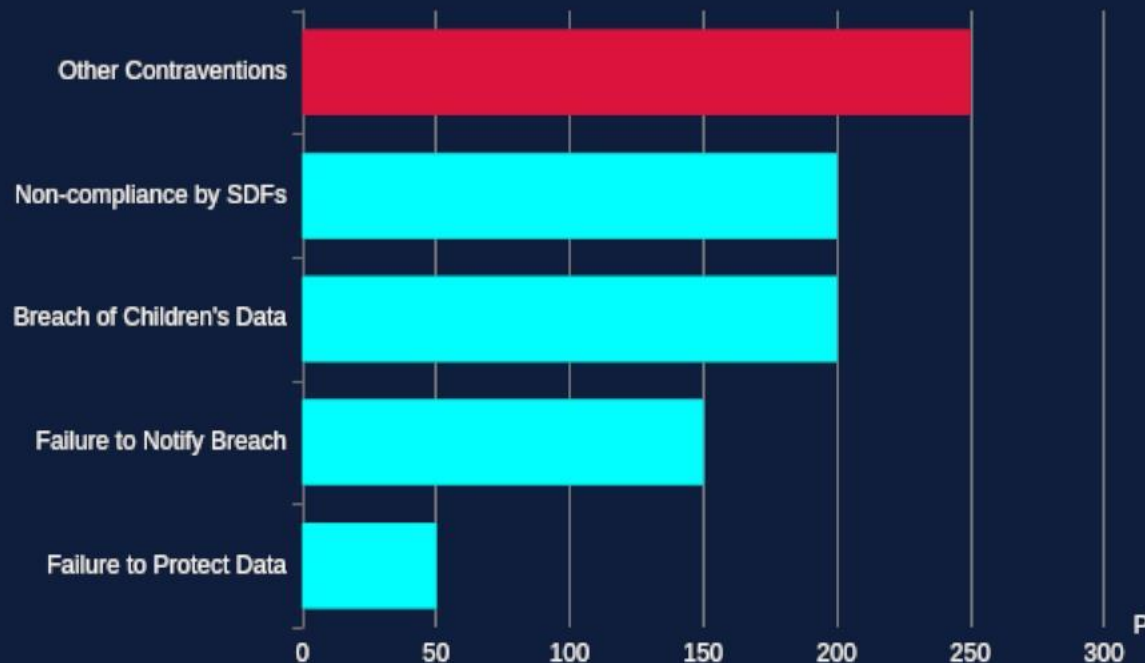


Data Protection Obligations

Fiduciaries must implement **reasonable security safeguards**, ensure data accuracy, and adhere to storage limitation principles.

Penalties for Non-Compliance under DPDP Act

DPDP Act: Penalty Structure Overview



Key Penalty Categories



Failure to Protect Data: Up to ₹250 crore

For not adopting reasonable security safeguards to prevent a data breach (Sec 34).



Failure to Notify Breach: Up to ₹200 crore

For not notifying the Board and affected Data Principals of a breach (Sec 35).



Breach of Children's Data Obligations: Up to ₹200 crore

For non-compliance with obligations related to children's data (Sec 33).



Non-compliance by SDFs: Up to ₹150 crore

For failure by Significant Data Fiduciaries to meet additional obligations (Sec 36).



Other Contraventions: Up to ₹50 crore

Applicable for other breaches of the Act not specifically categorized (Sec 37).

Significant Data Fiduciaries (SDFs) and Special Cases

Verifiable Consent: Children & Disabled

- ▶ The DPDP Act mandates heightened consent requirements for processing data of vulnerable Data Principals.
- ▶ For children, consent must be 'verifiable' and obtained from a parent or legal guardian.
- ▶ Mechanisms must be accessible and comprehensible for individuals with disabilities.



Parental Consent

Accessibility

Strict Verification

SDF Designation Criteria

- ▶ Designation is based on the volume and sensitivity of personal data processed.
- ▶ Risk of harm to Data Principals and impact on national security are key factors.
- ▶ Ensures entities with higher risks face more rigorous data protection standards.



Volume & Sensitivity

Risk Profile

National Security

Rights of the Data Principal

Right to Information

Comprehensive Disclosure: Data Principals have the right to obtain a clear summary of their processed personal data, including purposes, categories, and recipient details.

Transparency: They are entitled to know retention periods and the method to exercise their rights, with the privacy notice as a key tool.

Data Visibility

Processing Details

Transparency



Right to Correction & Erasure

Data Accuracy: Data Principals can ensure their data is accurate and complete, requesting corrections as needed.

Data Control: They have the right to request data erasure when its purpose is fulfilled or consent is withdrawn.

Data Accuracy

Data Control

Right to Be Forgotten



Strategic Steps for DPDP Act Compliance: Policies & Consent

Policy Development & Implementation



- › Develop comprehensive internal policies for data handling, storage, and processing.
- › Move from defensive compliance to active governance with clear guidelines.
- › Ensure policies cover the full data lifecycle, from collection to deletion.

Internal Frameworks

Notice Management



- › Provide clear, itemized privacy notices at or before seeking consent.
- › Clearly state data categories, purposes, user rights, and redressal mechanisms.
- › Use plain, accessible language, considering multi-lingual options for reach.

Transparency

Informed Communication

Consent Management



- › Obtain consent that is Free, Specific, Informed, and Unambiguous (FSIU).
- › Limit consent scope strictly to the purposes stated in the notice.
- › Provide an easy-to-use mechanism for Data Principals to withdraw consent at any time.

Valid Consent

User Control

Challenges for Chartered Accountants under DPDP Act

Navigating the New Regulatory Landscape: Key Hurdles for Clients



Compliance Burden

Extensive documentation, rigorous policy revisions, and significant process overhauls for clients demand meticulous attention and ongoing adherence.



Data Mapping & Inventory

Identifying, classifying, and securing personal data across diverse client systems requires meticulous data mapping and comprehensive inventorying.



Consent Management Complexity

Handling valid consent, easy withdrawal options, and maintaining auditable records presents a significant operational challenge for businesses.



Cross-border Data Transfers

Navigating evolving restrictions for international data flows adds complexity, requiring compliance with both Indian and global privacy regulations.



Resource & Expertise Gap

Many clients lack specialized in-house legal and technical expertise, creating a critical capability gap and demand for external advisory support.



Penalties & Liabilities

Significant financial consequences (up to ₹250 crore) and reputational damage for non-compliance directly impact client risk assessments.

Opportunities for Chartered Accountants in the DPDP Era

Pivoting Challenges into Growth: A New Horizon for CAs

The complexities introduced by the Digital Personal Data Protection Act (DPDP Act) are not merely challenges but significant avenues for growth and diversification for Chartered Accountants. Leveraging their inherent expertise in compliance, risk management, and audit, CAs are uniquely positioned to offer critical new services, transforming client needs into substantial opportunities.

Navigating the DPDP Landscape: Key Service Expansion



Data Audit & Assurance

Validate Compliance



Virtual DPO Services

Outsourced Expertise



Advisory & Consulting

Strategic Guidance



Training & Capacity

Empowering Teams

1. Data Audit & Assurance Services

Leveraging existing audit expertise, CAs can provide crucial **data privacy compliance audits**. This involves reviewing data protection policies, procedures, and controls to ensure adherence to the DPDP Act.

2. Virtual Data Protection Officer (vDPO) Services

For businesses that cannot afford or do not require a full-time in-house DPO, CAs can offer **outsourced DPO functions**.

This involves overseeing data protection strategies, advising on data

Impact of DPDP Act on Internal Audit

Shifting Focus from Financial Ledgers to Data Flows



Expanded Audit Mandate

Internal Audit's scope now explicitly includes assessing data protection compliance across all business functions (e.g., HR, Sales, IT, Operations, Legal).



Risk-Based Approach

Prioritizing audit efforts based on the volume, sensitivity, and risk associated with personal data processing activities within the organization.



Controls Assurance

Verifying the design and operational effectiveness of internal controls related to consent management, data retention, data breach response, and data principal rights fulfillment.



Technology & Data Governance

Evaluating the adequacy of IT infrastructure, security measures, and data governance frameworks to protect digital personal data.



Regular Reporting

Providing independent assurance to the Board and management on the organization's

Impact of DPDP Act on External Audit

A Paradigm Shift in Audit Scope: Integrating Data Privacy into Financial Integrity



Financial Statement Impact

Assessing potential for material misstatements & contingent liabilities from non-compliance.

Fines Significant penalties creating direct financial liabilities.

Costs Legal and remediation expenses impacting profitability.

Liabilities Provisioning for potential future non-compliance costs.



Audit Risk Assessment

Incorporating data privacy into the overall audit risk model, especially for data-intensive entities like banks, healthcare, and e-commerce.

- ▶ Reviewing risks in handling large volumes of sensitive personal data.
- ▶ Evaluating the risk profile of cross-border data transfers.



Going Concern Implications

Considering if significant breaches or persistent non-compliance could cast doubt on the entity's ability to continue as a going concern.

✗ Assessing impact of severe financial penalties on liquidity.



Industry-Specific Focus (e.g., Banks)

Increasing scrutiny on data protection in highly regulated sectors like banking.

KYC Data Scrutiny of Know-Your-Customer data handling & protection.



Management's Compliance

Evaluating the adequacy and effectiveness of management's processes and internal controls for ensuring DPDP compliance.

▶ Assessing if controls indirectly affect financial reporting reliability.


▶ Verifying robust frameworks for consent and data principal rights.

A TECHNICAL
SYSTEMS AUDIT CHECKLIST
FOR A LABORATORY MEASUREMENT SYSTEM

Audited Project: _____
Auditee: _____
Audit Location: _____
Auditors: _____
Audit Dates: _____
Brief Project Description: _____

AUDIT QUESTIONS	Y	N	NA	COMMENT
A. QUALITY SYSTEM DOCUMENTATION				
1. Is there an approved QA Project Plan for this project involving personnel?				▶ Assessing if controls indirectly affect financial reporting reliability.
2. Is a copy of the approved QA Project Plan maintained at the site and where quality assurance (QA) and quality control (QC) requirements and procedures are documented at the site?				▶ Verifying robust frameworks for consent and data principal rights.
3. Is the implementation of the project in accordance with the QA Project Plan?				
4. Are there deviations from the QA Project Plan?				
5. Do any deviations from the QA Project Plan affect data quality?				
6. Are written and approved current standard operating procedures (SOPs) used in the project? If so, briefly describe how and where the project procedures are documented.				

Implementing Compliance: Inventory, Governance & Audit Necessity

 Data Center



Personal Data Inventory & Mapping

Data Discovery: Systematically identifying all personal data collected and processed, answering "What data do we have?" and "Where is it?"

Flow & Purpose Mapping: Understanding how data moves through systems (data flow) and for what specific reasons it is used (purpose).

Storage & Lifecycle: Documenting where data is stored, access controls, and its lifecycle from collection to erasure.

Data Discovery

Data Flow

Purpose Mapping

 Cyber Security Padlock



Data Protection Governance

Policy & Framework: Establishing robust internal policies, procedures, and a comprehensive framework for data protection.

Board Responsibility: Emphasizing that data protection is a board-level responsibility requiring active oversight and strategic direction.

Committee & Roles: Defining committees, roles (e.g., DPOs), and responsibilities to manage, monitor, and enforce data protection.

Oversight

Accountability

Structured Framework



Data Audit: When, How Often, and Coverage

When & How Often: Data Audit Frequency

Annually for SDFs: Mandatory annual requirement for Significant Data Fiduciaries to ensure continuous oversight.

Risk-Based for Others: Frequency determined by risk assessment based on data volume, sensitivity, and processing complexity.

Post-Changes/Incidents: Triggered immediately after significant system/process changes or any data security incident.

Mandatory

Dynamic

Event-Driven



Core Coverage: Foundational & Operational

- **Governance Framework:** Policies, roles, and oversight.
- **Data Lifecycle Mapping:** Data flow, inventory, and minimization.
- **Purpose Limitation:** Adherence to stated purposes.
- **Notices & Consent:** Clarity and validity of mechanisms.
- **Security Controls:** Technical and organizational measures.
- **Retention & Deletion:** Adherence to schedules and secure erasure.

Strategic & Specialized Audit Points

- **Technology Audit:** Deep dive into IT infrastructure and systems.
- **Breach Management:** Review of incident response plans.
- **Data Minimization:** Ongoing efforts to reduce data collection.
- **Retention Audit:** Specific review of data retention schedules.
- **Cross-Border Sharing:** Compliance with transfer regulations.

Detailed Scope: Virtual Data Protection Officer (vDPO) Services

Understanding the Data Protection Officer (DPO)

An individual appointed by a Significant Data Fiduciary to act as a point of contact for grievances and compliance (as per **Section 10(2)** of the DPDP Act).



 **Core Responsibilities**

 **Client Benefits**

Opportunities and Conclusion



Opportunities: Skill Upgradation



↗ The DPDP Act creates a significant demand for specialized skills, opening new career avenues. This includes dedicated roles like **Data Protection Officers (DPOs)**, crucial for ensuring compliance.

✓ There is a growing need for professionals proficient in **Data Audit methodologies**, capable of independently reviewing data lifecycle management and identifying compliance gaps.

⚙ With mandatory breach notification, expertise in



Advisory, Consulting & Governance



🏠 Organizations require expert **Advisory and Consulting Services** to navigate the complexities of DPDP Act compliances, including gap analysis, policy development, and implementation support.

🏛 A key opportunity lies in assisting businesses in **Fostering Robust Data Protection Governance Frameworks**, embedding privacy-by-design into organizational culture.

🛡 Services can help establish clear roles and

Advisory & Compliance Consulting - A CA's New Forte

Pioneering Data Privacy Solutions: Comprehensive Consulting for the DPDP Era



Policy Development

Assisting clients in drafting robust privacy policies, consent forms, and internal data handling procedures.



Implementation Support

Guiding organizations through the practical application of DPDP requirements, including data mapping frameworks.



Risk Assessment & Mitigation

Identifying potential data privacy risks and advising on strategies to reduce exposure.



Data Governance Frameworks

Helping establish internal structures, roles, and responsibilities for ongoing data protection compliance.



Vendor Management

Advising on due diligence and contractual obligations with third-party Data Processors and Fiduciaries.



Incident Response Planning

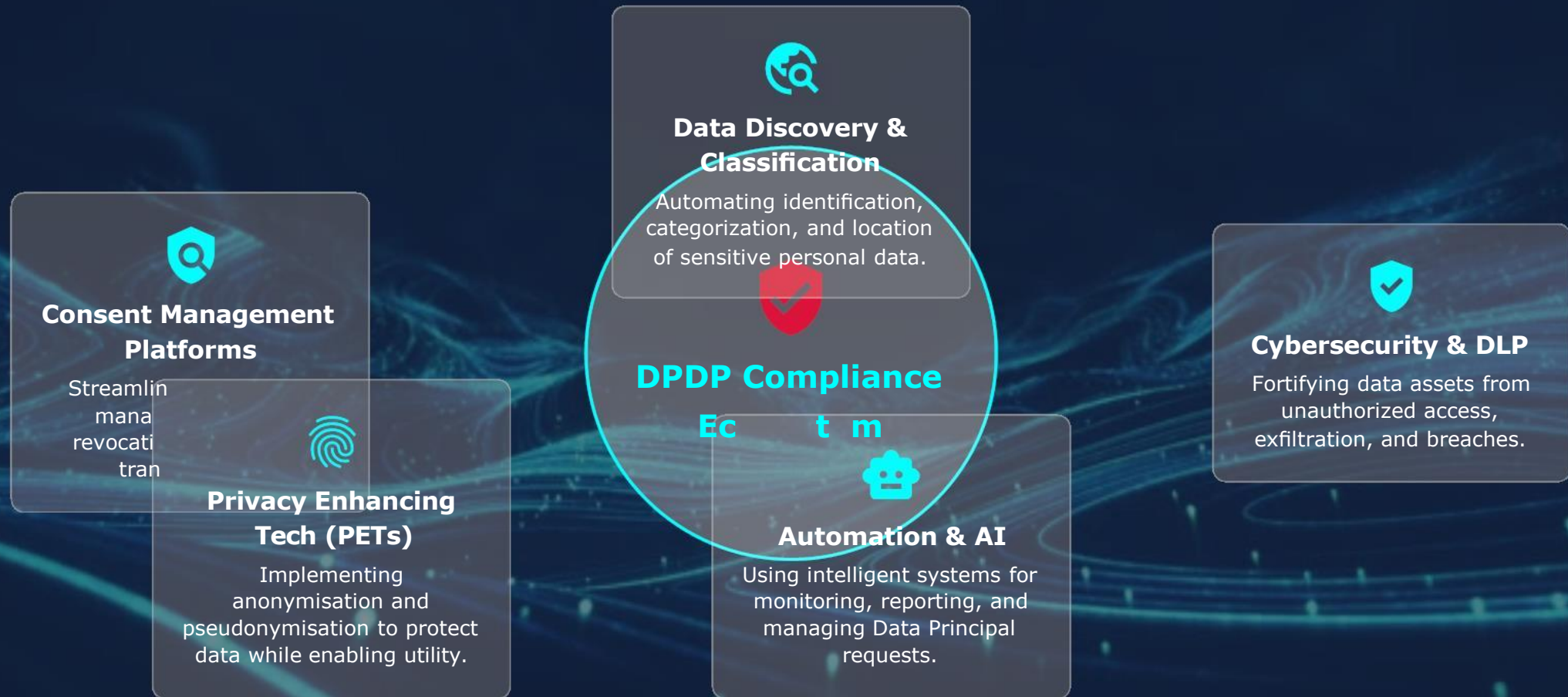
Developing protocols for effective and compliant handling of data breaches and security incidents.

A Strategic Imperative: The CA's Unrivaled Edge in Data

Leveraging Technology for DPDP Compliance

The Digital Advantage: Building a Resilient Compliance Ecosystem

In the dynamic landscape of the DPDP Act, technology is not just an enabler but a fundamental pillar for achieving and sustaining compliance. By strategically implementing advanced digital solutions, organizations can transform complex legal mandates into streamlined, efficient, and robust operational processes.



Q&A and Contact Information



Questions & Discussion

Thank You for Your Time!

