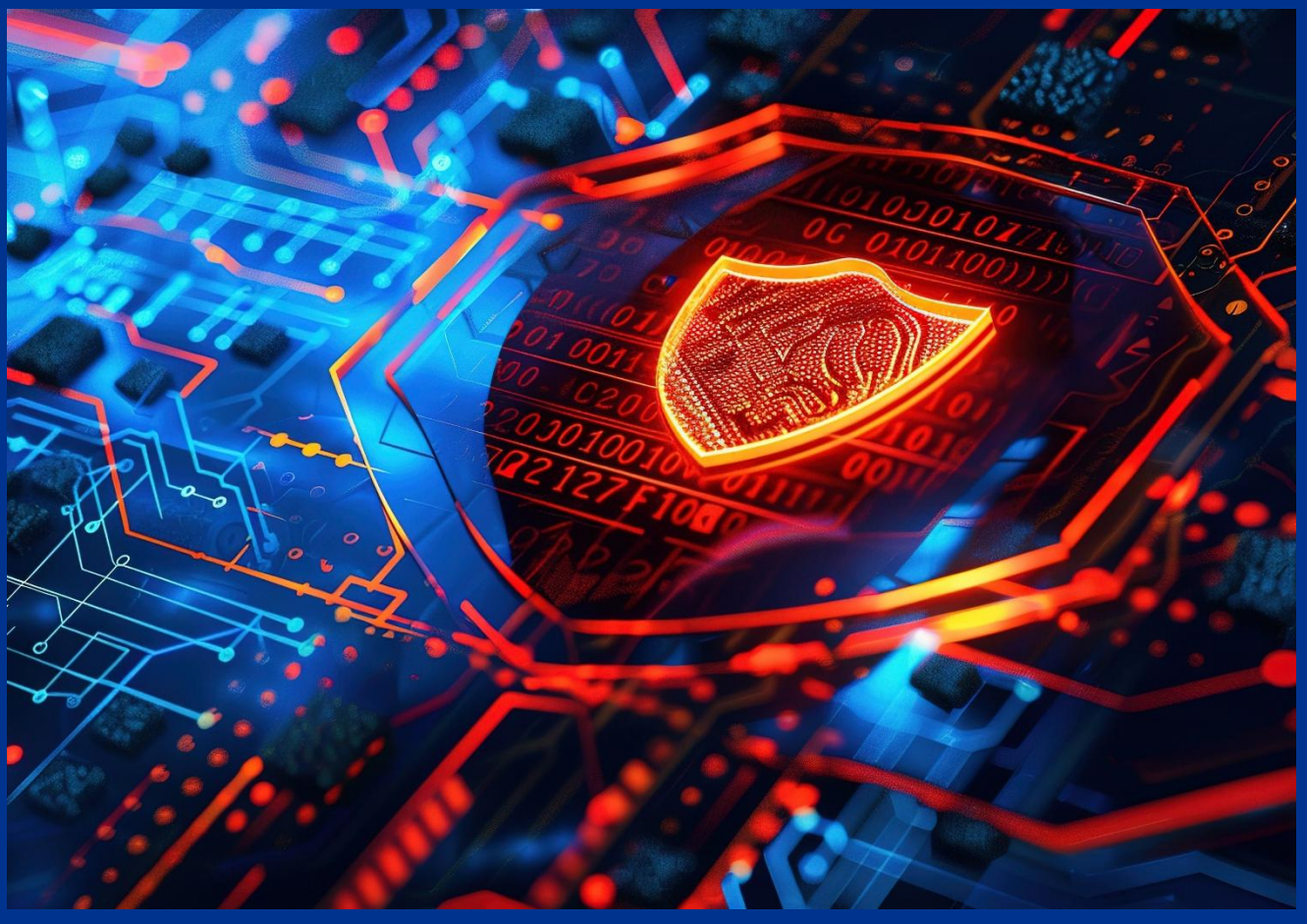
KPMG

Forensic perspective on personal data breach

KPMG. Make the Difference.



February 2026

kpmg.com/in

Imagine waking up to the news that your organisation has suffered a personal data breach. The bigger question isn't whether a breach occurred but whether you are prepared to answer what comes next.

Recognising the growing accountability of organisations in such situations, MeitY has now provided detailed direction through the Digital Personal Data Protection (DPDP) Rules, 2025.

Addressing this, the Ministry of Electronics and Information Technology (MeitY) has released the much-awaited Digital Personal Data Protection (DPDP) Rules, notified on November 14, 2025. While the act laid the foundation for a rights-based, consent-driven framework for personal data protection, ensuring accountability of Data Fiduciary and protecting Data Principal rights, the rules provide granular clarity on implementation timelines, consent mechanisms, breach reporting, and obligations of Data Fiduciaries and Significant Data Fiduciaries, please refer to MeitY official website for most updated act and the rules.

A breach happens - The questions begin

A data breach won't announce its arrival, but regulators will, and they won't come with just one question. This immediately raises concerns about your organisation's readiness to comply with the new DPDP rules.

When the scrutiny begins, the questions will come rapidly, and all at once:

1. Can your entity promptly identify what personal data was breached and which data principals are impacted?
2. Are logs, access trails, and system records available and retained to support forensic investigation?
3. Is the entity prepared and equipped to conduct a forensic investigation and submit its findings to the authority within 72 hours?
4. Can evidence be preserved immediately and defensibly after breach detection?
5. Can your entity reconstruct a clear breach timeline and chronology (occurrence → detection → containment)?
6. Is your entity prepared to submit fact based, regulator ready forensic reports to the Data Protection Board (DPB)?
7. Has your entity enabled incident response readiness, which might get overlooked by organisations? – **Forensic investigation** preparedness. Yes, you read that right.



Once a personal data breach occurs, a forensic investigation becomes critical to establish facts, preserve evidence, and support regulatory responses.

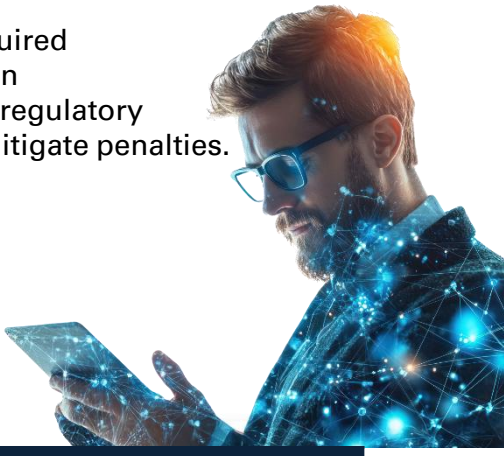
© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Incident to insight: The forensic path to DPDP Rule 7 compliance

According to Rule 7 of the DPDP Rules, in an event of personal data breach, the Data Fiduciary is required to immediately intimate the Data Protection Board (DPB) a description of the breach, including the nature, extent, timing and location and the likely impact of the occurrence. Further, within 72 hours, additional details are required to be furnished, including details such as root cause, persons responsible, and remedial measures. The entity must investigate a personal data breach to assess scope, identify responsibility, implement controls, and prevent recurrence, and promptly notify affected Data Principals of the breach, its impact, remedial actions, and grievance redressal channels.

The investigation process must comply with the provisions of Section 8(6) of the Act and Rule 7 of the Rules. To ensure compliance, a forensic investigation of the incident must be conducted in accordance with globally recognised industry standards such as ISO/IEC 27037 (Guidelines for Digital Evidence Handling), NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response), and ACFE Forensic Accounting Principles. Such assessments include impact analysis, root cause identification, risk and consequence assessment, evidence preservation and compliance mapping.

Whistleblowers trigger early warnings, and the Redressal Forum required under the Act ensures timely resolution strengthening data protection compliance. Proactive breach identification and investigation before regulatory intervention position the entity as compliant, responsive, and help mitigate penalties.



KPMG in India can help organisations with the following areas of expertise:

Business Impact	KPMG in India – Forensic investigation/eDiscovery
Regulatory action and response	
1. Evidence-driven regulatory response through forensic readiness and eDiscovery.	1. Prepare forensic reports, fact-based and defensible, timeline driven, aligned with DPDP rules 2. Translate technical findings into precise language expected by regulators 3. eDiscovery support to facilitate identification, preservation, collection, review, and analysis of Electronically Stored Information (ESI) 4. Provide credible audit trails.
Breach response and management	
1. Evaluate breach impact via traceable data access logs/records 2. DPDP-compliant vendor contracts on liability, indemnity and regulatory cooperation.	1. Determine whether the incident qualifies as a personal data breach under DPDP 2. Identify the type of personal data, sensitivity, scale, and affected Data Principals 3. Establish who accessed what, when, and under whose authority for accountability 4. Help entities contractually ring-fence DPDP risk by strengthening vendor liability, indemnification, and regulatory cooperation obligations.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Business Impact	KPMG in India – Forensic investigation/eDiscovery
Compliance management	
1. A living data protection compliance framework, reviewed and updated regularly 2. Strong whistleblowing framework to cover personal data related escalations.	1. Design cost-efficient compliance frameworks to cover personal data aspects 2. Enhance whistleblowing and Redressal Forum framework – to-dos 3. Conduct quarterly surprise forensic reviews to reduce gaps and regulatory risks 4. Update privacy policies and support trainings/workshops.

For better preparedness, KPMG in India also offers personal data breach simulation programmes.



KPMG in India contacts:

Manoj Kumar Vijai
Office Managing Partner, Mumbai
Head - Risk Advisory
E: mkumar@kpmg.com

Suveer Khanna
Partner and Head
Forensic Services
E: skhanna@kpmg.com

Kirit Amichandwala
Partner
Forensic Services
E: kirita@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the quoted third parties and do not necessarily represent the views and opinions of KPMG in India.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai – 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2026 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

This document is for e-communication only.