Privacy Pillar

Introductory Edition

Privacy & Beyond

Your Monthly Brief on Global Privacy, Technology, AI, Risk & Compliance Updates.

Privacy Pillar India Private Limited
November 2025

Privacy Partner

AISS2025

Contents

Foreword

Every few years, the way we understand privacy shifts, slowly at first, and then all at once. We are living through one of those turning points. Conversations about data protection, AI ethics and digital responsibility are no longer confined to compliance teams; they now shape business strategy, product decisions and, most importantly, public trust.

What defines this moment is not just the pace of regulation, but the depth of reflection it demands. With the DPDP Rules officially notified on 13 November 2025, organizations in India can no longer wait for clarity, clarity has arrived. The real question now is not whether we comply, but whether we deserve the trust that people place in us when they share their data.

This first edition of our newsletter brings together the developments shaping this shift, from the operational realities of India's new privacy regime to global movements redefining AI responsibility, enforcement, and digital accountability. Each update and case study highlights the same truth: data governance is not simply a legal requirement; it is a measure of an organization's integrity.

At Privacy Pillar, we believe that progress happens when technology and accountability work together, not in opposition. My hope is that this edition doesn't just inform you but encourages you to think differently about what it means to protect, respect and genuinely earn the data you hold.

- **Dharmesh Patel [Founder & CEO - Privacy Pillar]**

India

Privacy Regulatory Updates

- **BFSI Sector in India**
- **DPDPA Enforcement Updates**

India

Privacy Regulatory Updates

BFSI Sector in India

Fintech is evolving fast, and so are the rules. Reserve Bank of India ('RBI') and Securities and Exchange Board of India ('SEBI') are driving a new wave of responsible AI and data privacy in the Banking Financial Services and Insurance ('BFSI') sector.

a. **FREE-AI Committee Report – Framework for Responsible and Ethical Enablement of Artificial Intelligence (RBI)**

RBI's Committee has released its report on the Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREE-AI) in the financial sector. The framework is built on seven sutras (foundational principles) and twenty-six targeted recommendations under six strategic pillars, providing a holistic blueprint for responsible AI adoption across the financial ecosystem. [1]

b. **SEBI Consultation on Responsible Use of AI/ML in Securities Markets**

SEBI has not formally notified AI/ML guidelines for the securities market as of early October 2025, but it has issued several consultation papers and rules to address the use of technology. The most recent and comprehensive proposals for a regulatory framework were released in a consultation paper dated June 20, 2025, with input sought from the public until July 11, 2025. [2]

c. **The 2025 RBI Digital Lending Directions strengthen privacy.**

The 2025 RBI Digital Lending Guidelines strengthen privacy by mandating explicit borrower consent for data sharing, restricting sensitive phone data access (like contacts, call logs, and media), and requiring all data to be stored on servers within India with a 24-hour data localization mandate. The Directions align closely with the Digital Personal Data Protection Act, 2023 ('DPDPA'), reinforcing data protection principles specific to collection, usage, sharing of personal data with third parties and storage of data. [3]

[1] https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/FREEAIR130820250A24FF2D4578453F824C72ED9F5D5851.PDF
[2] https://www.sebi.gov.in/reports-and-statistics/reports/jun-2025/consultation-paper-on-guidelines-for-responsible-usage-of-ai-ml-in-indian-securities-markets_94687.html
[3] https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12848&Mode=0

India

Privacy Regulatory Updates

DPDPA Enforcement Updates

With the DPDP Rules 2025 now officially notified, organizations finally have clarity on phased compliance timelines. Businesses can begin aligning their processes with the new obligations while preparing for upcoming consent- manager and core compliance rollouts.

a. **India Notifies Digital Personal Data Protection Rules 2025**

On November 13th, 2025, the Ministry of Electronics and IT notified the Digital Personal Data Protection Rules, 2025, establishing phased rollout timelines. While core administrative provisions take effect immediately, consent-manager obligations activate after one year, followed by major compliance requirements within 18 months. The Rules mandate enhanced security measures, including encryption, log retention, and 72-hour breach reporting. They also impose new responsibilities on Significant Data Fiduciaries, requiring algorithmic risk reviews, periodic DPIAs, and independent audits to ensure accountability.[4]

The DPDP framework is coming into force in clearly defined stages, ensuring organizations have time to prepare for major changes

Implementation Tier	Effective Date	Key Rules and Focus
Immediate	November 13, 2025	Foundational Institutions: Establishes DPB, key definitions, and DPB's structure and operational rules.
One Year	November 13, 2026	Consent Management: Enables Consent Manager registration and penalties for violations.
18 Months	May 13, 2027	Core Operational Rules: Enforces notice, security, erasure, SDF duties, and Data Principal rights.

b. **India Releases BRD for Consent-Management Under DPDP**

In June 2025, Ministry of Electronics and Information Technology (MeitY) through its National e-Governance Division (NeGD), published a Business Requirements Document (BRD) for consent-management systems under the Digital Personal Data Protection Act, 2023 (DPDPA). The document outlines how organizations should manage consent lifecycles in line with the law's principles.[5]

4 https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

5 https://d38ibwa0xdgwxx.cloudfront.net/whatsnew-docs/8d5409f5-d26c-4697-b10e-5f6fb2d583ef.pdf

Global

Cyber and Digital Governance Updates

- **UK Cyber Governance Code**
- **UK Data (Use and Access) Act 2025**
- **NZ Privacy Amendment Act 2025**
- **TAKE IT DOWN Act**
- **California Privacy Regulations**
- **Florida Bar mandates cybersecurity**
- **CNIL Mobile App Guidance**
- **EU Data Act**
- **EU Guidelines on DMA-GDPR Interaction**
- **EDPB Clarifies DSA-GDPR Alignment**

Global

Cyber and Digital Governance Updates

a. Cyber Governance Code of Practice Guidance (UK)

The Cyber Governance Code of Practice, published in April 2025, guides boards and directors in managing cyber security risks. It outlines key governance actions, supported by free government resources such as Cyber Governance Training and the Cyber Security Toolkit for Boards, helping leaders strengthen accountability and resilience in cyber risk management. [6]

b. Data (Use and Access) Act 2025: Data Protection and Privacy Changes (UK)

The Data (Use and Access) Act 2025 (DUAA) modernises UK data laws to support innovation and responsible data use while keeping strong privacy standards. It refines rules on automated decision making, subject access, children's data, research, and international transfers, introduces new lawful grounds for processing, and eases certain cookie consent rules. The changes take effect gradually within 2–12 months of Royal Assent. [7]

c. Collection of personal information other than from individual concerned-Privacy Amendment Act 2025 (New Zealand)

New Zealand's Privacy Amendment Act 2025 introduces a new Information Privacy Principle 3A (IPP3A), requiring agencies that collect personal data from sources other than the individual to notify them, unless an exemption applies. The notice must explain why the data is collected, how it will be used, and who will receive it. This change enhances transparency and ensures individuals are aware when their data is gathered indirectly. [8]

d. TAKE IT DOWN Act Strengthens Privacy Against Deepfake Exploitation

The U.S. House of Representatives has passed the bipartisan TAKE IT DOWN Act, now awaiting presidential approval. The law criminalizes the publication of non-consensual intimate imagery, including AI-generated deepfakes, and compels online platforms to remove such content within 48 hours of a victim's notice. By addressing digital consent and image misuse, the Act strengthens privacy protection in the age of synthetic media. [9]

[6] https://www.gov.uk/government/publications/cyber-governance-code-of-practice/cyber-governance-code-of-practice
[7] https://www.gov.uk/guidance/data-use-and-access-act-2025-data-protection-and-privacy-changes
[8] https://www.legislation.govt.nz/act/public/2025/0053/latest/LMS899131.html
[9] https://www.commerce.senate.gov/2025/4/take-it-down-act-passes-the-house-heads-to-president-trump-s-desk

Global

Cyber and Digital Governance Updates

e. California Finalizes Regulations to Strengthen Consumers' Privacy.

On September 23, 2025, the California Privacy Protection Agency (CPPA) approved new regulations enhancing accountability and data protection. The rules introduce stricter requirements for cybersecurity audits, risk assessments, and oversight of automated decision-making systems. Together, they aim to reinforce consumer privacy and transparency in how organizations manage personal data. [10]

f. Florida Bar Committee on Cybersecurity and Privacy Law Recommendation

The Florida Bar's Committee on Cybersecurity and Privacy Law has issued Recommendation 25-1, urging lawyers and firms to create and annually update an Incident Response Plan (IRP) to better protect client and firm data. Though non-binding, the guidance promotes best practices for cybersecurity readiness and reinforces the profession's responsibility to safeguard sensitive information. [11]

g. Mobile applications: CNIL publishes its recommendations for better privacy protection

The French Data Protection Authority (CNIL) has released final recommendations to help app developers design mobile applications that respect user privacy and meet GDPR standards. The guidance covers consent, data minimization, and transparency, with enforcement actions set to begin in 2025 to ensure stronger privacy compliance in the mobile ecosystem. [12]

h. EU Data Act Unlocks Fair Access to IoT Data

Effective from September 12, 2025, the EU Data Act (Regulation (EU) 2023/2854) introduces harmonized rules on fair access to and use of data generated by connected devices. It grants users the right to access and share their IoT data with third parties, reinforcing individual control. Complementing the GDPR, the Act requires manufacturers to design products with accessible data by default and prohibits unfair contractual terms. [13]

[10] https://cppa.ca.gov/announcements/2025/20250923.html

[11] https://www.workplaceprivacyreport.com/wp-content/uploads/sites/938/2025/04/FL-Bar-Committee-on-Cybersecurity-and-Privacy-Law-Recommendation-25-1.pdf

[12] https://www.cnil.fr/en/mobile-applications-cnil-publishes-its-recommendations-better-privacy-protection

[13] https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

Global

Cyber and Digital Governance Updates

i. **EU Issues Joint Guidelines on DMA–GDPR Interplay**

Released on October 9, 2025, the European Commission and European Data Protection Board's (EDPB) joint guidelines clarify how the Digital Markets Act (DMA) aligns with the GDPR. Targeting large tech "gatekeepers," the guidelines emphasize that personal data may be combined only with valid GDPR consent under Article 5(2) of the DMA. Additional provisions address anonymization standards, strengthened data portability rights, and data minimization in interoperable digital services.[14]

j. **EDPB Clarifies Alignment Between the DSA and GDPR**

Published for public consultation on September 11, 2025, the EDPB guidelines explain how the Digital Services Act (DSA) aligns with the GDPR for intermediary service providers. They outline the lawful basis for processing personal data in content moderation, mandate non-profiling options in recommender systems, and reinforce protections for minors. The guidance confirms that using sensitive data for ad profiling is prohibited even with consent. [15]

[14] https://www.edpb.europa.eu/system/files/2025-10/joint_com-%09edpb_gls_interplay_dma_gdpr_for_public_consultation_en.pdf

[15] https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf

Global

Data Breach Updates

- **Tea App Data Breach**
- **Allianz Life Data Breach**

Global

Data Breach Updates

The past quarter has seen a surge in high-impact data breaches exposing not just personal, but deeply intimate and biometric information, reminding us that privacy protection extends beyond compliance to safeguarding human dignity.

a. Tea App Data Breach Exposes Highly Sensitive User Information

Behind the Case:

Tea, a social chat app popular among young users, confirmed a second major breach in July 2025, exposing over 1.1 million private messages containing highly sensitive personal discussions and profile data.

Who Was Affected and What Data Was Exposed:

Impacted data subjects: Registered Tea app users worldwide.

Data Exposed:

- Private messages
- Verification data, including photo IDs and selfies
- User profile details (emails, phone numbers, other identifiers)

Impact & Consequences:

The exposure of intimate communications and biometric data significantly heightens the risk of misuse, eroding user trust and increasing the likelihood of identity theft, impersonation, and harassment. The incident underscores the need for strong encryption, access controls, secure storage of verification data, and a rehearsed incident-response process to ensure timely notification to regulators and affected users.

DPDP Impact: What If This Happened in India?

Had a breach of this scale occurred in India, it would have invoked Section 8 of the DPDPA, 2023, read with Rules 6 and 7, potentially attracting penalties of up to INR 250 Crore. The Tea App incident ultimately highlights how weak protection of sensitive identifiers and intimate communications can result in serious regulatory and reputational consequences, reinforcing the importance of robust data-security practices.[16]

[16] https://www.bbc.com/news/articles/cd0dgkjgzvjo

Data Breach Updates

b. Allianz Life Breach Highlights Third-Party Risk in Financial Services

Behind the Case:

Allianz Life reported a July 2025 breach after a third-party CRM vendor was compromised, exposing policyholder data, but leaving its core systems and financial records untouched.

Who Was Affected and What Data Was Exposed:

Impacted data subjects: U.S. policyholders.

Data Exposed:

- Names and contact details (addresses, phone numbers, emails)
- Dates of birth
- Other personally identifiable policyholder data

No financial account details were compromised.

Impact & Consequences:

The incident raised concerns over delayed breach notification and weak vendor oversight, leading to regulatory scrutiny, class actions, and reputational damage. It underscores the need for strict due diligence, continuous vendor monitoring, and a clear incident-response plan.

DPDP Impact: What If This Happened in India?

Had such a breach occurred in India, Section 8 of the DPDPA read with Rules 6 and 7 would require prompt reporting and could trigger penalties up to INR 250 Crore. The Allianz case highlights that poor vendor controls can quickly escalate into legal and trust-related consequences.[17]

[17] https://economictimes.indiatimes.com/news/international/global-trends/insurance-giant-allianz-life-hit-by-data-breach-hackers-fooled-the-system-not-the-servers-and-nearly-1-4-million-affected/articleshow/122932918.cms

Global

The DPO Dilemma: Lessons from Case Law on DPO Position & Independence

- **Datatilsynet - Telenor ASA (Norway)**
- **Toyota Bank Polska S.A. (Poland)**

Global

The DPO Dilemma

From Europe to India, regulators agree, DPOs must be truly independent. As India readies for DPDPA enforcement, the Telenor ASA (Norway) and Toyota Bank Polska (Poland) cases show how weak DPO structures can trigger regulatory action.

a. Datatilsynet - Telenor ASA (Norway)

Year: 5th February 2025

Background:

Telenor ASA, a leading telecom provider in Norway, was investigated by the Norwegian Data Protection Authority (Datatilsynet) for shortcomings in its Data Protection Officer (DPO) structure. Though unrelated to a data breach, the probe found that the DPO lacked independence, direct reporting authority, and adequate resources, violating Articles 37 to 39 of the GDPR. The case underscores how structural gaps in DPO governance can trigger enforcement and offers key lessons for Indian organizations under the DPDPA.

Issues Raised:

- Whether the DPO had a clear and documented reporting line to top management?
- Whether the DPO's role was exercised with independence and free of conflicts of interest?
- Whether Telenor had provided the DPO with adequate resources and internal support to perform their tasks effectively?

EU-GDPR Articles Involved:

- Article 37 – Designation of the DPO.
- Article 38 – Position of the DPO (independence, reporting lines, resources).
- Article 39 – Tasks of the DPO.

Decision & Takeaways:

Datatilsynet found Telenor ASA's DPO lacked independence, direct reporting, and adequate resources, breaching GDPR Articles 37–39. The case underscores that DPOs must be independent, well-resourced, and conflict-free to ensure effective compliance.

The DPO Dilemma

b. President of the Personal Data Protection Office – Toyota Bank Polska S.A. (Poland)

Year: Decision - 18th December 2024; publicized - 2025

Background:

Toyota Bank Polska, a financial institution in Poland, was investigated by the Polish Personal Data Protection Office (UODO) for deficiencies in its Data Protection Officer (DPO) structure and its compliance with GDPR documentation obligations. The case examined whether the DPO was appropriately positioned within the organization and whether the bank maintained accurate and complete records of high-risk processing activities, such as profiling.

Issues Raised:

- Whether the DPO was independent and positioned appropriately, with a direct reporting line to top management.
- Whether the bank had documented profiling activities in its Records of Processing Activities (ROPA) and conducted proper Data Protection Impact Assessments (DPIAs).

EU-GDPR Articles Involved:

- Article 30 – Records of Processing Activities (ROPA)
- Article 35 – Data Protection Impact Assessment (DPIA)
- Article 38 – Position and independence of the DPO

Decision & Takeaways:

The Polish Data Protection Authority found that Toyota Bank Polska's DPO lacked independence by reporting through the IT/Security Department, breaching Article 38. The bank also failed to document profiling in its ROPA and conducted weak DPIAs, violating Articles 30 and 35.

Lessons for India under the DPDPA

Section 10 of the DPDP Act read with Rule 13 places additional responsibilities on Significant Data Fiduciaries, including the requirement to appoint a DPO located in India who reports directly to the Board. This role must be free from any conflicts of interest, as a lack of independence or overlapping responsibilities can compromise effective compliance.

Global

Advancements in Privacy Enhancement Technologies (PETs) & Their Use Cases

- **Advancements in HE**
- **Progress in ZKPs**

Global

Advancements in Privacy Enhancement Technologies (PETs) & Their Use Cases

The Privacy-Enhancing Technologies (PETs) market is growing rapidly, valued at USD 3.1–3.2 billion in 2024 and projected to reach USD 12.3 billion by 2030. Long-term forecasts estimate it could climb to USD 28.4 billion by 2034, driven by stricter regulations, rising privacy risks, and digital transformation. Data privacy and security are now among the fastest-growing segments in enterprise software, reinforced by global compliance mandates and the surge in data breaches. [18]

a. Advancements in Homomorphic Encryption (HE)

Imagine you have a locked box. You want a friend to perform a task on what's inside like adding numbers, but you don't want them to see the contents. Homomorphic Encryption (HE) is like a special magic box. It lets your friend work with the items inside without ever unlocking the box. When they're done and they give the box back, you can unlock it to see the result, knowing your secrets were never exposed. In the tech world, this "magic box" allows computers to perform calculations on encrypted (locked) data. This is a game-changer for privacy.

Use Case:	Objective:	Challenge:	Solution:
Using encrypted cloud analytics to study patient ecords while maintaining confidentiality and enabling secure, privacy-preserving medical insights generation.	Enable hospitals to analyse sensitive patient datasets in cloud environments without exposing personal information or compromising regulatory requirements.	Analysing data normally requires decryption, risking exposure of sensitive patient information, and causing privacy, security, and compliance concerns.	Patient data is encrypted before sending to the cloud, enabling secure processing and returning outputs decrypted by hospitals.

Key Takeaways:

- Strong Privacy: Data remains encrypted and confidential throughout processing.
- Performance Trade-off: Homomorphic encryption offers high security but can slow computation; starting small helps manage performance.

The growing focus on privacy-preserving computation highlights how techniques like HE can bridge the gap between innovation and regulatory compliance in sensitive sectors.

[18] Privacy Enhancing Technologies Market Size Report, 2030

Advancements in Privacy Enhancement Technologies (PETs) & Their Use Cases

b. Progress in Zero-Knowledge Proofs (ZKPs)

Imagine you know a secret, like the answer to "Where's Waldo?" You want to prove to a friend that you found him, but you don't want to show them where he is on the page. So, you take a giant piece of cardboard, cut a tiny hole in it just big enough for Waldo's face, and place it over the page. Your friend can look through the hole and see Waldo, confirming you found him. But they can't see anything else on the page, so his location remains your secret. This is the core idea behind Zero-Knowledge Proofs (ZKPs). They are a "magic trick" that lets you prove a statement is true without revealing the secret information that makes it true.

Use Case:	**Objective:**	**Challenge:**	**Solution:**
Enabling private blockchain transactions where users can validate, they have sufficient funds to pay, while keeping account balances and transaction amounts completely hidden from the network.	Allow users to participate in blockchain transactions securely by proving financial validity without exposing sensitive account information or revealing personal transaction details publicly.	Traditional blockchains make all transaction details publicly visible, creating significant privacy risks and preventing users from keeping balances, identities, and payment amounts confidential during transfers.	Zero-Knowledge Proofs lets users generate cryptographic proofs confirming funds and authorization, enabling the network to verify transactions without learning any balance, identity, or amount of information.

Key Takeaways:

- **Security Without Sacrificing Privacy:** ZKPs verify transactions without revealing sensitive data.
- **Powerful but Complex:** Modern protocols like zk-SNARKs and zk-STARKs offer speed and scalability but require expert implementation.

Integrating ZKPs into blockchain and identity systems demonstrates how privacy-enhancing technologies can support both innovation and regulatory accountability.

Under Rule 6 of the DPDP Rules, organizations must adopt reasonable security safeguards. Privacy-preserving technologies like Homomorphic Encryption and Zero-Knowledge Proofs enable encrypted, verifiable processing, reduce exposure risks, and help operationalize privacy-by-design for stronger compliance.

Global

AI Governance Updates

- **Italy Enacts First AI Law**
- **U.S. AI Antitrust Strategy Released**
- **India Releases AI Governance Guidelines**

Global

AI Governance Updates

From ethical frameworks to enforcement-ready rules, AI governance is moving to the forefront of privacy and compliance discussions. Here are the latest developments shaping how organizations design and deploy AI responsibly.

a. Italy Enacts First Comprehensive National AI Law in the EU

On September 17, 2025, Italy became the first EU country to pass a national AI law, introducing stricter oversight alongside the European Union Artificial Intelligence (EU AI) Act. The law mandates parental consent for AI use by children under 14, imposes criminal penalties for harmful AI misuse, and restricts text and data mining of copyrighted content. It highlights the growing trend of national-level AI governance and the need for adaptable, localized compliance frameworks across Europe. [19]

b. U.S. Strategy for AI and Antitrust: Ensuring Fair Market Dynamics

On September 18, 2025, the U.S. Justice Department underscored antitrust enforcement as a key pillar of AI governance, warning against market dominance by major tech firms controlling data and computational power. The Department pledged stronger enforcement to preserve fair competition, including support for rulings requiring data-sharing among rivals. The move highlights that AI governance extends beyond ethics and safety to ensuring open, competitive, and innovation-driven markets. [20]

c. India Releases National AI Governance Guidelines

On November 5, 2025, MeitY introduced India's first comprehensive AI Governance Guidelines under the IndiaAI Mission, outlining a principle-based, innovation-friendly framework for safe and responsible AI deployment. The guidelines define core "sutras" on trust, fairness, accountability, and safety, adopt a risk-based approach, and provide direction on transparency, testing, and redressal. This marks a major step in India's push for flexible, growth-oriented AI governance while addressing emerging societal and safety risks.[21]

[19] Reuters – Italy enacts AI law covering privacy, oversight and child access
[20] Reuters – Trump's AI plan supports antitrust enforcement, DOJ official says
[21] https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251156856O1.pdf

Quick Roadmap for DPDPA Compliance

A practical, action-focused guide to help organizations align with the DPDP Act and its newly notified Rules. This roadmap outlines essential steps every Data Fiduciary must take to strengthen privacy practices and achieve timely compliance.

- **Refresh Your Notices:** Update privacy notices with clear, specific descriptions of what data you collect and why. Make it easy for users to understand before they consent.
- **Modernize Consent Flows:** Ensure consent is free, informed, specific, and easy to withdraw. Build seamless workflows that mirror the simplicity of giving consent.
- **Prepare for Consent Managers: E**nable systems to integrate with registered Consent Managers so individuals can manage permissions through unified, interoperable platforms.
- **Strengthen Security Basics:** Apply encryption, access controls, authentication, and monitoring as mandated. Techno-legal safeguards are now a compliance requirement, not a choice.
- **Enable User Rights:** Provide simple, accessible channels for people to request access, correction, deletion, or grievance redressal. Publish your DPO or contact person clearly.
- **Act Fast on Breaches:** Set up internal triggers to detect incidents early. Notify the Board within 72 hours and inform affected users without unnecessary delay.
- **Retain Responsibly:** Keep logs and related processing records for at least one year. Delete personal data once the purpose is fulfilled, unless another law requires retention.
- **Protect Children & Guardians:** Implement verifiable parental consent and disable tracking, profiling, or targeted ads for children. Always confirm lawful guardianship where required.
- **Check Your Vendors:** Update contracts with data processors to ensure they meet security, deletion, retention, and breach-support obligations. Compliance must flow across your ecosystem.
- **Audit & Improve Continuously:** Map your data flows, train internal teams, run periodic assessments, and prepare for future obligations, especially if categorized as a Significant Data Fiduciary.

India

Industry Voices

- **Ashiwni Siddhi**
- **Dr. Varda Mone**

Featuring: Ashwini Siddhi

Founder and Cybersecurity Professional

"Being heard in the room is itself half the battle. Once you find your voice, the rest is about showing up, learning and leading by example."

Could you tell us about your journey in cybersecurity and some challenges that shaped your path?

I started my career as a developer but soon realized I wanted to explore how systems worked, which led me to security after reading about OWASP and cross-site scripting attacks. I transitioned to a small security team within the same organization and learned about the job. Initially, pen testing seemed glamorous, but I soon appreciated the depth and diversity of security.

The biggest challenge wasn't just technical, it was navigating workplace dynamics as a woman, but persistence, clear communication and documenting my work made all the difference.

Could you share the challenges you faced while transitioning from an employee to a woman startup founder?

The transition to a startup felt organic, fueled by years of experience and a desire to tap into creativity beyond KPIs. The biggest challenge has been navigating the unpredictable nature of a startup, maintaining a pipeline, and building the brand.

Early in my career, I often managed projects alone and many times was the only woman in key discussions. Learning to navigate thoughtfully and communicate clearly built resilience and strategic skills, forming a strong foundation for leading a startup.

As a startup founder today, what guiding strategies help you manage security programs effectively?

For me, it's about giving your best every single day while keeping a long-term maturity-based approach. Security isn't something that can be built overnight; it evolves.

Every organization operates at a different level of maturity. Some are just starting with basic controls, while others are aiming for cutting-edge frameworks. We tailor our approach, accordingly, helping clients progress step by step rather than overwhelming them. At the end of the day, security and privacy may not directly generate revenue, but they strengthen trust, brand reputation, and resilience. That's true value creation.

While you have inspired and mentored many women in the tech & security space, how has that experience shaped you?

It's been one of the most fulfilling parts of my journey. I often meet young women who say they aspire to have a career like mine, and that truly humbles me.

Through mentorship programs like Women in Tech Network, I've connected with many women, helping them map career paths, build networks, and navigate challenges at work. Sometimes, seeing them grow gives me immense satisfaction and reminds me why representation matters.

Do you have mentors who've guided your professional growth?

Interestingly, I didn't have mentors early in my career. It was only later, during my time at Dell, that I met a few who made a huge impact.
They never told me what to do, instead, they asked questions that pushed me to think and reflect. That's the kind of mentorship I value most, one that empowers independent decision-making and self-awareness.

Finally, what advice would you give to someone just starting in cybersecurity?
Don't blindly follow someone else's journey. What worked for them may not work for you; everyone's path is unique. Try different things, explore multiple domains, and find where your true strengths lie.
Build one strong skill and stay aware of related areas, and most importantly, don't chase certifications just for the sake of it. Focus on what knowledge you bring to the table and how effectively you apply it.

Key Takeaways:

- Ashwini's path from developer to cybersecurity founder underscores curiosity and hands-on learning, a chance encounter with OWASP led her to explore web vulnerabilities and move into security. Technical skill mattered, but so did persistence, especially navigating workplace dynamics as one of few women at the table. She credits clear communication, thorough documentation, and showing up consistently for building credibility and influence.
- Founding a startup brought new challenges, unpredictability, pipeline management, and brand building. Ashwini's approach is pragmatic and maturity-based, assess where an organisation sits on the security curve and guide it forward step-by-step rather than forcing advanced frameworks prematurely. For her, security's ROI is trust, reputation, and resilience, not direct revenue.
- Mentorship shaped her later career, she values mentors who ask the right questions and encourage independent thinking. Today, mentoring others is deeply fulfilling and reinforces why representation matters.
- Her advice to beginners, experiment across domains, build one strong, practical skill, stay aware of related areas, and prioritise applied knowledge over checklist certifications. Find the path that fits your strengths and keep iterating.

Featuring: Dr. Varda Mone

Legal Academic and Data Privacy Specialist

"In medical universities, professors practice what they teach, but in law, that bridge between academia and industry is still missing. It's time we build it."

Can you tell us how your journey in privacy started and evolved over the years?

My journey into privacy began during law school when I participated in a national moot on digital identity and data protection, long before privacy became mainstream. It made me realize how personal data, even health information, can have deep social and legal implications. Later, my PhD research expanded this understanding, exploring privacy as both a constitutional right and a global governance challenge. The limited academic focus on data protection inspired me to advocate for stronger privacy education and interdisciplinary research in law schools.

Do you think there's still a gap between academic research on privacy and how it's applied in industry?

Yes, there's still a gap. Academic research often focuses on theoretical aspects of privacy, while industries seek practical, compliant solutions. Since privacy is deeply cultural, what works in Europe may not suit India or the U.S. Bridging this divide needs stronger collaboration between academia and industry, greater support for applied privacy research in India, and more initiatives that bring students and researchers closer to real-world privacy challenges.

How have these challenges shaped the way you mentor your students or guide young researchers in privacy and technology?

I always tell my students that privacy can't be learned from theory alone, it requires hands-on experience. I encourage internships where they see principles like purpose limitation applied in audits or compliance reviews.

In class, they analyze real company privacy notices, spot gaps, and suggest improvements, learning how principles translate into design and policy. Integrating practical tools and fostering industry-academia partnerships helps students gain real-world understanding.

While you have mentored many students yourself, has there been a mentor who guided you on your journey, and how did that shape your path in privacy and academia?

Yes, my biggest mentor has been my research guide. Though his expertise lies in international law rather than technology, his constant encouragement allowed me to explore privacy from a global governance perspective. He taught me to think critically about laws in transition, especially when India's data protection framework was still evolving.

Later, interactions with professors in Switzerland who had worked with scholars like Graham Greenleaf further refined my global outlook on privacy. Their support reinforced my belief that mentorship is about nurturing curiosity, not limiting it to one discipline.

Do you feel your work has influenced students, peers, or emerging women professionals in privacy and technology?

I believe my work has made a meaningful academic impact. Over the years, students and researchers from universities like JNU, DU, and IIM have reached out for my papers, many of which are published with global publishers like Cambridge University Press, Wiley, and Taylor & Francis. Recently, I've also had young women LLM students approach me for internships, which shows that my journey is encouraging more women to explore privacy research.

What advice would you give to women, students or young professionals aspiring to build careers in data privacy, technology law, or interdisciplinary research?

Move beyond surface-level research. Many students pick trending topics like AI without realizing much has already been explored. Focus on how global principles translate into local realities, for instance, studying how responsible AI policies are implemented. In India, technology law needs more empirical, field-based research. Observe, analyse, and connect theory to practice. Curiosity, practical exposure, and critical thinking are what create meaningful research and real impact in this field.

Key Takeaways:

- Dr. Varda's interest in privacy began during law school, where a national moot on digital identity exposed her to the legal and social impact of personal data. This shaped her academic direction and later her PhD, where she studied privacy as both a constitutional right and a global governance concern.
- She notes a clear gap between academic theory and industry needs, with universities focusing on concepts while organizations seek practical, culturally grounded solutions. She believes stronger collaboration and more applied research are essential to bridge this divide.
- Her teaching emphasizes hands-on learning, encouraging students to review real privacy notices, assess gaps, and understand how principles like purpose limitation or transparency work in practice. This helps them translate theory into real-world application.
- Mentorship has deeply influenced her outlook, from supervisors who encouraged interdisciplinary thinking to global scholars who broadened her perspective. Her advice to future professionals: look beyond trending topics, study how global ideas work in local contexts, pursue empirical research, and stay curious. impact lies in connecting theory with practice.

India

Featured Updates

Privacy Partner

AISS2025

December 03 - 05 Pullman Aerocity New Delhi

Booth #P1

We're thrilled to announce that Privacy Pillar is the Official **Privacy Partner** for the **Annual Information Security Summit (AISS) 2025**! This strategic partnership underscores our commitment to advancing privacy excellence and data protection standards across the industry.

Privacy Pillar will have a dedicated presence throughout the three-day summit. Stop by **Booth #P1** to explore our cutting-edge privacy solutions, experience live product demonstrations and discover how we're simplifying compliance for modern enterprises.

Why Privacy Pillar is at AISS 2025?

As the official privacy partner, Privacy Pillar combines proven enterprise privacy expertise with cutting-edge technology that meets evolving regulatory demands. Our team brings a global perspective with deep local market understanding, united by a commitment to advancing privacy standards across the industry.

Exclusive Opportunity:

The Privacy Pillar founding team is flying in from the United States specifically for AISS 2025! This is a rare opportunity to connect directly with the visionaries behind Privacy Pillar's innovative approach to privacy management. Whether you're exploring privacy solutions, seeking strategic guidance or interested in partnership opportunities, our founders are here to engage in meaningful conversations.

DHARMESH PATEL
Founder & CEO

KASHYAP VYAS
Co-Founder & COO

BOOK YOUR MEETING NOW

Don't miss this exclusive opportunity! Secure your personalized consultation with Privacy Pillar founders - every conversation is designed to provide tailored insights and actionable solutions for your specific privacy needs.

India

Privacy Pillar Updates

We're excited to announce our latest whitepaper, **"DPDPA Compliance Playbook: Starter Guide!"** This guide helps organizations navigate the essentials of the Digital Personal Data Protection Act, 2023, offering practical insights, actionable steps and best practices to simplify compliance and strengthen your data privacy strategy.

DOWNLOAD PLAYBOOK

***With the DPDPA Rules 2025 now officially released, we're working on an updated version of this playbook to incorporate the latest regulatory requirements. Keep an eye on Privacy Pillar's Official LinkedIn Page for the upcoming release!

Upcoming Webinars:

- Navigating DPDP: Real Challenges for Privacy Leaders - TBA
- AI, Innovation & Privacy: Balancing DPDP Demands - TBA

Contributors:

MS. KRITHI SHETTY
Associate Director - Data Privacy

MS. TANYA SINHA
Senior Data Privacy Consultant

MR. PAWAN KALYAN
Data Privacy Consultant

MR. AMEETH ALWA
Data Privacy Consultant

MS. HARSHITA REDDY
Data Privacy Consultant

Get In Touch With Our Privacy Team:

MR. DHARMESH PATEL - Founder & CEO	dharmesh@privacypillar.com
MR. KASHYAP VYAS - Co Founder & COO	kash@privacypillar.com
MR. AKHILESH MS - Director [Strategy & Growth]	akhilesh.ms@privacypillar.com | +91 88868 88465
MS. KRITHI SHETTY - Associate Director [Data Privacy]	krithi.shetty@privacypillar.com | +91 81051 19604

India's New Digital Personal Data Protection Rules Are Here - Are You Ready?

Book a one-to-one session with Privacy Pillar's privacy experts to get personalized guidance or answer your privacy queries on navigating India's Digital Personal Data Protection Rules, 2025 (DPDPA).

BOOK 1:1 SESSION