Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Protecting our Personal Information: Best Practices under Recent Privacy Laws

Satirtha Basak[a]

[a]Law Centre 1, Faculty of Law, Delhi University, Delhi, India

Received 24 February 2025; *Accepted* 24 March 2025; *Published* 28 March 2025

This article delves into methods for safeguarding personal data. It examines leading privacy regulations like the GDPR, CCPA, LGPD, and Australia's Privacy Act. It also looks at legal duties, enforcement hurdles, and areas where compliance might fail. The study highlights complex factors, including legal intricacies, consent management, and data security concerns. Additionally, it explores how AI and IoT affect privacy. Organisations play a central role in protecting sensitive details. This article underscores the value of informed consent and careful data use. It urges flexible oversight that adjusts to new technologies. International coordination is stressed as essential for effective protection. The study also recommends solid internal governance. Transparent policies and accountability measures are vital for building trust. Steps reinforce privacy globally. Real-world examples showcase complex compliance hurdles and spotlight enforcement issues. They reveal how organisations handle evolving privacy mandates. Lessons from these scenarios shape effective strategies. This research presents targeted guidance for governments, firms, and communities. It urges tougher oversight, promotes tech-based safeguards, and champions user rights. Ultimately, it sparks conversations on advancing privacy laws in a rapidly changing digital world.

Keywords: *data privacy, enforcement, compliance, transparency, regulation, trust, innovation.*

INTRODUCTION

Personal data is any detail linked to an identifiable person. It covers direct markers like names and Social Security numbers. It also includes indirect clues such as IP addresses. These clues can pinpoint an individual's identity when combined with other information. In today's digital age, this information is highly valuable. It drives innovation and fuels economic growth across industries globally now. Companies use personal data to improve their operations. They analyse information to make better decisions. This data helps tailor services to individual needs. Firms use these insights to boost efficiency and competitiveness.

In the modern market, data-driven strategies offer a significant advantage. Businesses invest in data protection and compliance. They balance innovation with privacy to maintain trust and legal integrity.[1] The rapid rise of big data analytics, artificial intelligence, the Internet of Things, and targeted digital marketing has greatly boosted the collection and processing of personal details. This explosion of data increases privacy risks and fuels growing public concern. As more information is gathered and analysed, individuals become increasingly vulnerable to misuse and exploitation in today's digital environment across platforms. Major data breaches have exposed glaring flaws in data protection practices.

The Facebook-Cambridge Analytica scandal demonstrated how personal information can be exploited for political profiling. The Equifax breach compromised the sensitive financial data of millions. These incidents underscore the urgent need for strong security measures, regulatory oversight, and robust safeguards to protect individuals and restore trust in digital information systems.[2] This article sets out to discover effective best practices in protecting data by closely examining the latest privacy laws and their implementation. It reviews legal duties imposed on organisations and considers how regulators enforce these rules. It also evaluates the hurdles that challenge compliance. The research offers clear insights into safeguarding personal information within our ever-changing digital landscape globally today.

---

[1] Bogdan Halcu, 'Personal Data: The New Oil of The Digital Economy' (*Chambers and Partners*, 29 November 2016) <https://chambers.com/articles/personal-data-the-new-oil-of-the-digital-economy> accessed 19 February 2025

[2] 'Cybersecurity History: Hacking & Data Breaches' (*Monroe University*) <https://www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches> accessed 19 February 2025

HISTORICAL AND LEGAL BACKGROUND OF PRIVACY LAW

Privacy rights have evolved significantly over time. They originate from common law principles that continue to change. This shift reflects society's growing need for personal security. Over many years, legal concepts expanded to protect individual privacy. These rights are now fundamental in a world where personal data is at risk. They underpin modern legal protections. These principles guide legal fairness. In 1905, a landmark case marked the legal recognition of privacy rights. The Georgia Supreme Court ruled in Pavesich v New England Life Insurance Co. that individuals could seek a remedy for privacy invasions.

This decision established an early legal remedy and set a precedent for protecting personal boundaries. It significantly influenced later privacy laws and shaped the legal landscape decisively.[3] Privacy rights in the United States are protected through four specific legal torts. One is an intrusion, where someone unlawfully invades another's private space. Another is appropriation, where a person's identity is used without permission. Additionally, public disclosure involves revealing sensitive information not meant for public view. Lastly, false light misrepresents someone in a damaging manner. They have shaped modern privacy. Indeed, these legal tools are vital for protecting privacy. They empower individuals to seek redress when their private lives are invaded. Courts use these claims to address harms from unauthorised data use or exposure.

They provide a framework for accountability and compensation. As society evolves, these remedies remain essential for upholding respect for dignity and maintaining trust in legal protections.[4] Key judicial cases have greatly shaped privacy rights over the years. One landmark case was Katz v United States in 1967. In this decision, the U.S. Supreme Court declared that the Fourth Amendment protects individuals rather than specific places. The court introduced the concept of a reasonable expectation of privacy that has since influenced many legal rulings. This ruling shifted the focus from physical spaces to the privacy interests of people. It continues to serve as a fundamental precedent in privacy law. The principles established in this case guide numerous decisions and remain vital in protecting personal

[3] Daniel J. Solove, 'A Brief History of Information Privacy Law' in Christopher Wolf (ed), *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age* (Practising Law Institute 2006)
[4] Robert Rafii , 'Invasion of Privacy: Public Disclosure of Private Facts' (*Find Law,* 03 August 2023) <https://www.findlaw.com/injury/torts-and-personal-injuries/invasion-of-privacy--public-disclosure-of-private-facts.html> accessed 18 February 2025

rights today. Indeed.[5] In India, a landmark ruling further solidified privacy rights. The case Justice K.S. Puttaswamy (Retd.) v Union of India in 2017 recognised privacy as a fundamental right under the Constitution. This decision marked a major shift in Indian law and affirmed the value of personal privacy. It underlined the global recognition of privacy as an essential human right. The ruling has influenced subsequent legal decisions and policy discussions in India. Its impact is seen in how privacy is now protected and respected in the digital age. This precedent continues to inspire legal reforms across the country. A turning point indeed.[6]

EVOLUTION OF PRIVACY LAWS

Modern privacy laws evolved through major legislative milestones. The 1974 U.S. Privacy Act emerged amid fears of growing computerised databases. It governs how federal agencies handle, maintain, and use personal information. This law sets essential safeguards against privacy violations. Individuals received new protections from data abuses. Congress aimed to address the risks of technological advancement. The Act introduced accountability for governmental data management. It clarified the boundaries of acceptable data use. This was a critical move toward personal privacy rights. Early efforts like these shaped the groundwork for today's frameworks. Each development responded to the expanding digital landscape effectively and proactively.[7]

The 1995 EU Data Protection Directive was another pivotal milestone. It aimed to align data protection rules across all European Union nations. This directive sets key principles for handling personal data fairly. It required organisations to ensure transparency, security, and legitimate purposes for data use. Governments implemented national laws based on these standards. Although broad in scope, the directive eventually faced technological challenges. Rapid digital innovations exposed gaps in protection. This realisation spurred efforts to update regulations. The directive became a foundation for the General Data Protection Regulation.

Modern privacy frameworks now owe their origins to this ground-breaking legislative step.[8] In the early 2000s, privacy laws grew more consumer-focused worldwide. Many legislatures

[5] *Katz v United States* [1967] 389 U.S. 347
[6] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1
[7] The Privacy Act 1974
[8] Paul M. Schwartz, 'THE EU-U.S. PRIVACY COLLISION: A TURN TO INSTITUTIONS AND PROCEDURES' (2013) 126(1) Harvard law review <https://www.law.berkeley.edu/files/Schwartz_Paper_-_EU_US_Priv_Collission_(Galleys_03_14_13).pdf> accessed 12 February 2025

introduced stronger protections against data misuse. California led the way in 2003 by passing data breach notification laws. This landmark move forced businesses to inform individuals if personal data was compromised. Other regions followed, adopting similar measures and reinforcing privacy safeguards. These regulations underscored the rising importance of consumer trust. They pressured companies to enhance security practices and accountability. This era marked a turning point for data privacy laws. Legislators recognised evolving threats in a digital landscape. They responded by pushing for robust, transparent, and forward-looking consumer-centric frameworks.[9]

OVERVIEW OF RECENT PRIVACY LAWS

Many leaders have approved strong privacy laws to protect personal data. Governments are increasingly concerned about digital security. We emphasise major frameworks such as Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States. These laws set clear rules for data use and its enforcement. They aim to safeguard individual rights. This review also discusses other significant laws from around the world. It examines Brazil's Lei Geral de Proteção de Dados and Australia's Privacy Act. These regulations contribute to a global context for data protection. Their provisions help harmonise standards across borders. This broader view enriches our understanding of privacy and informs ongoing legal reforms. These laws are essential for progress.

General Data Protection Regulation (GDPR) – Europe: The GDPR, General Data Protection Regulation, was authorised in 2018. It is a comprehensive privacy law for all EU (European Union) members. The regulation exercises control over how personal data is protected, processed, and transferred. It sets clear rules on data use. Individuals gain the right to access and control their personal information. Explicit consent is required before data is used. This law marks a major shift. A key feature is the notification of data breaches. The regulation requires companies to inform users quickly. It also introduces the role of a Data Protection Officer. This position ensures compliance with the law. Moreover, the GDPR has

[9] *Ibid*

extraterritorial reach. Companies worldwide must follow their rules if they handle EU citizens' data. The law sets a global privacy standard indeed.[10]

California Consumer Privacy Act (CCPA) – United States: The California Consumer Privacy Act (CCPA) took effect in 2018. It is the most complete data privacy law in the United States. While it shares some features with Europe's GDPR, key differences remain. The CCPA gives the people of California rights over personal data collection. They can request data deletion. They can also opt out of data sales. The law is consumer-driven and shaped by technology. Beneath the CCPA, businesses must disclose data collection practices. They must also provide clear opt-out tools. This stands in contrast to the GDPR. The GDPR focuses on protecting residents wherever they live. The CCPA emphasises commercial activities instead. Its scope highlights consumer transactions. This shift demonstrates the distinct regulatory landscape in the United States. It marks a significant departure from Europe.[11]

Lei Geral de Proteção de Dados - Brazil's: Brazil's Lei Geral de Proteção de Dados became law in 2018. It responds to rising worries over data privacy. The regulation takes substantial cues from Europe's GDPR. Both laws share many foundational principles. Like the GDPR, Brazil's version grants people rights over their data. It requires explicit consent. It also mandates data breach notifications. The parallels are notably strong. However, the LGPD has unique elements distinct from Europe's model. It created the National Data Protection Authority to oversee enforcement. It also mandates a valid legal basis for handling sensitive data. Unlike the GDPR, its global scope is narrower. It focuses more on domestic data practices. Overall, the law reflects Brazil's commitment to stricter privacy protections. This fosters trust globally.[12]

Privacy Act – Australia: The Privacy Act is Australia's main law for protecting personal data. It applies to government bodies. It covers certain private sectors, including healthcare and telecommunications. The law oversees how personal data is gathered, used, and shared. It also provides individuals the right to see and correct their data. This fosters accountability across key industries nationwide. The Act provides ways to file privacy complaints.

---

[10] Ben Dooley, 'Navigating Data Privacy Regulations: Comparative Insights into GDPR, CCPA, LGPD, PDPA, and Privacy Act' (*Infocepts Data & AI*, 23 August 2023) <https://www.infocepts.ai/blog/navigating-data-privacy-regulations-comparative-insights-into-gdpr-ccpa-lgpd-pdpa-and-privacy-act/> accessed 18 February 2025

[11] Osman Husain, 'Pipeda v GDPR, CCPA, LGDPA, and Other Privacy Laws' (*enzuzo*, 02 December 2023) <https://www.enzuzo.com/blog/pipeda-v-other-privacy-laws> accessed 18 February 2025

[12] Brazilian General Data Protection Law 2018

However, it differs from the GDPR and CCPA. It does not require mandatory breach notifications. This means organisations might not have to disclose data incidents. Critics argue that this gap weakens transparency or consumer trust. Calls for reforms aim to align Australia's framework with global norms. Government reviews are underway.[13][14]

COMPARATIVE ANALYSIS

These privacy laws share the same goal: protecting personal data. Yet, they differ in scope, enforcement, and requirements. The GDPR and Brazil's LGPD cover any entity handling their citizens' data, wherever it is processed. By contrast, the CCPA usually applies to businesses in California or those meeting revenue thresholds. Australia's Privacy Act applies to government bodies and certain private industries.

Enforcement also varies significantly. The GDPR has authorities like the European Data Protection Board. Brazil's ANPD enforces the LGPD. Meanwhile, the CCPA falls under the California Attorney General. Australia's Privacy Act is supervised by the Office of the Australian Information Commissioner. These different models reflect unique approaches. They impact how organisations maintain compliance and manage personal data in each jurisdiction. Ll frameworks stress transparency, consent, and individual rights. The GDPR imposes strict demands and heavy fines for violations. The CCPA focuses on consumer rights involving data sales. The Australian Privacy Act offers broad guidelines but lacks mandatory breach disclosure. Recognising these similarities and differences is crucial. Global organisations must adapt to varied data protection rules. Effective compliance ensures trust and legal security.

BEST PRACTICES FOR PROTECTING PERSONAL INFORMATION

Protecting personal information is crucial. Our world is data-driven. Strong data protection measures are needed. They ensure compliance with regulations. They build trust with individuals. Laws require privacy safeguards. Companies must invest in security systems. Trust grows when privacy is respected. People feel safe when data is protected. This is

[13] Moses Blessing, 'Comparative Analysis of Data Protection Laws: Learning from Global Best Practices' (2024) Research Gate <https://www.researchgate.net/publication/385139126_Comparative_Analysis_of_Data_Protection_Laws_Learning_from_Global_Best_Practices> accessed 18 February 2025

[14] Anas Baig et al., 'Navigating Privacy Laws: GDPR v Australia Privacy Act' (*Security*, 16 September 2024) <https://securiti.ai/gdpr-vs-australia-privacy-act/> accessed 18 February 2025

essential for businesses and society. Privacy benefits all individuals equally. Key privacy principles guide data protection. Organisations must practice data minimisation. They limit data to its purpose. Consent must be informed and clear. Transparency is required at all times. Data security must be enforced strictly. Users have rights over their data. Emerging technologies shape privacy practices. AI and IoT drive innovation. These principles are vital for a secure digital future.

Data Minimisation and Purpose Limitation: Data minimisation means gathering only the personal data needed. Only necessary information is collected. This principle is central to privacy laws. For example, the GDPR requires data to be adequate, relevant, and limited. It prevents collecting extra details. This approach lowers the risk of breaches. It also helps organisations meet legal standards. By following this rule, companies secure user information. Purpose limitation requires data to be collected for clear reasons. Data must serve explicit, legitimate purposes. It should not be used for other reasons later. This rule ensures data remains safe and stops misuse. Organisations must clearly state why they gather data. Following this principle reduces risks and builds trust. It helps meet legal standards and protects user rights every day.[15]

Informed Consent and Transparency: Clear consent is key. People must know what they agree to. Consent must be freely given. It must be specific. It must be informed and unambiguous. Data processing begins only after consent is obtained. This step is a cornerstone of data protection. It respects individual rights. It builds trust and ensures accountability. It meets legal standards and supports privacy practices. Transparency is essential. Companies must share clear details about data processing. They must use simple language. Information should be accessible to everyone. Clear communication helps individuals make informed choices. This openness builds trust. It also reinforces accountability. Transparency is required by laws like the GDPR. It supports ethical data practices. It ensures that organisations act with integrity and respect always.[16]

Data Security and Breach Notification: Strong data security is a must. It shields personal information. It prevents unauthorised access, changes, or destruction. Companies should use risk assessments and encryption. They must implement strict access controls. Regular

[15] General Data Protection Regulation, art 5
[16] Robb Taylor-Hiscock, 'Understanding the 7 principles of the GDPR' (*onetrust*, 17 May 2021) <https://www.onetrust.com/blog/gdpr-principles/> accessed 18 February 2025

employee training is also required. These measures create a secure environment. They protect sensitive data. Strong security is the first step in data protection. This approach safeguards consumer trust. Prompt breach notification is vital. Affected individuals must be informed quickly. Authorities also need timely alerts. For example, under the GDPR, breaches must be reported within 72 hours. Quick action minimises harm. It allows swift remediation. Companies must have a clear breach response plan. This plan should be tested often. Fast notifications help restore trust. Immediate response limits further damage.[17]

Rights of Data Subjects: Respecting the rights of data subjects is vital. Individuals must have full access to their data. They can request corrections and demand deletion, known as the right to be forgotten. They are entitled to data portability. These rights empower users. Organisations must honour these rights by setting clear, efficient processes that are transparent and fully compliant with data protection laws. Recognising data subject rights builds trust and accountability. Companies benefit from clear guidelines and efficient procedures. Transparent processes ensure individuals know their options and can act on them. By upholding these rights, organisations avoid legal issues. This practice not only complies with regulations but also fosters positive relationships. Such measures protect personal privacy and support a secure digital environment effectively.[18]

Impact of Emerging Technologies: Emerging technologies bring new challenges and opportunities. AI and IoT lead the change. AI systems need large datasets. This need raises privacy concerns. Data minimisation becomes difficult. Purpose limitation is often ignored. New tech pushes data protection to its limits. The call for strong controls grows. Companies must address these issues with urgency and care in our world. Organisations should use privacy by design. They must build security into systems from the start. Data protection principles must guide development. This ensures safeguards are built in early. Such designs lower the risk of breaches. They help companies stay compliant. New tools help manage

[17] 'Guide to the General Data Protection Regulation (GDPR)' (*Information Commissioner's Office*, 02 August 2018) <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed 18 February 2025

[18] 'Principles of Data Protection' (*Data Protection Commission*) <https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection> accessed 18 February 2025

emerging risks. Businesses must adapt their practices. These steps protect both users and data for a safer future.[19]

LEGAL OBLIGATIONS AND RESPONSIBILITIES FOR ORGANISATIONS

Legal Obligations under Recent Privacy Laws: Under GDPR, companies must follow strict rules. They must act lawfully, fairly, and transparently. They must limit data to its purpose and collect only what is needed. They must keep data accurate and secure. Technical and organisational measures are required. Risk assessments for high-risk processing must be done. Fines for non-compliance can reach €20 million or 4% of turnover promptly.[20]

Under CCPA, businesses must inform consumers about the collected data. They must specify the data categories and their uses. They must disclose third parties that receive the data. Consumers can access, delete, or block data sales. Organisations must provide clear opt-out options. Privacy policies need regular updates. Non-compliance results in civil penalties enforced by the Attorney General to ensure fairness immediately.

Role and Responsibilities of Data Protection Officers and Compliance Teams: Under GDPR, appointing a Data Protection Officer is required. This applies to public bodies and organisations that process sensitive data on a large scale. The DPO monitors compliance with data protection laws. They advise on impact assessments. They train staff on privacy obligations. They serve as the contact for authorities. Organisations must give the DPO independence and adequate resources. Compliance teams support the DPO by enforcing privacy measures. They conduct regular audits of data practices. They ensure that processing activities follow legal rules. Their work builds a strong culture of data protection. They help prevent breaches and maintain trust. Through clear policies and training, they guide the organisation. Their role is critical in safeguarding personal data consistently every day.[21]

Internal Governance: Organisations must enforce strong internal governance. They create data protection policies. These policies explain data handling and breach responses. They also set out the data subject's rights. Clear policies guide staff. They help prevent privacy

[19] Nadeem Mustafa, 'Protecting Privacy in the Age of AI, IoT, and Related Technologies' (*Medium*, 04 February 2024) <https://medium.com/illumination/the-impact-of-ai-iot-and-related-technologies-on-our-privacy-e317454e3ad7> accessed 18 February 2025
[20] Guide to the General Data Protection Regulation (GDPR) (n 17)
[21] 'The data protection officer: An overview' (*Data Guard*, 18 June 2024) <https://www.dataguard.com/blog/data-protection-officer-an-overview> accessed 18 February 2025

breaches. Robust internal systems build trust. They ensure accountability and compliance with laws. Solid governance practices protect sensitive information and build a secure foundation for the organisation.

Companies enforce privacy through strict third-party contracts. They require partners to follow data protection laws. Regular audits and assessments are conducted. These reviews help identify risks. They also reduce potential threats. This approach shows a commitment to data security. It builds trust among consumers and partners. Strong contractual clauses and routine audits foster a culture of security and accountability every day.

Liability Issues and Enforcement Trends: Non-compliance with data protection laws causes serious legal and financial problems. Enforcement agencies are now more active. They penalise organisations that do not follow the rules. Under the GDPR, supervisory authorities impose heavy fines. Fines depend on severity, duration, and intent. These measures ensure that organisations take data protection seriously. Such strict enforcement promotes compliance and protects individual privacy rights globally. Recent trends emphasise transparency and lawful data processing. Data subject rights receive focus. Organisations must monitor regulatory updates and adjust practices accordingly. They need to keep privacy policies current. This approach reduces potential liabilities. Companies that maintain robust data protection build trust. Adhering to legal standards is essential for avoiding penalties and ensuring a secure digital environment. Improvement is vital.[22]

CHALLENGES IN THE IMPLEMENTATION AND ENFORCEMENT OF DATA PRIVACY REGULATIONS

New data privacy laws set high standards. The GDPR in Europe leads the way. The CCPA governs U.S. practices. Both laws protect personal data strictly. They force organisations to follow rigorous rules. Companies must secure and manage data carefully. However, enforcing these rules is not simple. Many practical challenges emerge. Businesses must adjust quickly and effectively to stay compliant. Organisations face many challenges. The first is legal complexity. GDPR and CCPA are hard to understand. They require deep legal and technical skills. Many companies struggle to interpret every rule.

[22] Guide to the General Data Protection Regulation (GDPR) (n 17)

This leads to gaps in compliance. Businesses must invest in expertise and training. Clear guidelines are needed to avoid mistakes and protect data accurately and reliably each day without error. Consent management is another challenge. Both GDPR and CCPA demand explicit consent. Companies must inform users. They need reliable systems to record consent. Digital environments make this task harder. Tools must be updated often. Proper planning is crucial. Businesses must design consent methods. This step is key to maintaining trust and ensuring users have full control over their data.[23]

Data privacy laws are hard to enforce uniformly. Regulations vary by jurisdiction. Even the GDPR faces challenges. Each member state handles enforcement differently. This creates gaps and uncertainty. Many data protection authorities have limited resources. They cannot monitor all organisations effectively. Often, the system depends on self-reporting. This reliance may delay or miss violations. As a result, full compliance is difficult to achieve. Voluntary compliance further weakens enforcement. Many frameworks rely on companies to report their breaches. This self-reporting is often slow and unreliable. Some organisations may even hide issues. Without strict oversight, enforcement gaps grow wider. Regulators struggle to verify every claim. The overall system loses impact when companies are left to police themselves. More robust measures and clearer guidelines are needed.

Global data exchange adds extra complexity. Data moves across many borders. Each country sets its own rules. Multinational organisations face a tough challenge. They must navigate diverse legal landscapes. Ensuring compliance across multiple jurisdictions is daunting. National rules often clash. This patchwork of regulations makes secure data management harder. Companies must work hard to meet all requirements at once. National sovereignty deepens the challenge. Local laws can conflict with international data agreements. Some countries require data to remain within their borders. Data localisation mandates force companies to adjust their global strategies. These rules add operational burdens. Organisations must invest in new systems to comply. Balancing local rules with international cooperation remains a persistent struggle for data managers worldwide.

[23] 'Navigating the Impact of GDPR and CCPA on Businesses: Data Privacy Compliance Challenges and Best Practices' (*Concord*, 27 June 2024) <https://www.concord.tech/blog/navigating-the-impact-of-gdpr-and-ccpa> accessed 18 February 2025

CASE STUDIES ILLUSTRATING IMPLEMENTATION AND ENFORCEMENT CHALLENGES

Uber's GDPR Violation: In July 2024, the Dutch Data Protection Authority fined Uber €290 million for a GDPR violation. Uber sent sensitive personal data of European drivers to US servers. This data included account details, location, and criminal and medical records. They did not use safeguards. The practice lasted for two years. Uber did not use standard contractual clauses or approved transfer methods. Uber plans to appeal the decision. They argue their data transfer processes complied with the rules. Uber claims regulatory uncertainty between the EU and the US clouded requirements. They believe their methods met standards, then the company remains determined to challenge the fine. Their appeal will focus on the regulatory context and interpretation of data protection laws and present their case.[24] The company remains determined to challenge the fine. Their appeal will focus on the regulatory context and interpretation of data protection laws and present their case.[25]

Sephora's CCPA Settlement: In August 2022, the California Attorney General announced a settlement with Sephora. The settlement was $1.2 million. Sephora was accused of violating the CCPA. The company did not inform consumers about data sales. It failed to honour opt-out requests. The company did not cure the issues in the required 30 days. The allegations were clear and serious. This is unacceptable. Under the settlement, Sephora must update its online disclosures. It will revise its privacy policy immediately. The company must provide easy opt-out options. New measures must ensure compliance with the CCPA. Sephora is required to improve transparency. This change will protect consumer rights. The settlement is a wake-up call. Companies must respect privacy laws now. It sets a strong example.[26]

These cases show many challenges. Data privacy laws are hard to follow. Organisations face complex rules. Companies operating in many regions struggle. Uber's case highlights international data transfer issues. Legal uncertainty makes compliance difficult. Compliance needs major investments. Legal experts and new technology are required. Smaller companies

[24] 'Dutch SA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US' (*edpb*, 26 August 2024) <https://www.edpb.europa.eu/news/news/2024/dutch-sa-imposes-fine-290-million-euro-uber-because-transfers-drivers-data-us_en> accessed 18 February 2025

[25] *Ibid*

[26] *THE PEOPLE OF THE STATE OF CALIFORNIA v SEPHORA USA, INC.* CGC - 22 - 601380

may struggle with these costs. They bear heavy operational burdens. Every company suffers. Enforcement is uneven across regions. Self-reporting creates gaps.

Regulators vary in capacity. Some bodies struggle with oversight. The California Attorney General set a strong example. The Sephora case shows proactive enforcement. Vigilance is needed to protect consumer rights. Inconsistent enforcement weakens privacy. Regulators must act swiftly. They must ensure fairness. Strong oversight is key for trust. These steps are crucial.

INDIA'S ANSWER TO GLOBAL DATA PRIVACY CHALLENGES

India's Ministry of Electronics and Information Technology released draft rules. They are called the Digital Personal Data Protection (Act) Rules, 2025. They are open for public consultation until February 18. This is a major step. It marks a milestone in India's data protection journey. The rules support the Digital Personal Data Protection Act of 2023. They explain how to put the Act into practice.

An explanatory note was also published. It clears up key points.[27] Under the DPDP Act, companies must report data breaches immediately. They must alert the Data Protection Board of India and notify affected individuals. The Ministry of Electronics and Information Technology has issued draft rules outlining the reporting process. These rules stress prompt notification and set data fiduciary duties.

Public feedback is actively welcomed online until February 18, 2025. Organisations must build strong internal systems. They need tools to detect and report breaches. They must communicate quickly with the Board and affected individuals. They should keep records of all data processing. Failure to comply can lead to heavy penalties. This makes it crucial to follow the prescribed protocols.

Every step is vital for protecting data and ensuring regulatory adherence. The DPDP Act strives for balance. It protects individual privacy while allowing lawful data processing. This approach mirrors global data protection trends. Organisations in India should study the Act. They must learn the draft rules. Familiarity is key for compliance. Participation in public

[27] Supratim Chakraborty and Siddharth Sonkar, 'Decoding India's draft DPDPA rules for the world' (*iapp*, 09 January 2025) <https://iapp.org/news/a/decoding-india-s-draft-dpdpa-rules-for-the-world> accessed 18 February 2025

consultation is encouraged. Adopting these practices will boost trust and ensure responsible data management across all sectors.[28]

FUTURE TRENDS AND POLICY RECOMMENDATIONS IN DATA PRIVACY

Emerging Trends and Technological Impacts on Privacy: AI and ML merge data from many sources. They analyse large datasets. They may re-identify anonymised data. This breaches privacy. IoT devices add many data points. They often lack security. Privacy-enhancing technologies like homomorphic encryption and differential privacy are emerging. They offer secure methods to process data. They reduce personal data exposure. These advancements are crucial for protecting privacy. Indeed.[29][30][31]

Recommendations for Strengthening Legal Frameworks and Enforcement: Adaptive regulatory approaches are key. Shift from rigid rules to outcome-based frameworks. This change adds flexibility. It keeps regulations effective as technology evolves. Global collaboration is vital. Harmonised data protection standards can ease cross-border issues. Regulators must work together. Authorities also need more support. They must have enough resources and power. This boost is essential for strong oversight and compliance.[32]

Role of Non-State Actors in Shaping Future Privacy Practices: Non-governmental organisations play a key role in protecting privacy. They hold companies accountable. They launch legal challenges against violators. They raise public awareness. Their work exposes privacy breaches. NGOs push for transparency. They champion individual rights. Their advocacy drives change. Their efforts influence policy. They are crucial in shaping future privacy practices. Their work remains vital in today's digital world, truly.[33] Businesses also

---

[28] 'Explainer: Draft DPDP Rules 2025 aim to protect citizens' data; here's how you can share feedback before enactment' *The Economic Times* (09 January 2025) <https://government.economictimes.indiatimes.com/news/governance/explainer-draft-dpdp-rules-2025-aim-to-protect-citizens-data-heres-how-you-can-share-feedback-before-enactment/117077685> accessed 18 February 2025

[29] Gábor Erdélyi et al., 'Data Fusion Challenges Privacy: What Can Privacy Regulation Do?' (2021) Cornell University <https://doi.org/10.48550/arXiv.2111.13304> accessed 18 February 2025

[30] Jennifer Huddleston et al., 'Mitigating Privacy Risks While Enabling Emerging Technologies' (*Mercatus*, 24 October 2019) <https://www.mercatus.org/students/research/public-interest-comments/mitigating-privacy-risks-while-enabling-emerging> accessed 18 February 2025

[31] 'Emerging privacy-enhancing technologies: Current regulatory and policy approaches' (2023) OECD Digital Economy Papers, No 351/2023 <https://doi.org/10.1787/bf121be4-en> accessed 18 February 2025

[32] Ellie Graeden et al., 'A new framework for global data regulation' (2023) Cornell University <http://dx.doi.org/10.48550/arXiv.2308.12955> accessed 18 February 2025

[33] Wojciech Wiewiórowski, 'Civil society organizations as natural allies of the data protection authorities' (*European Data Protection Supervisor*, 15 May 2018) <https://www.edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection_en> accessed 18 February 2025

lead in privacy protection. They partner with civil society groups. They develop strong data policies. They ensure responsible data use. They promote clear transparency in data handling. These corporate initiatives foster trust. They encourage ethical practices. Such partnerships set a new standard. Together, companies and civil society drive meaningful change in data protection and privacy norms. Their joint efforts are making a difference.[34] Civil society plays a key role in privacy. They educate the public on privacy rights. They explain the risks of data misuse. They empower individuals with knowledge. Their outreach builds a culture of informed consent. They push for accountability in data practices. This grassroots engagement drives change. It helps shape policies. It ensures privacy remains a priority for everyone. Their influence is both powerful and essential.[35]

CONCLUSION

This research reveals a complex landscape in personal data protection. Privacy laws have evolved rapidly. Modern regulations such as the GDPR, CCPA, LGPD, and Australia's Privacy Act have raised the bar. They impose strict obligations on organisations. Yet compliance remains challenging. Companies face legal complexity and significant resource demands.

Enforcement is uneven, and self-reporting is common. Emerging technologies further complicate matters. Data breaches expose vulnerabilities and erode trust. Robust internal governance is critical. Organisations must adopt adaptive regulatory approaches. Cooperation across borders is essential. Clear consent and transparent practices are key. Non-state actors, including NGOs and private partnerships, play a vital role. Their advocacy drives improvements in privacy practices. This study offers practical insights for policymakers and businesses. Ultimately, protecting personal data builds trust and safeguards individual rights. It creates a safer digital environment. Future reforms must address enforcement gaps and resource limitations for lasting impact.

---

[34] 'The role of the private sector in protecting civic space' (*Chatham House*, February 2021) <https://www.chathamhouse.org/sites/default/files/2021-01/2021-01-29-private-sector-protecting-civic-space-freeman-et-al.pdf.pdf> accessed 18 February 2025

[35] 'Civil Society Organizations and General Data Protection Regulation Compliance Challenges, Opportunities, and Best Practices' (*Open Society Foundations*, 16 December 2019) <https://www.theengineroom.org/wp-content/uploads/2020/02/GDPR_Report-2019_12_16.pdf> accessed 18 February 2025