manupatra®

A Comparison of Data Privacy frameworks across different Countries

www.manupatra.com

A Comparison of Data Privacy frameworks across different Countries

Key Acts

Country	Key Acts
India	The Digital Personal Data Protection Act, 2023
UK	The Data Protection Act, 2018
EU	General Data Protection Regulation, 2016
Australia	The Privacy Act, 1988
Japan	The Act on the Protection of Personal Information, 2003
USA	Health Insurance Portability and Accountability Act, 1996; The California Consumer Privacy Act of 2018; The California Privacy Rights Act, 2020; Children's Online Privacy Protection Act, 2000
China	The China Personal Information Protection Law, 2021
Canada	The Privacy Act, 1983; Personal Information Protection and Electronic Documents Act, 2000

A Comparison of Data Privacy frameworks across different Countries

Consent & Notice

Country	Consent & Notice
India	Data fiduciaries must provide data principals with a notice before or during the time of obtaining consent for processing of personal data
UK	Organisations must inform the concerned individual whenever they want to collect/ process personal data and obtain consent
EU	Organisations must inform the concerned individual whenever they want to collect/ process personal data and obtain consent
Australia	Organisations must inform the concerned individual whenever they want to collect/ process personal data and obtain consent including implied consent
Japan	Handling Operators are required to obtain the consent of the principal barring statutory exceptions
USA	• It differs by state. The CCPA and CPRA focus on transparency and the right to opt out of data sales but generally do not require explicit consent for most data processing • Businesses must inform individuals about their data collection practices
China	• PIPL requires that personal information be collected and processed with explicit consent • Information handlers are required to provide clear notices to data subjects
Canada	Organizations are required to obtain informed consent

A Comparison of Data Privacy frameworks across different Countries

Consent Manager

Country	Consent Manager
India	Mechanism to create "Consent Managers" that offer data principals a platform to give, manage, review, and withdraw their consent provided to data fiduciaries
UK	The regulations only outline Controllers and Processors of personal data. No provision recognising Consent Managers
EU	The regulations only outline Controllers and Processors of personal data. No provision recognising Consent Managers
Australia	The regulations only outline Organisations and Agencies. No provision recognising Consent Managers
Japan	No provision recognising Consent Managers
USA	• No formal requirement for a centralized consent manager at the federal level • CPRA and similar state laws include provisions that allow users to manage consent through preference management systems
China	The PIPL does not explicitly establish a Consent Manager, however, regulations promote the use of digital platforms to manage consent.
Canada	No provision recognising Consent Managers

A Comparison of Data Privacy frameworks across different Countries

Data Security

Country	Data Security
India	Consent Managers and Data Fiduciaries are required to adapt reasonable and appropriate data protection measures and mechanisms
UK	Controllers and Processors must adapt appropriate technical and organisational measures (encryption, access controls, backup, etc.) to ensure a level of security appropriate to the risks arising from the processing of personal data
EU	Controllers and Processors must adapt appropriate technical and organisational measures (encryption, access controls, backup, etc.) to ensure a level of security appropriate to the risks arising from the processing of personal data
Australia	• There are no specific security measures outlined by the Privacy Act • Entities are expected to take reasonable steps (practices, procedures and systems) to ensure compliance with Australian Privacy Principles (APPs)
Japan	• Handling Operators are required to take necessary and proper measures to prevent leakage, loss or damage, and for other security control, of personal data • These include "Systematic Security Control Measures", "Human Security Control Measures", "Physical Security Measures" and "Technical Security Control Measures"
USA	U.S. laws (such as the CCPA and HIPAA) mandate that businesses adopt reasonable security measures
China	The PIPL mandates that personal information handlers enforce stringent security measures to protect personal data, including technical safeguards like encryption, access controls, and cybersecurity monitoring
Canada	Organizations must take extra care when collecting, using, and disclosing certain types of personal information, such as health information and financial data

A Comparison of Data Privacy frameworks across different Countries

Cross Border Transfer of Data

Country	Cross Border Transfer of Data
India	Personal data can be transferred outside the country unless such country is blacklisted by the appropriate authority or such database is prohibited from being transferred
UK	Personal data can be transfered in line with the notified regulations unless such category of personal data is restricted by the Secretary of State
EU	• Organizations within the EU can transfer personal data to other EU member states as long as they comply with the general data protection principles, and establish a data processing agreement (DPA) • Data can be transferred to third countries/ organisations provided appropriate safeguards have been undertaken, including Binding Corporate Rules (BCR) and Standard Contractual Clauses (SCCs)
Australia	• Privacy Act allows cross border transfer of data • Safeguards need to be taken when the transfer is being done to a country that is not 'adequate' to ensure the overseas recipient does not breach the APPs • Data Subjects can provide consent after being expressly informed of such transfer
Japan	• Transfers of personal data to third countries is permissible if they are approved adequate/whitelisted jurisdictions • Apart from the general requirements for third party transfer, prior consent of data subjects specifying the receiving country is required for transfers to third parties in foreign countries • Organisations must execute a data transfer agreement or an internal rule which provides obligations equivalent to those provided under the APPI
USA	U.S. laws generally do not impose direct restrictions on cross-border data transfers
China	The PIPL enforces strict rules on cross-border data transfers, allowing them only if the destination country provides adequate data protection, similar to the GDPR
Canada	• Organizations storing personal information outside Canada must ensure that the personal information is protected in accordance with PIPEDA • Individuals must be notified if their data is to be transferred outside Canada

A Comparison of Data Privacy frameworks across different Countries

Data Breach

Country	Data Breach
India	Data breaches must be notified to the Data Principals and the Board immediately upon becoming aware of the breach without delay. A detailed report needs to be submitted to the Board within 72 hours
UK	• Data breaches must be notified to the Commissioner "without undue delay" but within 72 hours. Detailed report must be provided within 72 hours. If the timeline is not feasible, the information must be provided in batches without undue further delay. • Processors must notify Controllers without undue delay after becoming aware of a personal data breach. • Data subjects are only to be notified if the data breach is likely to result in a high risk to the rights and freedoms of the individuals "without undue delay"
EU	• Data breaches must be notified to the Superviory Authority "without undue delay" but within 72 hours for breaches that result in a risk to the rights and freedoms of natural persons. Detailed report must be provided within 72 hours. If the timeline is not feasible, the information must be provided in batches without undue delay. • Processors must notify Controllers without undue delay after becoming aware of a personal data breach. • Data subjects are only to be notified if the data breach is likely to result in a high risk to the rights and freedoms of the individuals "without undue delay"
Australia	• Eligible Data Breaches must be notified to the affected individuals and the Office of the Australian Information Commissioner (OAIC) • Individuals need not be notified when the risk of any serious harm can be mitigated before any serious harm is suffered by the individuals
Japan	• "Data Breach" is not used by the Act • Certain Reportable Incidents related to leakage, loss, and damage to personal data must be reported to the PPC if it involves sensitive personal information, affect over 1,000 individuals, or result from unlawful access • Non-material data breaches must be reported to the Financial Services Agency • Breaches must be notified to principals unless such communication is difficult and an alternative measure has been taken • A preliminary report must be filed with the PPC without delay with a final report within 30 days
USA	Most U.S. states require businesses to notify affected individuals and, in some cases, state authorities within 30-60 days of a data breach. Federal laws like HIPAA and Gramm-Leach-Bliley also impose specific breach notification requirements
China	• The PIPL mandates that personal information handlers notify authorities and affected individuals of a data breach within 72 hours, with some flexibility depending on the breach's severity • It must also inform affected individuals of their rights to take protective actions
Canada	The OPC, affected individuals, and relevant third parties must be notified of any breaches of security safeguards that pose a real risk of significant harm

A Comparison of Data Privacy frameworks across different Countries

Personal Data of Children and Persons with Disabilities

Country	Personal Data of Children and Persons with Disabilities
India	Data Fiduciaries need to develop mechanisms to obtain verifiable consent from the from the parent or legal guardian of children and persons with disabilities
UK	• Personal data of Children and individuals with disabilities can be processed without their consent where such specific processing is necessary as per outlined in the statute and is required for substantial public interest. • A Parent or Guardian must provide for consent for a child below the age of 13 years for a “information society service” (social media services, online gaming and web-based voice, video and text messaging, etc.)
EU	• Personal data of Children and individuals with disabilities can be processed without their consent where such specific processing is necessary as per outlined in the statute and is required for substantial public interest. • A Parent or Guardian must provide for consent for a child below the age of 16 years for a “information society service” (social media services, online gaming and web-based voice, video and text messaging, etc.). However, member states can lower the age of consent to 13 years
Australia	• A Parent or Guardian must provide for consent for a child below the age of 15 years • If an individual cannot provide meaningful consent due to a disability, consent must be obtained from a legal guardian or authorized representative.
Japan	• If a principal below the age of 18 years does not have the capability to provide informed consent, consent must be obtained from parent or guardian • If an individual with a disability cannot provide meaningful consent due to cognitive or physical impairments, consent must be obtained from a legal guardian or authorized representative
USA	• Parental/ Guardian consent is required for the collection or use of any personal information of children below 13 years of age • Individuals with disabilities or their lawful representatives (e.g., guardians) must provide informed, written consent.
China	• Parental/ Guardian consent is required for the collection or use of any personal information of children below 14 years of age • If an individual with a disability is unable to provide meaningful consent, consent may be obtained from their legal guardian or representative.
Canada	• Parental/ Guardian consent is required for the collection or use of any personal information of children below 13 years of age • Parental/ Guardian consent is required for the collection or use of any personal information of persons with disabilities who cannot provide consent due to their disability

Penalties

Country	Penalties
India	Up to ₹250 Cr
UK	Up to £17.5 million or 4% of global annual turnover
EU	Up to €20 million, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding fiscal year, whichever is higher
Australia	• Up to AU$ 2.5 million per contravention for individuals and small businesses • Up to AU$ 50 million or 30% of adjusted annual turnover or 3 times the benefit obtained from the breach
Japan	• Up to ¥100 million for companies. • Up to 6 months imprisonment or ¥300,000 for individuals.
USA	• Health Insurance Portability and Accountability Act (HIPAA): Civil Penalties: Tiered system ranging from $100 to $50,000 per violation, with an annual maximum of $1.5 million per type of violation. Criminal Penalties: Fines up to $250,000 and imprisonment for up to 10 years for deliberate violations. • CCPA: Civil penalties of up to $2,500 per violation or $7,500 per intentional violation • CPRA: Up to $7,500 per affected minor
China	Up to CN¥ 50 million or 5% of the preceding year's turnover, in addition to potential suspension or revocation of business operations
Canada	• Up to Can$ 100,000 per violation • Quebec's Bill 64 (Law 25) allows fines up to Can$ 25 million or 4% of global turnover

Governing Body

Country	Governing Body
India	Data Protection Board of India
UK	Information Commissioner
EU	• Independent Supervisory Body at the Member States level • European Data Protection Board on the European Union level
Australia	Office of the Australian Information Commissioner
Japan	Personal Information Protection Commission
USA	Federal Trade Commission (FTC) or State Attorney Generals
China	Cyberspace Administration of China
Canada	Office of the Privacy Commissioner of Canada