Jurisdiction	Law	Enforceable?	Applicability	Data Breaches	Collection Requirements	Data Uses	Corporate Safeguards	Data Transfers	Consumers Rights	Penalties
New Zealand	Privacy Act 2020	Yes	Applies to data handlers in New Zealand and offshore organizations that collect data from New Zealanders	It is mandatory to report breaches to the Privacy Commissioner and any impacted customers if they have the potential to cause "serious harm," such as leaking outside the organization or risking identity theft.	Data must be collected in a fair, lawful and non-intrusive way. Data may usually only be collected directly from the subject.	Typically, data can only be collected for a purpose related to providing a good or service to the subject. Once collected, organizations may only use data for that purpose, keeping it no longer than necessary.	Organizations must have "reasonable safeguards" against data misuse, including encryption or limiting the amount of employees with access to consumer data. Privacy officers must be appointed to oversee compliance and handle any privacy issues.	Data may only be transferred to a jurisdiction with equivalent privacy regulations, except in the case of overseas cloud companies that merely store the data.	Access and correct personal data Transparency about the purposes of data collection, the location of any data transfers, and any consequences for choosing to opt-out of data collection.	Unreported breaches can be fined at around $7,000 per breach. In some cases, the Privacy Commissioner may file a complaint with the Human Rights Tribunal, with fines of up to $162,000.
Brazil	General Data Protection Law (LGPD)	Yes	Applies to any personal data processing operation in Brazil, of subjects located in Brazil or for the purpose of providing goods and services to individuals in Brazil.	Organizations must make an effort to prevent any breaches or unlawful processing. In the case of a breach that puts subjects at risk, organizations must notify Brazil's data protection authority and impacted individuals.	Organizations must have a "lawful basis" for processing data, such as clear and informed consent from subjects, the necessity of collection for the subject's safety, or contractual obligations to process data when the subject is a party in the contract.	Data can be collected if it fulfills the "legitimate interests" of a collector or third-party, as long as this is not outweighed by the harm to the subject's rights or liberties. Data that reveals "sensitive personal information" about the subject-- such as race or political beliefs-- may only be collected in the interests of legal obligation or the subject's safety.	Companies must hire a Data Protection Officer responsible for data processing operations and accountable for any violation of LGPD. Records of processing activity and data impact assessments are required.	Data may only be transferred to a jurisdiction with an "adequate level of protection". In other cases, controllers must use standard contractual clauses (SCCs).	Withdraw consent Access, correct and delete personal data Transfer their data for one organization to another (data portability) Know information about the purpose, type, and duration of data processing, with access to the controller's identity and contact information. Access records of third-party transfers	Maximum of $8.866 million, enforceable only after August 2021
Canada	Consumer Privacy Protection Act (CPPA)	No. Currently just a bill, with the Personal Information Protection and Electronic Documents Act (PIPEDA) acting as Canada's effective data privacy law.	Applies to data activity by organizations carrying out business in Canada unrelated to the handling of employee information.	For breaches where there is "real risk of significant harm," companies are obliged to report to the privacy commissioner and affected individuals as soon as possible. Companies are also required to notify other organizations with the ability to mitigate harm.	Organizations can not ask individuals to consent to data use beyond what is necessary for the organization's purposes.	Subjects must give clear and informed consent prior to any data practices. Exceptions to this rule include when data collecting is necessary for delivering a product or service, reducing commercial risk or ensuring network security. Organizations can collect without consent if it is impossible to communicate with the subject or discern their identity from the data.	Controllers with a substantial amount of data must create a privacy management program, formalizing all compliance policies and procedures. Such policies must be accessible by the Canadian privacy commissioner upon request. Organizations are required to de-identify any data they hold.	No restriction to the transfer of personal information outside of Canada.	Withdraw consent Access, correct and delete personal data Transfer their data for one organization to another (data portability) Sue for damages resulting from a failure to comply Know how automated decision-making algorithms have been used to make decisions about them	Up to $19.2 million, or 5 percent of the violators global revenue.

Dubai	DPL 2020	Yes	Applies to Dubai-based businesses as well as any offshore business with a consistent processing relationship with subjects from Dubai	Must notify privacy commissioner and impacted subjects in the case of a breach that puts consumers at risk.	Must be collected for a specific purpose, to a degree that is not excessive given that purpose. If the legal basis for processing has passed, personal data can only be kept in encrypted or anonymized form.	Data must be processed fairly, lawfully and securely. The subject must actively express consent. It is the collector's responsibility to assess the ongoing validity of the subject's consent. If deemed invalid, the subject must reaffirm their consent for the processing to continue.	A Data Protection Officer is mandatory for companies that take part in "high-risk" processing activities-- such as collecting a high volume of data or sensitive personal information like race and health, as well as creating profiles of consumers based on data.	Transfers are allowed to jurisdictions with an adequate level of protection. Transfers to other jurisdictions are allowed if there is a legally binding contract in-place to ensure compliance with DPL.	Withdraw consent Access, correct and delete personal data Object to certain processing practices, like automated decision making and profiling Transfer their data for one organization to another (data portability) Sue for damages resulting from a failure to comply Not be discriminated against when exercising their data privacy rights	Maximum of $100,000 for an administrative breach, with unlimited fines for more serious violations.
Japan	Act on the Protection of Personal Information (APPI)	Yes, with amendments enforceable in Spring 2022	Applies to any organization that obtains personal information from data subjects in Japan	Breaches of a large scale or ones with the potential to violate subjects' rights must be reported to the privacy commissioner. Two reports must be sent: one announcing the situation and another detailing the causes of the breach and the plan to deal with it.	Organizations are required to publish the purposes of data use. Organizations may not use personal data in unlawful and excessive ways.	Consent is only required for data uses involving sensitive personal information or transfers to third-parties.	In high-risk cases, organizations must take security measures to avoid data misuse. These can include appointing an employee to be in charge of data privacy, staff training, area access control or encryption.	Expressed consent from the subject is mandatory for any third-party transfers When consent is given, organizations must ensure that the third-party uses the data in compliance with APPI.	Access, correct and delete personal data in cases when their personal interests are at risk, when the collector has obtained the data through improper means or used in ways beyond what the purposes of collection call for Call for the cessation of data use and provision to third parties when the data is not "pseudonymized" Access all records of third-party transfers of their data Choose how records of their personal data will be sent to them	Violations carry a penalty of up to $944,000. Falsifying a report to the privacy commissioner carries a fine of up to $4,700. Individuals found responsible for a breach could face a fine of $9,400 and a year in prison.
California	California Consumer Privacy Act (CCPA)	Yes	Applies to any company that earns at least half its revenue by selling the personal data of Californians, handles the data of over 50,000 California individuals, or collects over $25M in revenue	Consumers have a private right of action. They can seek damages in the case of data breaches where companies failed to implement reasonable security measures.	Companies may not use data for "materially different" purposes than disclosed at collection.	Customers must be notified when their data is being collected, at or before the time of collection. The notice of collection must be clear, concise, comprehensive and accessible, including the categories of personal	No directly imposed data security requirements	No restrictions on cross-border data transfers	Know what personal data is being collected, stored or sold Access or delete personal data Opt-out of data collection and sale	$2,500 for unintentional and $7,500 for intentional violations. Consumers can sue for damages between $100 and $750 for breaches. Organizations have a 30-day period where they can "cure" any violation to avoid enforcement.

						data collected and the purposes of collection.			Not be discriminated against when exercising their data privacy rights	
California	California Privacy and Enforcement Act (CPRA)	Yes	Applies to any company that earns at least half its revenue by selling or sharing the personal data of Californians, handles the data of over 100,000 California individuals, or collects over $25M in revenue	Consumers have a private right of action. They can seek damages in the case of data breaches where companies failed to implement reasonable security measures.	Companies may not use data for purposes other than those disclosed at collection, retaining the data for no longer than necessary.	Customers must be notified when their data is being collected, at or before the time of collection. The notice of collection must be clear, concise, comprehensive and accessible, including the categories of personal data collected and the purposes of collection. Subjects must "opt-in" to the sale of any personal data that is not publicly available	No directly imposed data security requirements	No transfers to third-parties for any purpose other than to provide a good or service. If consumers requests deletion, organization must request the deletion from any third-party they shared the data with	Know what personal data is being collected, stored or sold Access, delete or correct personal data Opt-out of data collection, sale or use for marketing and advertising Not be discriminated against when exercising their data privacy rights Opt-out of data collected by automated decision making technology, such as profiling	$2,500 for unintentional and $7,500 for intentional violations. Consumers can sue for damages between $100 and $750 for breaches. $7,500 fine for unintentionally breaking any law concerning the sale or collection of a child's data Organizations have a 30-day period where they can "cure" any violation to avoid enforcement.
European Union (EU)	General Data Protection Regulation (GDPR)	Yes	Applies to EU-based and offshore organizations that process data of EU-individuals while offering them products or monitoring their behavior.	Organizations must notify authorities and impacted subjects within 72 hours of discovering a breach, unless it is judged to pose little risk to data subjects.	Companies can only collect data for a clearly stated purpose, keeping it no longer than necessary. They must process only the data necessary for that purpose.	Companies are required to be transparent with subjects about the data they collect and the reason they collect it. Consent from data subjects must be clear, voluntary and informed.	Companies must hire a Data Protection Officer (DPO) if data processing is part of their core operations or they process certain types of data on a large-scale. There is a vaguely-defined requirement to use organizational measures, like encryption or pseudonymization, to protect data from security threats.	Cross-border transfers are only allowed to jurisdictions judged by the EU to have an "adequate level" of data protection. Other data transfers, using standard contractual clauses and binding corporate rules, may be allowed if offshore organizations can guarantee an adequate level of data protection.	Access, correct and delete personal data Restrict processing, under certain circumstances Transfer their data for one organization to another (data portability) Not be evaluated on the basis of automated processing Withdraw consent at any time	Up to the greater of $24 million or 4% of an organization's global revenue in the prior year
New York	Stop Hacks and Improve Electronic Data Security (SHIELD) Act	Yes	Applies to employers in New York or any business that holds personal data of New York residents.	For breaches involving the unauthorized access or acquisition of personal information, organizations must notify impacted customers and the Attorney General's office. Consumer reporting agencies must be	None	None	An organization will be in compliance if it implements a data program with "reasonable safeguards". These safeguards can be administrative (designating employees to coordinate the program, training	None	None	The greater of $5,000 or $20 per instance for inadvertent breach notification violations, with a cap of $250,000. Maximum penalty for reasonable safeguard violations is $5,000.

				notified if more that 5,000 New York residents are impacted. For inadvertent breaches unlikely to result in the misuse of information, companies must maintain documentation of the incident for 5 years, only notifying the Attorney General if more than 500 New York residents are impacted.			employees on security best practices), technical (assessing risks in software, network and IT design), or physical (preventing and responding to unauthorized access of data).			
New York	New York Privacy Act (NYPA)	No	Applies to all entities that conduct business in New York state or produce products intentionally targeted to New York residents.	Organizations must reasonably secure personal data from unauthorized access, notifying any impacted customers in the case of a breach.	Organizations may not use data for self-benefit at the expense of the data subject.	Consumers must opt-in to any data activity, voicing clear, informed and freely given consent.	Every entity that provides, sells or licenses personal information of consumers is obliged to exercise the "care, loyalty, and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk."	Organizations may not disclose, share or sell personal data to a third-party that doesn't adhere to the standards of NYPA.	Correct, restrict processing of, and delete personal data Pursue civil remedies when injured due to a violation of NYPA, limited to actual damages Access information about what personal data that is processed, if it has been sold to brokers or any third parties it has been shared with	Violators are subject to injunctions or civil penalties determined by the courts on a case-by-case basis.
New York	Biometric Privacy Act (BPA)	No	Applies to the use of biometric data that can reveal the identity of its subjects, including fingerprints, voiceprints, and scans of hands, faces or eyes.	None	Companies must inform the subject of the purpose and length of data activity and the subject must sign a release consenting to the use of their data.	Companies must dispose of data once the initial purpose for collection has been satisfied or within three years of their last interaction with the subject, whichever comes first.	Companies must keep clear retention schedules for data, including guidelines for how to destroy the data when necessary.	Companies may not profit from biometric data unless the subject consents, unless the action is necessary to complete a transaction authorized by the subject.	Recover damages for each violation.	For negligent violations, customers are entitled to the greater of $1,000 or the actual damages incurred. For intentional or reckless violations, the minimum payout is $5,000. Guilty parties are also expected to cover the legal costs of those involved.

Washington	Washington Privacy Act (WPA)	No	Applies to organizations that conduct business in Washington; any company that targets its products or services to Washington residents and processes the personal data of over 100,000 Washington residents annually; any company that makes over 25 percent of their revenue from selling personal data and processes the personal data of over 25,000 Washington residents annually	None	Companies must issue a readable and accessible privacy notice informing consumers of how their data will be used, including purposes, data categories, if the data is used for profiling, and who the data will be shared with Companies can not collect sensitive personal data (such as ethnicity, religion or sexual orientation) without consent from the subject	Companies may not use data for a purpose not listed in the privacy notice without consent from the subject	Data controllers are obliged to conduct impact assessments for any data activity that poses a substantial risk of harm to consumers. Such assessments must be accessible by the Attorney General upon request	To do business with a data controller, data processors would have to enter a binding written agreement with the controller on the types of data processed, the purpose for and duration of processing activity, and corporate safeguards.	Correct and delete personal data Know what personal data is being collected, stored or sold Transfer their data for one organization to another (data portability) Be informed of their rights through a privacy notice Opt-out of data collection if the data is used for targeted advertising and profiling decisions, or if it is sold to third-parties Seek damages for data misuse involving private health emergencies	The Attorney General may impose penalties and take preventative measures against future violations. The sizes of the penalties are left ambiguous.
India	Personal Data Protection Bill	No	Applies to companies that; are based in India; process data that has been collected, shared or processed within India or for the purpose of offering goods or services to Indian citizens; profile individuals in India	Companies must notify the data protection authority of breaches as soon as possible if they are likely to cause harm to individuals	In most cases, companies may only collect data after obtaining consent that is free, informed, specific, clear and capable of being withdrawn	Data must be processed for a legitimate, lawful purpose and only to the extent necessary for that purpose. Once the purpose has been fulfilled, the data should be deleted.	Companies are required to implement Privacy By Design policies internally, including security safeguards, transparency about processing activities, and data breach reports. Fiduciaries are required to undertake an impact assessment in cases that carry a risk of harm, such as the use of new technologies or sensitive data. A copy of all sensitive and critical personal data from Indian citizens must be stored within the country's borders	Data can only be transferred offshore into jurisdictions that match India's privacy protections. Sensitive personal data may only be transferred offshores if it is in accordance with a contractual clause, transferred by a country or international organization, or deemed necessary by the data protection authority.	Correct and delete personal data Know what personal data is being collected, stored or sold Transfer their data for one organization to another (data portability)	The greater of INR 50 million ($685,590) or 2 percent of their worldwide turnover in the preceding fiscal year for failing to adhere to obligations The greater of INR 150 million ($2.1 million) or 4 percent of their turnover for contraventions involving the processing of personal or sensitive data, cross-border transfers or adherence to safety standards. A fine of up to INR 20,000 ($2740) or three years in prison for re-identifying previously encrypted or anonymized data without the consent of the subject, fiduciary or processor.

Virginia	Consumer Data Protection Act (CDPA)	No	Applies to businesses that conduct business in Virginia or target Virginia residents if they control or process data of over 100,000 consumers or control or process data of over 25,000 consumers, and derive over half of their gross revenue from selling personal data	N/A	Controllers must obtain consent from the subject in order to collect data beyond what is necessary for the purposes disclosed to the consumer Sensitive data can not be processed without the subject's consent	Businesses must make a privacy notice accessible to consumers detailing the purposes for each category of data activity. Without consent from the subject, they can only use data to fulfill these purposes.	Organizations must establish administrative, technical and physical safeguards to protect consumer data. This includes entering into a contract with any processor establishing duties of confidentiality, to delete data upon their request and cooperate with any compliance assessments, and taking measures to ensure that deidentified data can not be reidentified When processing data for targeted advertising, profiling or sale, controllers must conduct and document a data protection assessment that weighs the benefits of data activity against the risk of harm to the consumer, as well as safeguards to mitigate the risk.	In the privacy notice, organizations must state the categories of third parties consumer data is shared with and the categories of data shared with third parties	Access, correct and delete personal data Transfer their data for one organization to another (data portability) Opt-out of data sale or data activity related to targeted advertising or profiling Submit up to two request per year for no fee	Up to $7,500, if violations are not cured 30 days after notice from the attorney general
Minnesota	HF 36	No	Applies to any company that earns at least half its revenue by selling the personal data, handles the data of over 50,000 consumers, or collects over $25M in revenue. Any company that is controlled by or shares common branding with an organization that meets the criteria will also be subject to the regulations	N/A	In order to collect personal information, organizations must provide a notice upon collection or sale including the categories of data collected and the purposes of collection	Organizations may not go beyond any of the purposes or categories listed in the initial notice without providing an additional notice to the consumer.	N/A	Consumers must be notified before their data is sold to a third party. This notice must include the categories of third parties that receive the data and the purpose for the sale. Data may not be sold in a way that deviates from the notice without an additional notice. The notice upon collection must include the categories of any third-parties the data is disclosed to, including the purpose of disclosure. Additional consent is needed to	Access and delete personal data Opt-out of sale or onward transfers of their personal information Opt-in to data sale, if aged 16 or under Request information on the source of their personal information, the purpose of collection and any third parties or service providers it has been shared with Personal information provided to consumers must be in a readable format that they can	Penalties enforced by the attorney general are yet to be specified, but these will include litigation costs Impacted individuals are entitled to the greater of actual damages or punitive damages between $100 or $750 per violation

								transfer data to third parties that aren't listed.	transfer to another entity (data portability) Not be discriminated against for exercising their data privacy rights Sue for damages resulting from a failure to comply	
Florida	HF 969	No	Applies to for-profit businesses that do business in Florida, make over $25 million in global annual gross revenue, collect personal information about consumers and determine how the personal information will be processed as well as for-profit companies that buy or receive the personal data of over 50,000 consumers, households or devices, or derive 50% or more of their revenue from selling or sharing personal data. Any company that is controlled by or shares common branding with an organization that meets the criteria will also be subject to the regulations.	Consumers have a private right to action, allowing them to seek statutory damages after being harmed by a data breach resulting from a violation of the law.	In order to collect personal data, organizations must create an easily-accessible privacy policy and a just-in-time notice upon or before collection that details the categories of data collected and the purposes of collection.	Organizations may not conduct any data activity beyond what is detailed in the notice without sending an additional notice to the consumer	Organizations must create a retention schedule. Personal data may not be retained after the initial purpose is satisfied, the contract with the consumer ends or one year passes since the consumer's last interaction with the organization	Data can not be transferred to a third-party unless consumers are given the opportunity to opt-out	Access personal data collected from them including information on the source of the data, the purposes of collection and the categories of third-parties with which it is shared. Consumers may exercise this right twice a year, free of charge. Delete personal data except for when the data is needed to obey a law, complete a transaction with the consumer or when the data use is "compatible with the context in which the consumer provided the information." Opt-out of sale or disclosure of their personal data to third-parties Opt-in to data sale, if aged 16 or under Personal information provided to consumers must be in a readable format that they can transfer to another entity (data portability) Not be discriminated against for exercising their data privacy rights	Up to $2,500 for unintentional violations and $7,500 for intentional violations, if violations are not cured within 30 days of notice Consumers that successfully exercise their private right to action will be entitled to the greater of statutory damages between $100 and $750 or actual damages as well as injunctive or declaratory relief.
Texas	HB 3741 and HB 3746	No	Applies to for-profit businesses that do business in Texas, have over 50 employees and collect the identifiable personal information on over 5,000 individuals,	When reporting data breaches involving over 250 Texas residents to the Attorney General, organizations must do so within 60 days	Businesses are obligated to provide a notice that details the categories of information processed, the type of processing used by the business,	Businesses are obliged to stop processing the data of individuals who close their account with the business and permanently delete the information no later	N/A	N/A	Know what personal information has been collected from them, the source of the information, the purpose of collection and any third parties the	Up to $10,000 per violation at a maximum of $1 million in total

			households, or devices that earn over $25 million in annual gross revenue or derive 50 percent or more of their revenue from processing personal data.	of identifying the breach detailing the nature, circumstances and magnitude of the breach as well as details involving the personal information compromised, the measures that have been taken and whether law enforcement has investigated the breach	the purposes for processing, and any involvement of a third-party in the processing	than a year after the account is closed			data has been transferred or sold to Correct and delete personal data Obtain a copy of the data in a readable format that consumers can transfer to another entity (data portability) Enter a contractual agreement with a business allowing the continuous transmission of their personal information for the businesses' monetization, customer relationship management or identification purposes	
USA (Federal)	Information Transparency and Personal Data Control Act	No	Applies to controllers, processors and third-parties involved in the use of personal data	N/A	Organizations that collect, transmit, store, process, sell or share sensitive personal data must inform consumers of their practices through a privacy and data use policy	Organizations must obtain consent from the subject before any data activity involving sensitive personal information Organizations must use personal data in ways that "are consistent with the context in which the consumers provide the data"	Entities that use sensitive information pertaining to 250,000 or more consumers must obtain an audit from an objective, independent and qualified third-party at least once every two years. This audit should determine whether the entity was found compliant, a decision that shall be made publicly available.	Controllers and processors must honor opt-out requests and communicate the request to any third-party they disclosed the data to. If the third-party fails to comply, the controller is not liable	Access and correct personal data Obtain a copy of the data in a readable format that consumers can transfer to another entity (data portability) Opt-in to activity involving sensitive personal data Opt-out of activity involving non-sensitive personal data	This act will be enforced by the FTC. In the case of a non-willful violation, the FTC will notify the violator and provide them with 30 days to cure it. If no enforcement action is taken by the FTC, a state attorney general may bring an action if a violation of the act is alleged to affect the state or its residents, providing written notice of the action to the FTC.
Utah	Utah Consumer Privacy Act (UCPA)	No	Applies to any controller or processor that conducts business in Utah or targets their product or service to Utah residents, if they control or process the personal data of 100,000 consumers during a calendar year or those that control and process the personal data of over 25,000 consumers, if they derive over 50% of their gross revenue	N/A	Controllers must provide a clear and accessible privacy notice to consumers detailing the categories of data processed and shared with third-parties, the purpose for processing, any third-parties the data is shared with and how they can exercise their data rights.	A controller may only collect data without consent if the collection is relevant to the explicitly stated purposes. Sensitive personal data-- race, religious beliefs, sexual orientation, health condition, immigration status-- may not be processed without the subject's consent.	Organizations must maintain technical, administrative and physical data security practices to protect the confidentiality of personal data and foresee risks of harm to consumer privacy. These security practices must be appropriate to the volume and nature of personal data involved.	N/A	Access, correct and delete personal data Confirm whether their data is being processed and obtain information on the categories of data that has been collected from them Obtain a copy of the data in a readable format that consumers can transfer to another entity (data portability)	Up to $1,000 per consumer per violation, or actual damages to consumers

			from the sale of personal data.				Annual data protection assessments must be conducted for the sale of data, processing of personal data for purposes of targeted advertising, and processing for the purpose of profiling, if the profiling poses a risk of deceiving or injuring the consumers. Any data activity that presents a heightened risk of harm to the consumer, including the processing of sensitive personal data, must be assessed as well.		Opt-out of data sale or use of personal data for targeted advertising or certain types of profiling Not be discriminated against for exercising their data privacy rights	
North Carolina	Consumer Privacy Act of North Carolina (CPA)	No	Applies to businesses that do business in North Carolina or target North Carolina residents that control or process the personal data of over 100,000 consumers or control or process the personal data of at least 25,000 consumers and derive over 50 percent of its gross revenue from the sale of personal data	N/A	Controllers must provide consumers with a privacy notice that includes the categories of data processed or shared with third-parties, the purpose for the processing, the categories of third-parties with whom the data is shared, one or more methods consumers can use to exercise their rights, and how consumers can appeal a denied request	Controllers must disclose the purposes for data activity to consumers, and can not collect data beyond what is necessary for those purposes without the consumer's consent.	Controllers must conduct data protection assessments' at least once a year for any processing activity for the purposes of targeted advertising, sale or profiling, or any activity that presents "a heightened risk of harm to consumers" or involves sensitive data. For any processing activity, a binding contract must be put in place between the controller and processor establishing the instructions for the processing, the purpose and duration of the activity, and the type of data involved.	N/A	Know if a controller is processing their personal data Access any personal data a controller has processed from them Correct inaccuracies in their data Delete any data provided by or obtained about them Obtain a portable copy of their data in a usable format that they can transmit to other controllers without hindrance Opt-out of the processing of data for the purposes of targeted advertising, sale and profiling for decisions that impact the consumer Not be discriminated against for exercising their data privacy rights	Up to $5,000 per violation plus compensation for the expenses incurred in the investigation if violations are not cured within 30 days of notice

Pennsylvania	Consumer Data Privacy Act (CDPA)	No	Applies to businesses that collect consumers' personal information-- either directly or through a mediating entity, such as a processor-- and do business in Pennsylvania that have a gross revenue over $10 million, buys, sells or shares the personal information of 50,000 or more consumers, households or devices or derives 50% or more of its annual revenue from selling consumers' personal information	Consumers have a private right to action when harmed by a breach resulting in a violation of the law. They can seek statutory damages between $100 and $750 per incident or actual damages, whichever is greater, as well as injunctive relief, declaratory relief or any other relief deemed appropriate by the court	N/A	N/A	N/A	Third parties may not resell personal data that has been sold to them unless they notify the subject and give them an opportunity to opt-out of the sale	Know what data is being collected about them including the source of the data, the purpose of collection and any third-party with whom the data is shared Access data collected about them Know whether their data is being sold and, if so, to whom Opt-out of the sale of their data Not be denied a good or service, charged a different price or provided a different level of quality for exercising their rights	Up to $7,500 per violation if violations are not cured within 30 days of notice
Colorado	Colorado Privacy Act (CPA)	No	Applies to any legal entities that conduct business or provide products or services intentionally targeted to Colorado residents that control or process the personal data of over 100,000 consumers annually or control or process the personal data of over 25,000 consumers and sell personal data for profit		Controllers must provide a "reasonably accessible, clear and meaningful" privacy notice including the controller's contact information, the categories of personal data collected and processed, the purposes for the processing of each category, the categories of data shared with third-parties and the categories of third-parties the data is shared with. It must also inform consumers of how they can exercise their privacy rights, including their right to appeal a controller's decision regarding a request.	Entities may only use data for the purposes specified in the notice, unless the consumer consents to other uses Entities may not sell data or use it for targeted advertising if the consumers has opted-out, unless they have explicitly consented to the activity	Controllers must conduct and document a data protection assessment for any processing activity that presents a "heightened risk of harm" to the consumer Processors and controllers must enter into a contract outlining the type, nature, purpose and duration of data processing. This contract must oblige the processor to delete or return all personal data to the controller upon request, make all information necessary to comply with CPA available to the controller and comply with all reasonable audits and inspections by the controller	N/A	Confirm whether their data is being processed Access data collected about or from them Correct inaccuracies in their data Delete any data provided by or obtained about them Obtain a copy of the data in a readable format that consumers can transfer to another entity (data portability) Opt-out of any data processing activity done for the purposes of sale, targeted advertising or profiling in furtherance of decisions that impact them Have another entity submit an opt-out request on their behalf Not be discriminated against for exercising their data privacy rights	Up to $20,000 per violation per consumer, with a maximum of $500,000 for a related series of violations, if violations are not cured within 60 days of notice.

China	Data Security Law of the People's Republic of China (DSL)	No	The scope of the law includes any processing activities outside of China that may undermine China's public interests, national security or the rights of its organizations and citizens. However, the criteria for judging what extraterritorial activities apply and how organizations outside of China can be held liable is left ambiguous.	N/A	N/A	N/A	"Important data" – as deemed so by supervisory authorities and China's national security agency – will be subject to enhanced protections. "National core data" – data related to vital public interests such as national security, the economy and important people's livelihoods – will be subject to even stricter protections than "important data." Processors of data that meet the criteria will need to assign the responsibility of DSL compliance to a data security officer and data protection department and submit regular risk assessments of their processing activity to authorities, outlining the nature of the processing, potential security risks and safeguards put in place to protect the data	"Important data" collected in China must be stored locally, unless cross-border transfers are necessary for business needs. In such cases, the data may be transferred abroad, given a security assessment is conducted. However, this privilege is only afforded to organizations that are "critical information infrastructure operators".	N/A	Fines and penalties for violations of DSL depend on the nature of the violation. • Organizations that breach the DSL's data security protection obligations may be subject to a fine from RMB 50,000 ($7725 USD) to RMB 2 million ($309,000 USD) while individuals responsible may be fined up to RMB 200,000 ($30,900 USD). • For violations deemed to impede or endanger national sovereignty, security or development interests, organizations will face fines between RMB 2 million and RMB 10 million ($1.5 million USD). • Violations of cross-border transfers requirements carry fines of up to RMB 10 million for organizations and RMB 1 million ($154,500 USD) for individuals. • For sharing data stored in China with foreign judicial or law enforcement agencies without first obtaining approval from the Chinese government, the fine is up to RMB

										• 5 million ($772,500 USB) for organizations and RMB 500,000 ($77,250 USD) for individuals. • Organizations that refuse to cooperate with access requests from the Chinese government may be fined up to RMB 500,000, while individuals face a maximum fine of RMB 100,000 ($15,500 USD) for such an offense.